Preface

Note The terms “Unidirectional Path Switched Ring” and “UPSR” may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as “Path Protected Mesh Network” and “PPMN,” refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This section explains the objectives, intended audience, and organization of this publication and describes the conventions that convey instructions and other information.

This section provides the following information:

Revision History

Date	Notes
November 2009	• Added this Revision History table. • Updated the section “NTP-A326 Create a Server Trail” in the chapter, “Create Circuits and VT Tunnels”. • Added a note in “Delete a PPM from the MRC-12, MRC-2.5G-4, or OC192-XFP Card” procedure in the chapter, “DLPs A500 to A599”. • Updated the figure for fan tray assembly in Chapter 1, “Install the Shelf and Backplane Cable” and Chapter 15, “Maintain the Node”.

Date	Notes
December 2009	• Updated the note in "Create Protection Groups" procedure in Chapter 4, Turn Up a Node. • Updated the fan tray caution in the section "NTP-A7 Install the Fan-Tray Assembly" in the chapter "Install the Shelf and Backplane Cable". • Updated NTP-A316 in the chapter, Install Cards and Fiber-Optic Cable.
January 2010	• Updated the sections "DLP-A600 Perform BLSR Lockout" and "DLP-A601 Remove BLSR Lockout" in the chapter "DLPs A600 to A699". • Updated the section "NTP-A94 Upgrade OC-N Cards and Spans Automatically" in the chapter "Upgrade Cards and Spans". • Updated the "Add a Path Protection Node" procedure in Chapter 14, "Add and Remove Nodes".
February 2010	• Added a note to NTP-A356 in the chapter, "Maintain the Node".
May 2010	• Updated the link integrity soak duration range as 200 ms to 10000 ms in the section "DLP-A581 Configure Link Integrity Timer" in the chapter "DLPs A500 to A599".
June 2010	• Updated "DLP-A578 Configuring Windows Vista to Support CTC" in the chapter, "Connect the PC and Log into the GUI". • Updated the section "NTP-A94 Upgrade OC-N Cards and Spans Automatically" in the chapter "Upgrade Cards and Spans".
August 2010	• Updated the procedures "Roll the Source or Destination of One Optical Circuit", "Roll One Cross-Connect from an Optical Circuit to a Second Optical Circuit", "Roll Two Cross-Connects on One Optical Circuit Using Automatic Routing", "Roll Two Cross-Connects on One Optical Circuit Using Manual Routing", "Roll Two Cross-Connects from One Optical Circuit to a Second Optical Circuit" in the chapter "DLPs A400 to A499". • Removed the reference to G1000 card support in the chapters "DLPs A500 to A599" and "Maintain the Node". • Added a note to DS3XM-12 in the chapter, "Maintain the Node".
September 2010	• Added a note to the table "OC-N Card Line Settings" in the chapter, DLPs A300 to A399.
October 2010	• Added a note in the chapters, "Maintain the Node", "Install the Shelf and Backplane Cable", and "DLPs A1 to A99".
November 2010	• Added Step 11 and a note to Step 9 in the procedure, "DLP-A17 Connect Office Power to the ONS 15454 Shelf". • Updated Step 1 in the procedure "DLP-A18 Turn On and Verify Office Power". • Added a note to DLP-A509 in the chapter, DLPs A500 to A599. • Updated Step 11 in the procedure "DLP-A448 Convert DS3XM-6 or DS3XM-12 Cards From 1:1 to 1:N Protection".

Date	Notes
December 2010	• Added a note to the “NTP-A94 Upgrade OC-N Cards and Spans Automatically” in the chapter, “Upgrade Cards and Spans”. • Updated the section “NTP-A306 Off-Load the Diagnostics File” in the chapter, “Maintain the Node”.
January 2011	• Updated the table “OC-N Card Line Settings” in the chapter, “DLPs A300 to A399”. • Updated the procedure “A370 Upgrade OC-N Cards to Multirate Cards” in the chapter, “Upgrade Cards and Spans”.
March 2011	• Added a note in the chapter, “Upgrade Cards and Spans”.
September 2011	• Updated the “Test DS1/E1-56 and DS3XM-12 Electrical Card Ports” in the chapter, “Maintain the Node”.
October 2011	Updated the section “DLP-A456 Configure the Node for RADIUS Authentication” in the chapter “DLPs A400 to A499”.
December 2011	Updated the procedure, “NTP-A94 Upgrade OC-N Cards and Spans Automatically” in the chapter, “Upgrade Cards and Spans”.
May 2012	• Added a note to “NTP-A94 Upgrade OC-N Cards and Spans Automatically” procedure in the chapter, “Upgrade Cards and Spans”. • Added a new procedure “NTP-A370 Upgrade OC-N Cards Manually” to the chapter, “Upgrade Cards and Spans”.
August 2012	• The full length book-PDF was generated.
November 2012	• Added a note to “NTP-A194 Create Overhead Circuits” procedure in the chapter “Create Circuits and VT Tunnels”. • Added a note to “DLP-A377 Provision Section DCC Terminations” and “DLP-A378 Provision Line DCC Terminations” procedures in the chapter “DLPs A300 to A399”. • Updated Table 12-1 in the procedure, “NTP-A370 Upgrade OC-N Cards Manually” in the chapter, “Upgrade Cards and Spans”. • Updated the “NTP-A107 Inspect and Replace the Air Filter” procedure in the chapter “Maintain the Node”.
January 2013	• Updated the procedure, “NTP-A94 Upgrade OC-N Cards and Spans Automatically” in the chapter, “Upgrade Cards and Spans”.
May 2013	Added the procedure, "NTP-A375 Set Up Secure Access to the ONS 15454 TL1" to the chapter, "Turn Up a Node".
June 2013	Added the procedure, “A376 Upgrading a BLSR Ring Using an MRC-12 Card” to the chapter, “Convert Network Configurations”.

Document Objectives

This guide provides procedures for installation, turn up, provisioning, and acceptance of ONS 15454 nodes and ONS 15454 networks. It is organized in a Cisco recommended work flow sequence for new installations, in addition to allowing easy access to procedures and tasks associated with adds, moves, and changes for existing installations.

Use the guide in conjunction with the appropriate publications listed in the Related Documentation section.

Audience

To use this publication, you should be familiar with Cisco or equivalent optical transmission hardware and cabling, telecommunications hardware and cabling, electronic circuitry and wiring practices, and preferably have experience as a telecommunications technician.

Document Organization

The organization of the guide reflects Cisco's recommended work flow for new installations. This organization also provides easy access to procedures and tasks used to modify existing installations. Verification procedures are provided, where necessary, to allow contract vendors to complete the physical installation and then turn over the site to craft personnel for verification, provisioning, turn up, and acceptance.

The front matter of the book appears in the following sequence:

1. Title Page
2. Table of Contents
3. List of Figures
4. List of Tables
5. List of Procedures
6. List of Tasks

The information in the book follows a task-oriented hierarchy using the elements described below.

Chapter (Director Level)

The guide is divided into logical work groups (chapters) that serve as director entry into the procedures. For example, if you are arriving on site after a contractor has installed the shelf hardware, proceed to Chapter 2, "Install Cards and Fiber-Optic Cable" and begin verifying installation and installing cards. You may proceed sequentially (recommended), or locate the work you want to perform from the list of procedures on the first page of every chapter (or turn to the front matter or index).

Each NTP is a list of steps designed to accomplish a specific procedure. Follow the steps until the procedure is complete. If you need more detailed instructions, refer to the Detailed Level Procedure (DLP) specified in the procedure steps.

Note Throughout this guide, NTPs are referred to as "procedures" and DLPs are termed "tasks." Every reference to a procedure includes its NTP number, and every reference to a task includes its DLP number.

Detailed Level Procedure (DLP)

The DLP (task) supplies additional task details to support the NTP. The DLP lists numbered steps that lead you through completion of a task. Some steps require that equipment indications be checked for verification. When the proper response is not obtained, the DLP provides a trouble clearing reference.

Related Documentation

Use the *Cisco ONS 15454 Procedure Guide* with the following referenced Release 9.1, 9.2, and 9.2.1 publications:

- *Cisco ONS 15454 Reference Manual*
  Provides detailed card specifications, hardware and software feature descriptions, network topology information, and network element defaults.
- *Cisco ONS 15454 Troubleshooting Guide*
  Provides alarm descriptions, alarm and general troubleshooting procedures, error messages, and transient conditions.
- *Cisco ONS SONET TL1 Command Guide*
  Provides a full TL1 command and autonomous message set including parameters, AIDs, conditions and modifiers for the Cisco ONS 15454, ONS 15600, ONS 15310-CL, and ONS 15310-MA systems.
- *Cisco ONS SONET TL1 Reference Guide*
  Provides general information, procedures, and errors for TL1 in the Cisco ONS 15454, ONS 15600, ONS 15310-CL, and ONS 15310-MA systems.
- *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*
  Provides software features for all Ethernet cards and configuration information for Cisco IOS on ML-Series cards.
- *Release Notes for the Cisco ONS 15454 Release 9.1*
  Provides caveats, closed issues, and new feature and functionality information.
- *Release Notes for Cisco ONS 15454 SONET and SDH, Release 9.2*
  Provides caveats, closed issues, and new feature and functionality information.
- *Release Notes for Cisco ONS 15454 SDH, Release 9.2.1*
  Provides caveats, closed issues, and new feature and functionality information.

For an update on End-of-Life and End-of-Sale notices, refer to http://www.cisco.com/en/US/products/hw/optical/ps2006/prod_eol_notices_list.html.

Document Conventions

This publication uses the following conventions:

Convention	Application
boldface	Commands and keywords in body text.
italic	Command input that is supplied by the user.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x | x | x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. The user must select one.
Ctrl	The control key. For example, where Ctrl + D is written, hold down the Control key while pressing the D key.
`screen font`	Examples of information displayed on the screen.
`boldface screen font`	Examples of information that the user must enter.
< >	Command parameters that must be replaced by module-specific codes.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Caution Means *reader be careful*. In this situation, the user might do something that could result in equipment damage or loss of data.

Warning **IMPORTAN SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

FONTOS BIZTONSÁGI ELOÍRÁSOK

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告　重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告　安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의　중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

Aviso　**INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.

GUARDE ESTAS INSTRUÇÕES

Advarsel　**VIGTIGE SIKKERHEDSANVISNINGER**

Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.

GEM DISSE ANVISNINGER

تحذير　**إرشادات الأمان الهامة**

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز.
قم بحفظ هذه الإرشادات

Upozorenje

VAŽNE SIGURNOSNE NAPOMENE

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SAČUVAJTE OVE UPUTE

Upozornění

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie **WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA**

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie **DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY**

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD

Obtaining Optical Networking Information

This section contains information that is specific to optical networking products. For information that pertains to all of Cisco, refer to the Obtaining Documentation and Submitting a Service Request section.

Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco Optical Transport Products Safety and Compliance Information* document that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15454 system. It also includes translations of the safety warnings that appear in the ONS 15454 system documentation.

Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15xxx product documentation, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated periodically and may be more current than printed documentation.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Cisco ONS Documentation Roadmap for Release 9.2.1

To quickly access publications of Cisco ONS Release 9.2.1, see the Cisco ONS Documentation Roadmap for Release 9.2.1.

CHAPTER 1

Install the Shelf and Backplane Cable

This chapter provides procedures for installing the Cisco ONS 15454. For a summary of the tools and equipment required for installation, see the "Required Tools and Equipment" section on page 1-2.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A1 Unpack and Inspect the ONS 15454 Shelf Assembly, page 1-4—Complete this procedure before continuing with the "NTP-A2 Install the Shelf Assembly" procedure on page 1-5.
2. NTP-A2 Install the Shelf Assembly, page 1-5—Complete this procedure to install the shelf assembly in a rack.
3. NTP-A3 Open and Remove the Front Door, page 1-6—Complete this procedure to access the equipment before continuing with other procedures.
4. NTP-A4 Remove the Backplane Covers, page 1-7—Complete this procedure to access the backplane before continuing with other procedures.
5. NTP-A5 Install the EIAs, page 1-8—Complete this procedure if you plan to install electrical cards. This procedure is a prerequisite to the "NTP-A9 Install the Electrical Card Cables on the Backplane" procedure on page 1-23.
6. NTP-A6 Install the Power and Ground, page 1-9—Complete this procedure before continuing with the "NTP-A7 Install the Fan-Tray Assembly" procedure on page 1-11.
7. NTP-A7 Install the Fan-Tray Assembly, page 1-11—Complete this procedure to install the fan-tray assembly in the shelf.
8. NTP-A119 Install the Alarm Expansion Panel, page 1-14—Complete this procedure if you are planning to install the Alarm Interface Controller–International (AIC-I) card and want to increase the number of alarm contacts provided by the AIC-I card.
9. NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-17—Complete this procedure as needed to set up wire-wrap pin connections.
10. NTP-A120 Install an External Wire-Wrap Panel to the AEP, page 1-18—Complete this procedure to connect an external wire-wrap panel to the alarm expansion panel (AEP).
11. NTP-A9 Install the Electrical Card Cables on the Backplane, page 1-23—Complete this procedure if you plan to install electrical card cables.
12. NTP-A10 Route Electrical Cables, page 1-24—Complete this procedure as needed to route electrical cables installed on the backplane.

13. NTP-A11 Install the Rear Cover, page 1-24—Complete this procedure as needed to install the rear cover.
14. NTP-A13 Perform the Shelf Installation Acceptance Test, page 1-31—Complete this procedure to determine if you have correctly completed all other procedures in the chapter.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **This unit is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.** Statement 37

Warning **Suitable for mounting on concrete or other non-combustible surface only.** Statement 345

Warning **The covers are an integral part of the safety design of the product. Do not operate the unit without the covers installed.** Statement 1077

Required Tools and Equipment

You need the following tools and equipment to install and test the ONS 15454.

Cisco-Supplied Materials

The following materials are required and are shipped with the ONS 15454 shelf (wrapped in plastic). The number in parentheses gives the quantity of the item included in the package.

- #12-24 x 3/4 pan-head Phillips mounting screws (48-1004-XX, 48-1007-XX) (8)
- #12 -24 x 3/4 socket set screws (48-1003-XX) (2)
- T-handle #12-24 hex tool for set screws (1)
- ESD wrist strap with 1.8 m (6 ft) coil cable (1)
- Tie wraps (10)
- Pinned hex (Allen) key for front door (1)
- Spacers (50-1193-XX) (4)
- Spacer mounting brackets (2)
- Clear plastic rear cover (1)
- External (bottom) brackets for the fan-tray air filter
- Shelf accessory kit (53-2329-XX) (optional)
  - Two mounting bars (700-19701-XX)
  - Four 1-inch standoffs (50-1193-01)

  - Four 1 3/8-inch standoffs (50-1492-01)
  - Eight 2-inch standoffs (50-1453-01)
  - Four flathead screws, 6-32 x 0.5 (48-2116-01)
- Standoff kit (53-0795-XX):
  - Plastic fiber management guides (2)
  - Fan filter bracket screws (53-48-0003) (6)

The following materials are required to install the optional air ramp. The number in parentheses gives the quantity of the item included in the package:

- M4.0x 8mm, SS pan-head Phillips mounting screws (2)
- Mounting brackets, 19 inch (482.6 mm), 23 inch (584.2 mm) (2)

User-Supplied Materials

The following materials and tools are required but are not supplied with the ONS 15454:

- One or more of the following equipment racks:
  - 19-inch ANSI Standard (Telcordia GR-63-CORE) (482.6 mm) rack; total width 22 inches (558.8 mm)
  - 23-inch ANSI Standard (Telcordia GR-63-CORE) (584.2 mm) rack; total width 26 inches (660.4 mm)
- Fuse panel
- Power cable (from fuse and alarm panel to assembly), #10 AWG, copper conductors, 194 degrees Fahrenheit (90 degrees Celsius)
- Ground cable #6 AWG stranded
- Alarm cable pairs for all alarm connections, #22 or #24 AWG (0.51 mm^2 or 0.64 mm^2), solid tinned
- 100-ohm shielded building integrated timing supply (BITS) clock cable pair #22 or #24 AWG (0.51 mm^2 or 0.64 mm^2), twisted-pair T1-type
- Single-mode SC fiber jumpers with UPC polish (55 dB or better) for optical (OC-N) cards
- Shielded coaxial cable terminated with SMB or BNC connectors for DS-3 cards
- Shielded ABAM cable terminated with AMP Champ connectors or unterminated for DS1N-14 cards with #22 or #24 AWG (0.51 mm^2 or 0.64 mm^2) ground wire (typically about two ft [61 cm] in length)
- 6-pair #29 AWG double-shielded cable
- Tie wraps and/or lacing cord
- Labels
- Listed pressure terminal connectors, typically dual lug type; connectors must be suitable for #6 AWG copper conductors with stud size and spacing per equipment rack specifications; connection to office ground typically through H-TAP compression connector, according to site practice

Tools Needed

The following tools are needed to install an ONS 15454:

- #2 Phillips screwdriver

- Medium slot-head screwdriver
- Small slot-head screwdriver
- Wire wrapper
- Wire cutters
- Wire strippers
- Crimp tool
- BNC insertion tool

Test Equipment

The following test equipment is needed to install an ONS 15454:

- Voltmeter
- Optical power meter (for use with fiber optics only)
- Bit error rate (BER) tester, DS-1 and DS-3

NTP-A1 Unpack and Inspect the ONS 15454 Shelf Assembly

Purpose	This procedure unpacks the ONS 15454 and verifies the contents.
Tools/Equipment	Pinned hex (Allen) key for front door
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note The ONS 15454 high-density shelf (15454-SA-HD) is required if you want to use the high-density electrical cards (DS3/EC1-48 and DS1/E1-56 cards).

Step 1 Complete the "DLP-A1 Unpack and Verify the Shelf Assembly" task on page 17-1.

Step 2 Complete the "DLP-A2 Inspect the Shelf Assembly" task on page 17-2.

Step 3 Continue with the "NTP-A2 Install the Shelf Assembly" procedure on page 1-5.

Stop. You have completed this procedure.

NTP-A2 Install the Shelf Assembly

Purpose	This procedure reverses the mounting bracket and mounts shelf assemblies in a rack.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Pinned hex key Two set screws (48-1003-XX)
Prerequisite Procedures	NTP-A1 Unpack and Inspect the ONS 15454 Shelf Assembly, page 1-4
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 131°F (55°C).** Statement 1047

Warning **To prevent airflow restriction, allow at least 1 inch (25.4 mm) of clearance around the ventilation openings.**Statement 1076

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

- **This unit should be mounted at the bottom of the rack if it is the only unit in the rack.**
- **When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.**
- **If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.** Statement 1006

Warning **The ONS 15454 must have 1 inch (25.4 mm) of airspace below the installed shelf assembly to allow air flow to the fan intake. The air ramp (the angled piece of sheet metal on top of the shelf assembly) provides this spacing and should not be modified in any way.**

Note To install the air filter inside the air ramp unit (15454E-AIR-RAMP or 15454-AIR-RAMP), use the ETSI version of the air filter (15454-FTF2 or 15454E-FTF4).

Note The 10-Gbps-compatible shelf assembly (15454-SA-HD) and fan-tray assembly (15454-FTA3) are required with the ONS 15454 XC10G, OC-192, and OC-48 any slot (AS) cards.

Note The ONS 15454 installations are suitable for Network Telecommunication facilities and locations where NEC are applicable.

Step 1 Complete the "DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack" task on page 17-2 if you need to convert from a 23-inch (584.2 mm) to a 19-inch (482.6 mm) rack.

Step 2 To install the air filter on the bottom of the shelf rather than below the fan-tray assembly, complete the "DLP-A4 Install the External Brackets and Air Filter" task on page 17-4.

Step 3 Complete the necessary rack mount task:

- DLP-A5 Mount the Shelf Assembly in a Rack (One Person), page 17-5
- DLP-A6 Mount the Shelf Assembly in a Rack (Two People), page 17-6
- DLP-A7 Mount Multiple Shelf Assemblies in a Rack, page 17-7

Step 4 Continue with the "NTP-A3 Open and Remove the Front Door" procedure on page 1-6.

Stop. You have completed this procedure.

NTP-A3 Open and Remove the Front Door

Purpose	This procedure opens and removes the front door to access the equipment.
Tools/Equipment	Open-end wrench Pinned hex key
Prerequisite Procedures	NTP-A2 Install the Shelf Assembly, page 1-5
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Complete the "DLP-A8 Open the Front Door" task on page 17-8.

Step 2 As needed, complete the "DLP-A9 Remove the Front Door" task on page 17-9.

Step 3 Continue with the "NTP-A4 Remove the Backplane Covers" procedure on page 1-7.

Stop. You have completed this procedure.

NTP-A4 Remove the Backplane Covers

Purpose	This procedure describes how to access the backplane by removing the covers. The backplane has two sheet metal covers (one on either side) and a lower backplane cover at the bottom.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	NTP-A2 Install the Shelf Assembly, page 1-5 NTP-A3 Open and Remove the Front Door, page 1-6
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **The covers are an integral part of the safety design of the product. Do not operate the unit without the covers installed.**

Step 1 Complete the "DLP-A10 Remove the Lower Backplane Cover" task on page 17-10.

Step 2 Complete the "DLP-A11 Remove the Backplane Sheet Metal Cover" task on page 17-11.

Step 3 If you plan to install electrical interface assemblies (EIAs), continue with the "NTP-A5 Install the EIAs" procedure on page 1-8. If not, continue with the "NTP-A6 Install the Power and Ground" procedure on page 1-9.

Stop. You have completed this procedure.

NTP-A5 Install the EIAs

Purpose	This procedure describes how to install electrical interface assemblies (EIAs). Typically, an EIA panel is installed on the backplane during manufacturing, but EIA panels can be ordered separately. Refer to the *Cisco ONS 15454 Reference Manual* for descriptions of the EIAs.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Perimeter screws (9) Inner screws (12) Backplane cover screws (5) EIA card (SMB, BNC, AMP Champ, UBIC-V, UBIC-H, MiniBNC)
Prerequisite Procedures	NTP-A4 Remove the Backplane Covers, page 1-7
Required/As Needed	Required if the node will use electrical signals
Onsite/Remote	Onsite
Security Level	None

Caution Always use the supplied ESD wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Note EIAs are normally factory installed. Verify that the correct EIA is installed on the shelf assembly. If not, install the correct EIA.

Note You do not need to power down the shelf before removing or installing an EIA. An in-service upgrade of one EIA (A side or B side) is possible if all electrical traffic (DS-1, DS-3, DS3XM-6, and EC-1) is being carried on the other side.

Step 1 Complete the "DLP-A12 Install a BNC or High-Density BNC EIA" task on page 17-12 as needed. BNCs are locking connectors; the high-density BNC provides access to every port on every card.

Step 2 Complete the "DLP-A373 Install a MiniBNC EIA" task on page 20-56 as needed. The MiniBNC allows up to 96 DS-3 circuits on each side of the ONS 15454.

Step 3 Complete the "DLP-A13 Install an SMB EIA" task on page 17-15 as needed. SMBs allow you to access every port on every card using more space and efficient cabling.

Step 4 Complete the "DLP-A14 Install the AMP Champ EIA" task on page 17-16 as needed. AMP Champs are exclusive to DS-1 cables.

Step 5 Complete the "DLP-A190 Install a UBIC-V EIA" task on page 18-59 as needed. The UBIC-V (vertical) EIAs allow you to use high-density electrical cards. The UBIC-V EIAs provide SCSI connectors.

Step 6 Complete the "DLP-A399 Install a UBIC-H EIA" task on page 20-108 as needed. The UBIC-H (horizontal) EIAs allow you to use high-density electrical cards. The UBIC-H EIAs provide SCSI connectors.

Note To attach cables to the EIAs, see the "NTP-A9 Install the Electrical Card Cables on the Backplane" procedure on page 1-23.

Step 7 Continue with the "NTP-A6 Install the Power and Ground" procedure on page 1-9.

Stop. You have completed this procedure.

NTP-A6 Install the Power and Ground

Purpose	This procedure installs power feeds and grounds the ONS 15454.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Screws Power cable (from fuse and alarm panel to assembly), #10 AWG, copper conductors, 194 degrees F (90 degrees C) Ground cable (from equipment frame to office ground), #6 AWG stranded Listed pressure terminal connectors, typically dual lug type; connectors must be suitable for #6 AWG copper conductors with stud size and spacing per equipment rack specifications; connection to office ground typically through H-TAP compression connector, according to site practice Wire cutters Wire strippers Crimp tool Fuse panel
Prerequisite Procedures	NTP-A4 Remove the Backplane Covers, page 1-7
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit.** Statement 1003

Warning **This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.** Statement 39

Warning **Use copper conductors only.** Statement 1025

Warning **Connect the unit only to DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC 60950 based safety standards.** Statement 1033

Warning **This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.** Statement 1045

Warning **A readily accessible two-poled disconnect device must be incorporated in the fixed wiring.** Statement 1022

Warning **This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.** Statement 1028

Caution Always use the supplied ESD wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Step 1 Verify one of the following:

- If you have the 15454-SA-ANSI or 15454-SA-HD shelf, a 100-A fuse panel (35-A fuse per shelf minimum) should be installed. If not, install one according to manufacturer's instructions.
- If you have the 15454-SA-NEBS3 shelf, a standard 80-A fuse panel (20-A fuse per shelf minimum) should be installed. If not, install one according to manufacturer's instructions.

Step 2 Connect the chassis to the office ground. For detailed instructions on grounding the chassis, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Step 3 Complete the "DLP-A17 Connect Office Power to the ONS 15454 Shelf" task on page 17-18.

Step 4 Complete the "DLP-A18 Turn On and Verify Office Power" task on page 17-20.

Step 5 Continue with the "NTP-A7 Install the Fan-Tray Assembly" procedure on page 1-11.

Stop. You have completed this procedure.

NTP-A372 View Shelf Voltage and Temperature

Purpose	This procedure displays the shelf voltage and temperature of the ONS 15454 chassis in CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As Needed
Onsite/Remote	Remote
Security Level	Provisioning or higher

Note The temperature measured by the TCC2/TCC2P sensors appears on the LCD screen in the ONS 15454 chassis.

Note Read all references of "TCC2/TCC2P cards" in this document as "TCC2/TCC2P/TCC3 cards".

Step 1 In node view (single-node mode) or multishelf view (multishelf mode), click the **Provisioning** > **General** > **Voltage/Temperature** tabs. The Voltage/Temperature pane appears.

Step 2 The Voltage/Temperature pane retrieves the following values:

- Voltage A—Voltage of the shelf that corresponds to power supply A, in millivolts.
- Voltage B—Voltage of the shelf that corresponds to power supply B, in millivolts.
- Chassis Temperature—Temperature of the shelf in degrees Celsius.

Step 3 Click the **Reset** button to refresh the voltage and temperature values.

Stop. You have completed this procedure.

NTP-A7 Install the Fan-Tray Assembly

Purpose	This procedure installs the fan-tray assembly. Refer to the *Cisco ONS 15454 Reference Manual* for specific information about fan-tray assembly compatibility and air filters.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	NTP-A3 Open and Remove the Front Door, page 1-6 NTP-A6 Install the Power and Ground, page 1-9
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Caution Do not operate an ONS 15454 without a fan-tray air filter. A fan-tray air filter is mandatory.

Caution The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 Release 3.1 or later shelf assemblies (15454-SA-ANSI, 800-19857; 15454-SA-HD, 800-24848). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released earlier than ONS 15454 Release 3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N 800-0714915454). Installing the 15454-FTA3 in a noncompliant shelf assembly might result in failure of the alarm interface panel (AIP), which in turn, will result in power loss to the fan-tray assembly.

Note 15454-CC-FTA is compatible with Software Release 2.2.2 and greater and shelf assemblies 15454-SA-HD and 15454-SA-ANSI.

Caution You must place the edge of the air filter flush against the front of the fan-tray assembly compartment when installing the fan tray on top of the filter. Failure to do so could result in damage to the filter, the fan tray, or both.

Caution Do not force a fan-tray assembly into place. Doing so can damage the connectors on the fan tray and/or the connectors on the back panel of the shelf assembly.

Caution If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and readjust the position of the reusable filter until the fan tray fits correctly. Be sure that the grid on the reusable filter is on the side facing the fan tray.

Note If you are installing the ONS 15454 in an outside plant cabinet, remove the air filter to provide maximum cooling capabilities and to comply with Telcordia GR-487-CORE.

Note To install the fan-tray assembly, it is not necessary to move any of the cable-management facilities.

Step 1 Install the air filter. The air filter can be installed internally between the fan tray and shelf assembly, or externally by mounting the air filter bracket on the bottom of the shelf assembly. Slide the air filter into the bracket.

Caution Although the air filter can work with older fan trays if it is installed with either side facing up, Cisco recommends that you install it with the metal bracing facing up to preserve the surface of the filter. You must install the air filter with the metal bracing facing up with 15454-CC-FTA.

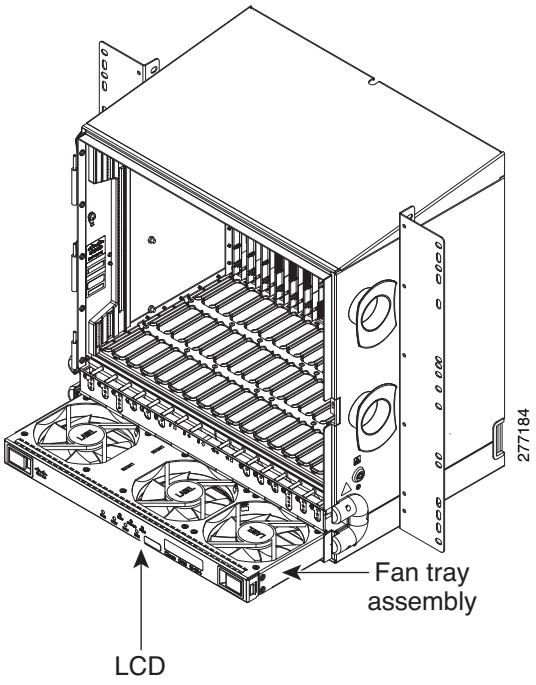
Step 2 Install the fan-tray assembly. The fan-tray assembly has locks on the outer edges. Press and hold the locks as you slide the fan-tray assembly into the shelf assembly. The electrical plug at the rear of the tray should plug into the corresponding receptacle on the assembly.

Caution Do not force a fan-tray assembly into place. This can damage the connectors on the fan-tray assembly and/or the connectors on the back panel of the shelf assembly.

Step 3 To verify that the tray has plugged into the backplane, look at the fan tray and listen to determine that the fans are running.

Figure 1-1 shows the location of the fan tray.

Figure 1-1 Installing the Fan-Tray Assembly



Step 4 Continue with the "NTP-A119 Install the Alarm Expansion Panel" procedure on page 1-14 if you plan to install an alarm expansion panel (AEP). If not, continue with the "NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections" procedure on page 1-17.

Stop. You have completed this procedure.

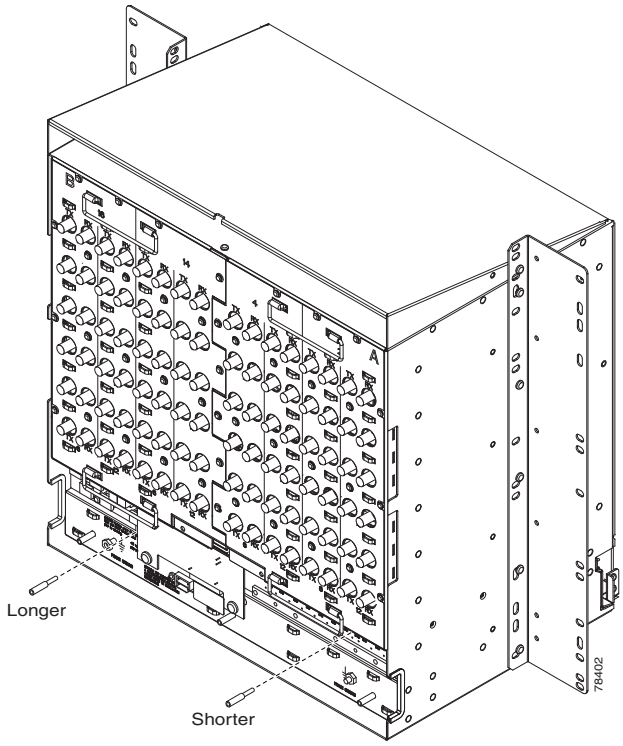
NTP-A119 Install the Alarm Expansion Panel

Purpose	This procedure installs an alarm expansion panel (AEP) onto the 15454-SA-ANSI or 15454-SA-HD shelf backplane. The AEP provides alarm contacts in addition to the 16 provided by the AIC-I card. Typically, the AEP is preinstalled when ordered with the ONS 15454; however, the AEP can be ordered separately. The AIC-I card must be installed before you can provision the alarm contacts enabled by the AEP.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Wire wrapper Standoffs (4)
Prerequisite Procedures	DLP-A10 Remove the Lower Backplane Cover, page 17-10
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note The AIC-I card provides direct alarm contacts (external alarm inputs and external control outputs). In the ANSI shelf, these AIC-I alarm contacts are routed through the backplane to wire-wrap pins accessible from the back of the shelf. When you install an AEP, the direct AIC-I alarm contacts cannot be used. Only the AEP alarm contacts can be used.

Step 1 Remove the two backplane screws. Replace the two screws with standoffs. Insert the longer standoff on the left and the shorter standoff on the right (Figure 1-2).

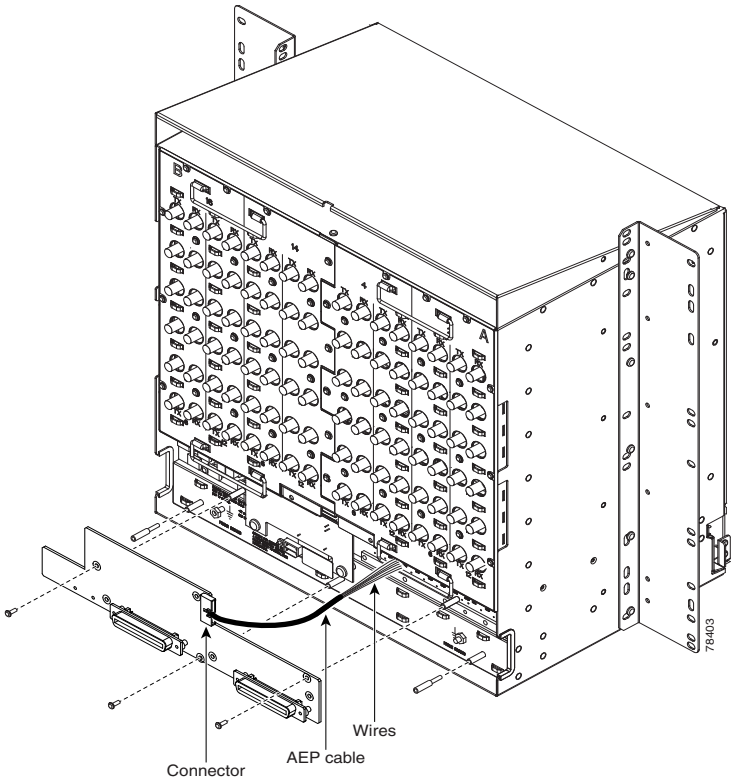
Figure 1-2 Replace Backplane Screws with Standoffs



Step 2 Attach the remaining two standoffs on either side of the backplane (Figure 1-3).

Step 3 Position the AEP board over the standoffs.

Figure 1-3 Installing Standoffs and the AEP



Step 4 Insert and tighten three screws to secure the AEP to the backplane.

Step 5 Connect the AEP cable to the backplane and AEP:

a. Connect the 10 colored wires to the wire-wrap pins on the backplane. Figure 1-4 shows where the cable wires are connected. Table 1-1 shows AEP and AIC-I signals that each wire carries.

b. Plug the other end of the AEP cable into AEP connector port. The brown pin is on the top.

Figure 1-4 AEP Wire-Wrap Connections to Backplane Pins

Table 1-1 Pin Assignments for the AEP

AEP Cable Wire	Backplane Pin	AIC-I Signal	AEP Signal
Black	A1	GND	AEP_GND
White	A2	AE_+5	AEP_+5
Slate	A3	VBAT–	VBAT–
Violet	A4	VB+	VB+
Blue	A5	AE_CLK_P	AE_CLK_P
Green	A6	AE_CLK_N	AE_CLK_N
Yellow	A7	AE_DIN_P	AE_DOUT_P
Orange	A8	AE_DIN_N	AE_DOUT_N
Red	A9	AE_DOUT_P	AE_DIN_P
Brown	A10	AE_DOUT_N	AE_DIN_N

Step 6 Continue with the "NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections" procedure on page 1-17.

Stop. You have completed this procedure.

NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections

Purpose	This procedure describes how to install alarm, timing, LAN, and craft wires.
Tools/Equipment	Wire wrapper #22 or #24 AWG (0.51 mm² or 0.64 mm²) alarm wires
Prerequisite Procedures	NTP-A4 Remove the Backplane Covers, page 1-7

Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **The covers are an integral part of the safety design of the product. Do not operate the unit without the covers installed.** Statement 1077

Step 1 Complete the "DLP-A19 Install Alarm Wires on the Backplane" task on page 17-21 if you are using an AIC-I card and are not using an AEP.

Step 2 Complete the "DLP-A20 Install Timing Wires on the Backplane" task on page 17-24 as needed. Timing wires are necessary to provision external timing.

Step 3 Complete the "DLP-A21 Install LAN Wires on the Backplane" task on page 17-25 as needed. LAN wires (or the LAN port on the TCC2/TCC2P) are necessary to create an external LAN connection.

Step 4 Complete the "DLP-A22 Install the TL1 Craft Interface" task on page 17-26 as needed. Craft wires (or the EIA/TIA-232 port on the TCC2/TCC2P) are required to access TL1 using the craft interface.

Caution Always use the supplied ESD wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Step 5 Complete one of the following:

- If you installed an AEP, continue with the "NTP-A120 Install an External Wire-Wrap Panel to the AEP" procedure on page 1-18.
- If you did not install an AEP and you plan to install electrical cards, continue with the "NTP-A9 Install the Electrical Card Cables on the Backplane" procedure on page 1-23.
- If you did not install an AEP and do not plan to install electrical cards, continue with the "NTP-A11 Install the Rear Cover" procedure on page 1-24.

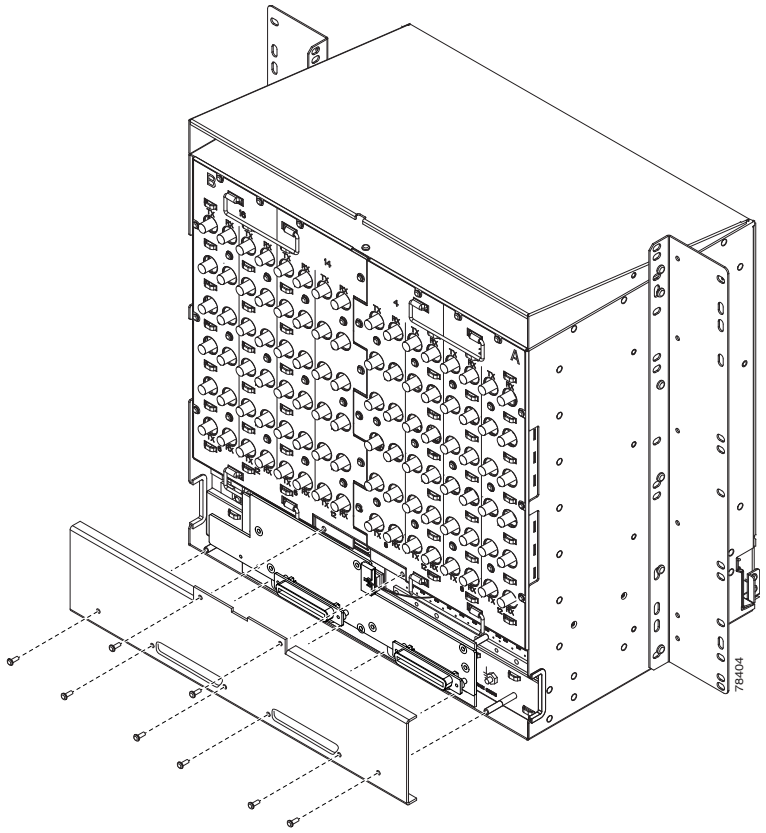
Stop. You have completed this procedure.

NTP-A120 Install an External Wire-Wrap Panel to the AEP

Purpose	This procedure connects an external wire-wrap panel to the AEP to provide the physical alarm contacts for the AEP.
Tools/Equipment	External wire-wrap panel
Prerequisite Procedures	NTP-A119 Install the Alarm Expansion Panel, page 1-14
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Position the lower cover over the AEP. Make sure that the AEP AMP Champ connectors protrude through the cutouts in the lower cover (Figure 1-5).

Figure 1-5 Installing the AEP Cover



Step 2 Insert and tighten the eight screws to secure the AEP cover to the AEP.

Step 3 Connect the cables from the external wire-wrap panel to the AMP Champ connectors on the AEP. Table 1-2 lists the alarm input pin assignments.

Table 1-2 Alarm Input Pin Assignments

AMP Champ Pin	Signal Name	AMP Champ Pin	Signal Name
1	ALARM_IN_1–	27	GND
2	GND	28	ALARM_IN_2–
3	ALARM_IN_3–	29	ALARM_IN_4–
4	ALARM_IN_5–	30	GND
5	GND	31	ALARM_IN_6–
6	ALARM_IN_7–	32	ALARM_IN_8–
7	ALARM_IN_9–	33	GND
8	GND	34	ALARM_IN_10–
9	ALARM_IN_11–	35	ALARM_IN_12–
10	ALARM_IN_13–	36	GND
11	GND	37	ALARM_IN_14–
12	ALARM_IN_15–	38	ALARM_IN_16–

Table 1-2 Alarm Input Pin Assignments (continued)

AMP Champ Pin	Signal Name	AMP Champ Pin	Signal Name
13	ALARM_IN_17–	39	GND
14	GND	40	ALARM_IN_18–
15	ALARM_IN_19–	41	ALARM_IN_20–
16	ALARM_IN_21–	42	GND
17	GND	43	ALARM_IN_22–
18	ALARM_IN_23–	44	ALARM_IN_24–
19	ALARM_IN_25–	45	GND
20	GND	46	ALARM_IN_26–
21	ALARM_IN_27–	47	ALARM_IN_28–
22	ALARM_IN_29–	48	GND
23	GND	49	ALARM_IN_30–
24	ALARM_IN_31–	50	—
25	ALARM_IN_+	51	GND1
26	ALARM_IN_0-	52	GND2

Table 1-3 lists the alarm output pin assignments.

Table 1-3 Alarm Output Pin Assignments

AMP Champ Pin	Signal Name	AMP Champ Pin	Signal Name
1	—	27	COM_0
2	COM_1	28	—
3	NO_1	29	NO_2
4	—	30	COM_2
5	COM_3	31	—
6	NO_3	32	NO_4
7	—	33	COM_4
8	COM_5	34	—
9	NO_5	35	NO_6
10	—	36	COM_6
11	COM_7	37	—
12	NO_7	38	NO_8
13	—	39	COM_8
14	COM_9	40	—
15	NO_9	41	NO_10
16	—	42	COM_10
17	COM_11	43	—

Table 1-3 Alarm Output Pin Assignments (continued)

AMP Champ Pin	Signal Name	AMP Champ Pin	Signal Name
18	NO_11	44	NO_12
19	—	45	COM_12
20	COM_13	46	—
21	NO_13	47	NO_14
22	—	48	COM_14
23	COM_15	49	—
24	NO_15	50	—
25	—	51	GND1
26	NO_0	52	GND2

Figure 1-6 illustrates the alarm input connectors.

Figure 1-6 Alarm Input Connector

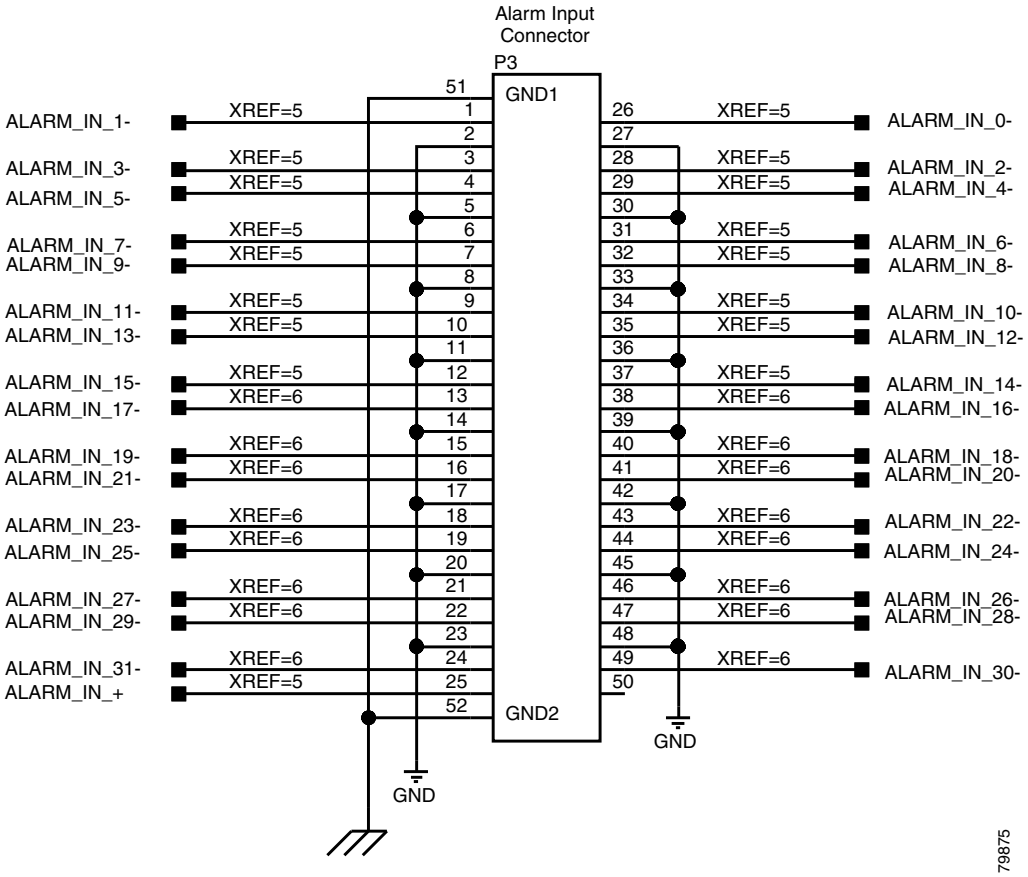
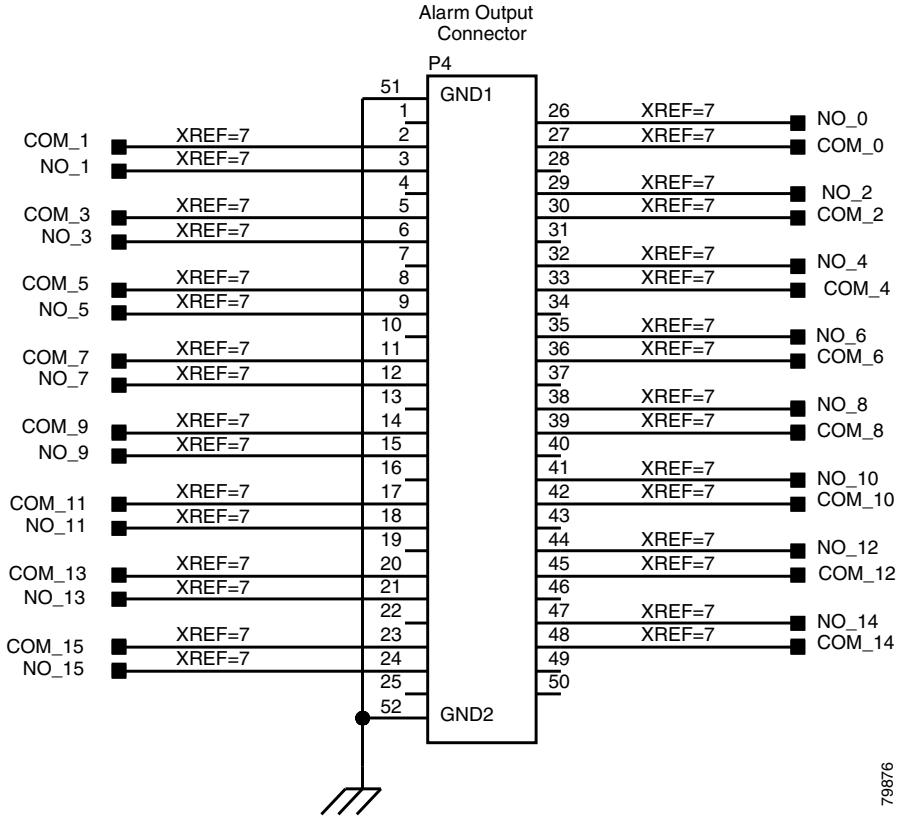


Figure 1-7 illustrates the alarm output connectors.

Figure 1-7 Alarm Output Connector



Step 4 Complete one of the following:

- If you plan to install electrical cards, continue with the "NTP-A9 Install the Electrical Card Cables on the Backplane" procedure on page 1-23.
- If you do not plan to install electrical cards, continue with the "NTP-A11 Install the Rear Cover" procedure on page 1-24.

Stop. You have completed this procedure.

NTP-A9 Install the Electrical Card Cables on the Backplane

Purpose	Optional EIA backplane covers are typically preinstalled when ordered with the ONS 15454. The following procedure describes how to install the electrical card cables to the backplane. If the shelf was not shipped with the correct EIA interface, you must order and install the correct EIA.
Tools/Equipment	Wire wrapper Twisted-pair cables BNC insertion tool SMB cable connector #2 Phillips screwdriver Medium slot-head screwdriver DS-1 and DS-3 cables, as needed Tie-down bar, as needed
Prerequisite Procedures	NTP-A5 Install the EIAs, page 1-8
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution Always use the supplied ESD wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Note Refer to the *Cisco ONS 15454 Reference Manual* for more information about EIAs.

Step 1 Complete the "DLP-A530 Install the Tie-Down Bar" task on page 22-31 as needed for routing the electrical cables you will install.

Step 2 Complete the "DLP-A23 Install DS-1 Cables Using Electrical Interface Adapters (Balun)" task on page 17-27 as needed. Baluns are used on SMB EIAs to properly terminate DS-1 signals.

Step 3 To install DS-1 cables using AMP Champ cables, complete the "DLP-A24 Install DS-1 AMP Champ Cables on the AMP Champ EIA" task on page 17-28.

Step 4 Complete the "DLP-A25 Install Coaxial Cable With BNC Connectors" task on page 17-31 as needed.

Step 5 Complete the "DLP-A26 Install Coaxial Cable With High-Density BNC Connectors" task on page 17-32 as needed.

Step 6 Complete the "DLP-A27 Install Coaxial Cable with SMB Connectors" task on page 17-32 as needed.

Step 7 Complete the "DLP-A386 Install Electrical Cables on the UBIC-V EIAs" task on page 20-84 as needed.

Step 8 Complete the "DLP-A441 Install Electrical Cables on the UBIC-H EIAs" task on page 21-23 as needed.

Step 9 Continue with the "NTP-A10 Route Electrical Cables" procedure on page 1-24.

Stop. You have completed this procedure.

NTP-A10 Route Electrical Cables

Purpose	This procedure routes and manages electrical (backplane) cables.
Tools/Equipment	RG179, RG59 (735A) #26 AWG cable, or RG59 (734A) #20 AWG cable
Prerequisite Procedures	NTP-A9 Install the Electrical Card Cables on the Backplane, page 1-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Complete the "DLP-A28 Route Coaxial Cables" task on page 17-34 as needed.

Step 2 Complete the "DLP-A29 Route DS-1 Twisted-Pair Cables" task on page 17-35 as needed.

Step 3 Continue with the "NTP-A11 Install the Rear Cover" procedure on page 1-24.

Stop. You have completed this procedure.

NTP-A11 Install the Rear Cover

Purpose	This procedure explains how to install the rear cover.
Tools/Equipment	#2 Phillips screwdriver 5/16-inch nut driver Shelf accessory kit (53-2329-XX) • Two mounting bars (700-19701-XX) • Four 1-inch standoffs (50-1193-01) • Four 1 3/8-inch standoffs (50-1492-01) • Eight 2-inch standoffs (50-1453-01) • Four flathead screws, 6-32 x 0.5 (48-2116-01) Plastic rear cover (700-06029-XX)
Prerequisite Procedures	NTP-A3 Open and Remove the Front Door, page 1-6
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Identify the EIA type where you will install the rear cover.

Step 2 According to Table 1-4, assemble the extended standoffs for that EIA type. Start with a 1 3/8-inch standoff and attach the other standoff(s) to that standoff to create an extended standoff. You should assemble two extended standoffs for each side, for a total of four extended standoffs per shelf.

Table 1-4 Standoffs Required for EIA Types

EIA Type	Required Standoffs for One Extended Standoff	Total Required Standoffs per Shelf
UBIC-V	One 1 3/8-inch Two 2-inch	Four 1 3/8-inch Eight 2-inch
UBIC-H	One 1 3/8-inch One 2-inch	Four 1 3/8-inch Four 2-inch
MiniBNC	One 1 3/8-inch One 2-inch	Four 1 3/8-inch Four 2-inch
BNC	One 1 3/8-inch One 1-inch	Four 1 3/8-inch Four 1-inch
High-Density BNC		
SMB		
AMP Champ		

Note As needed, attach additional standoffs to the extended standoffs to meet site-specific cable management requirements.

Step 3 Locate the mounting holes where you will install the standoffs on the EIAs you are using. Figure 1-8 shows the mounting holes on the UBIC-V. Figure 1-9 shows the mounting holes on the UBIC-H. Figure 1-10 shows the mounting holes on the remaining EIA types (MiniBNC, SMB, etc.). You can identify the mounting holes on all EIAs by locating the *REAR COVER BRACKET LOCATION* designation.

Figure 1-8 Mounting Holes on the UBIC-V EIA

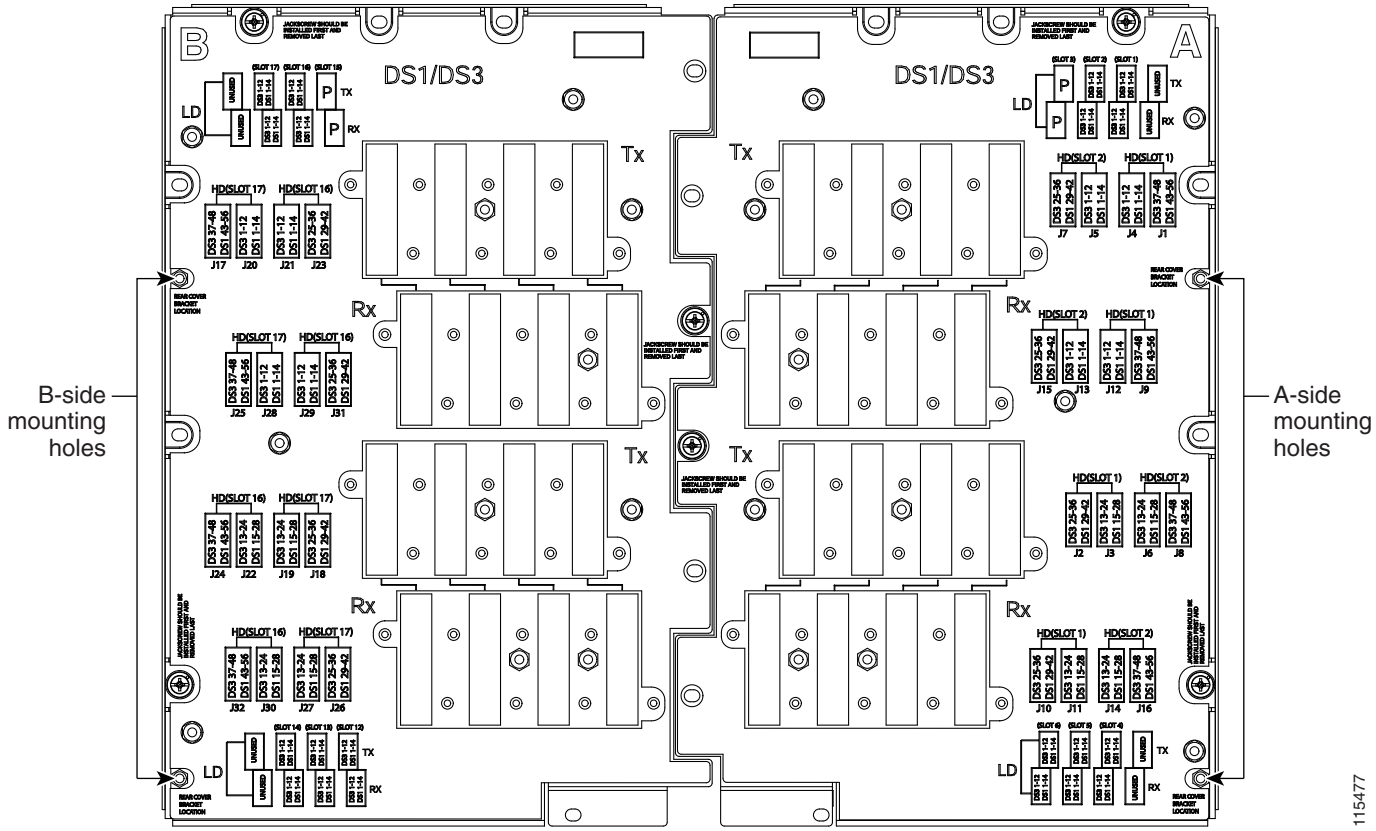


Figure 1-9 Mounting Holes on the UBIC-H

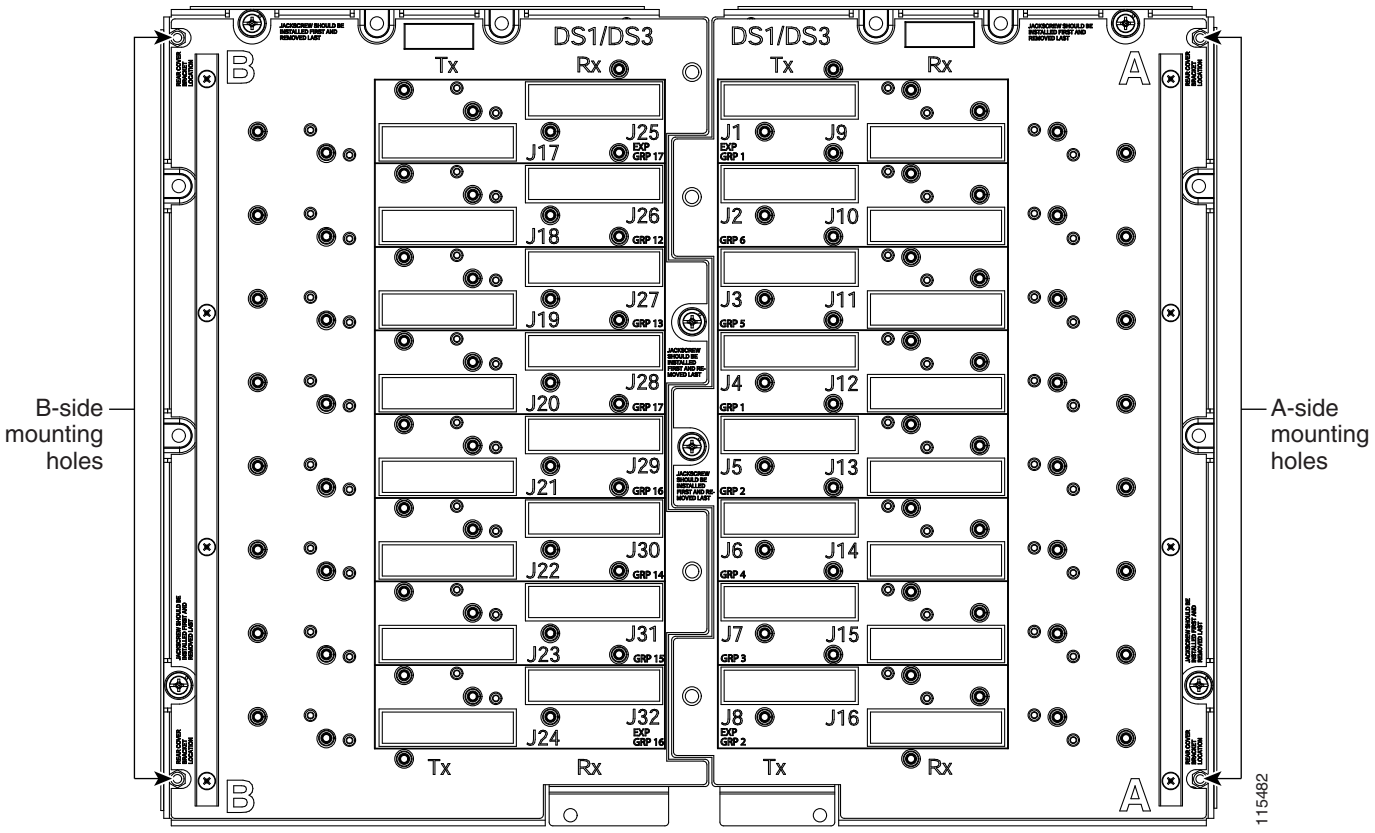
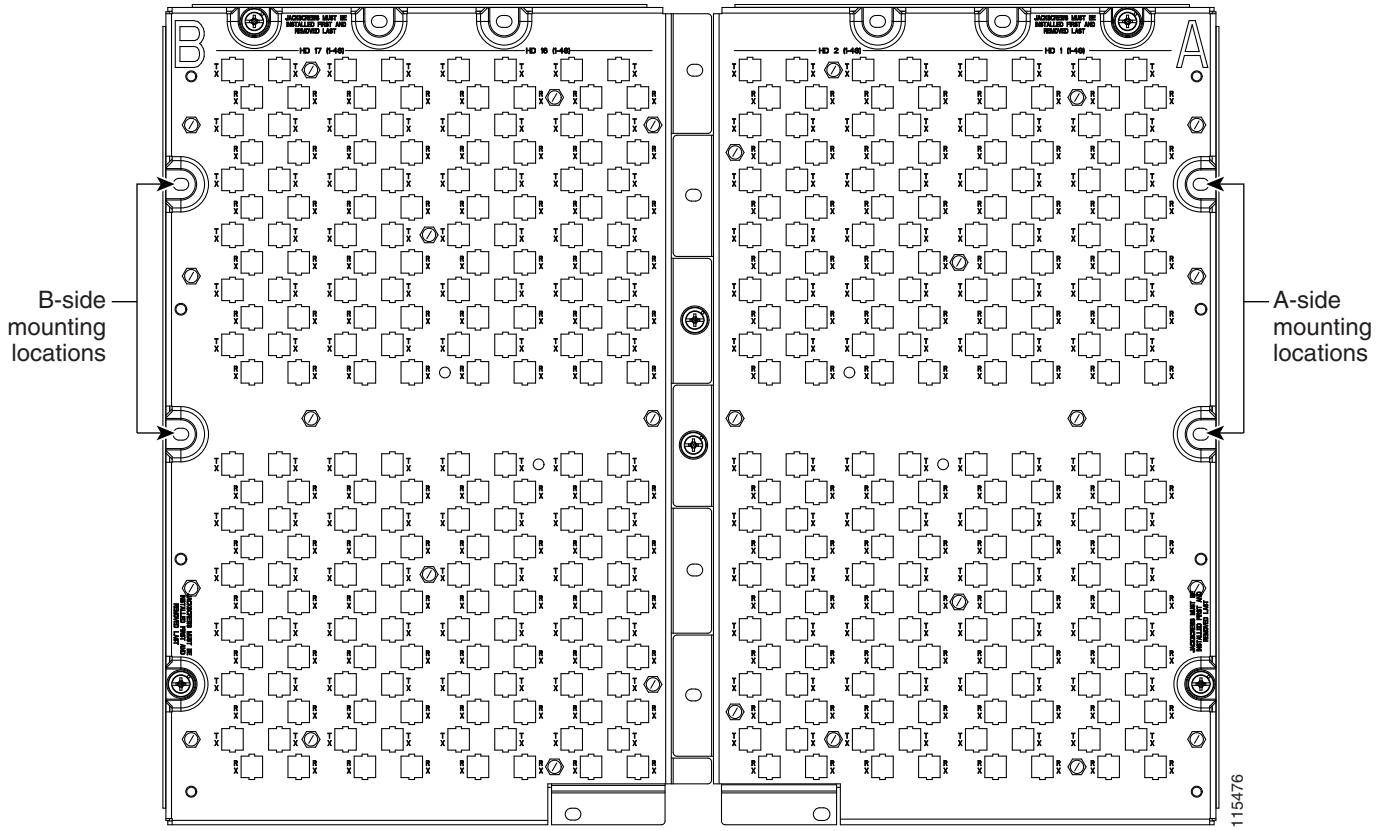


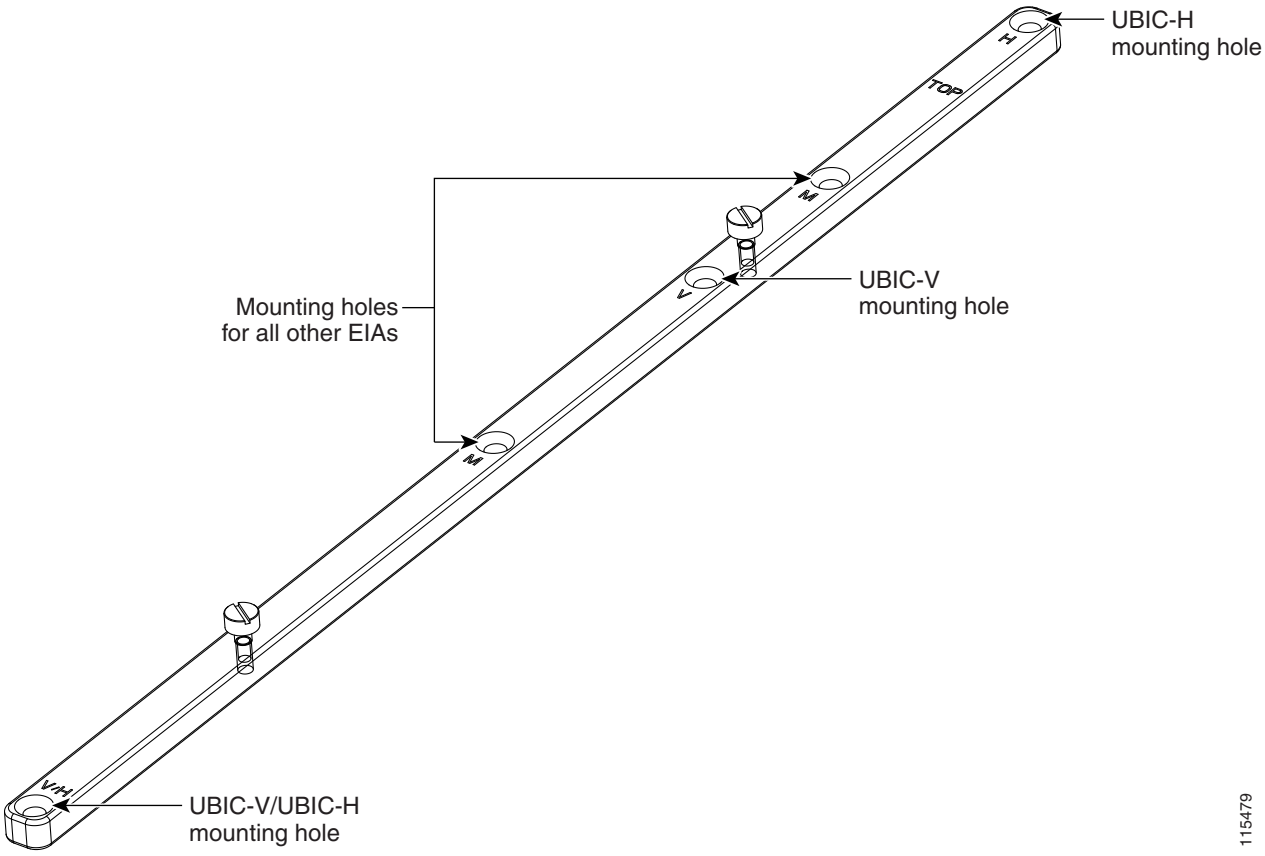
Figure 1-10 Mounting Holes on All Other EIA Types



Step 4 Use a 5/16-inch nutdriver to install the extended standoffs in the mounting holes.

Step 5 Locate the *TOP* designation on one of the mounting bars (700-19701-XX) and align the appropriate holes for your EIA with the extended standoffs (Figure 1-11).

Figure 1-11 EIA Labeling on the Mounting Bar



Step 6 Tighten the two screws (48-2116-01) for each mounting bar.

Step 7 Repeat Steps 5 and 6 for the second mounting bar.

Step 8 Attach the rear cover (700-06029-XX) by hanging it from the mounting screws on the back of the mounting bars and pulling it down until it fits firmly into place (Figure 1-12) or by using standoffs (Figure 1-13).

Figure 1-12 Installing the Rear Cover Onto the Mounting Bars

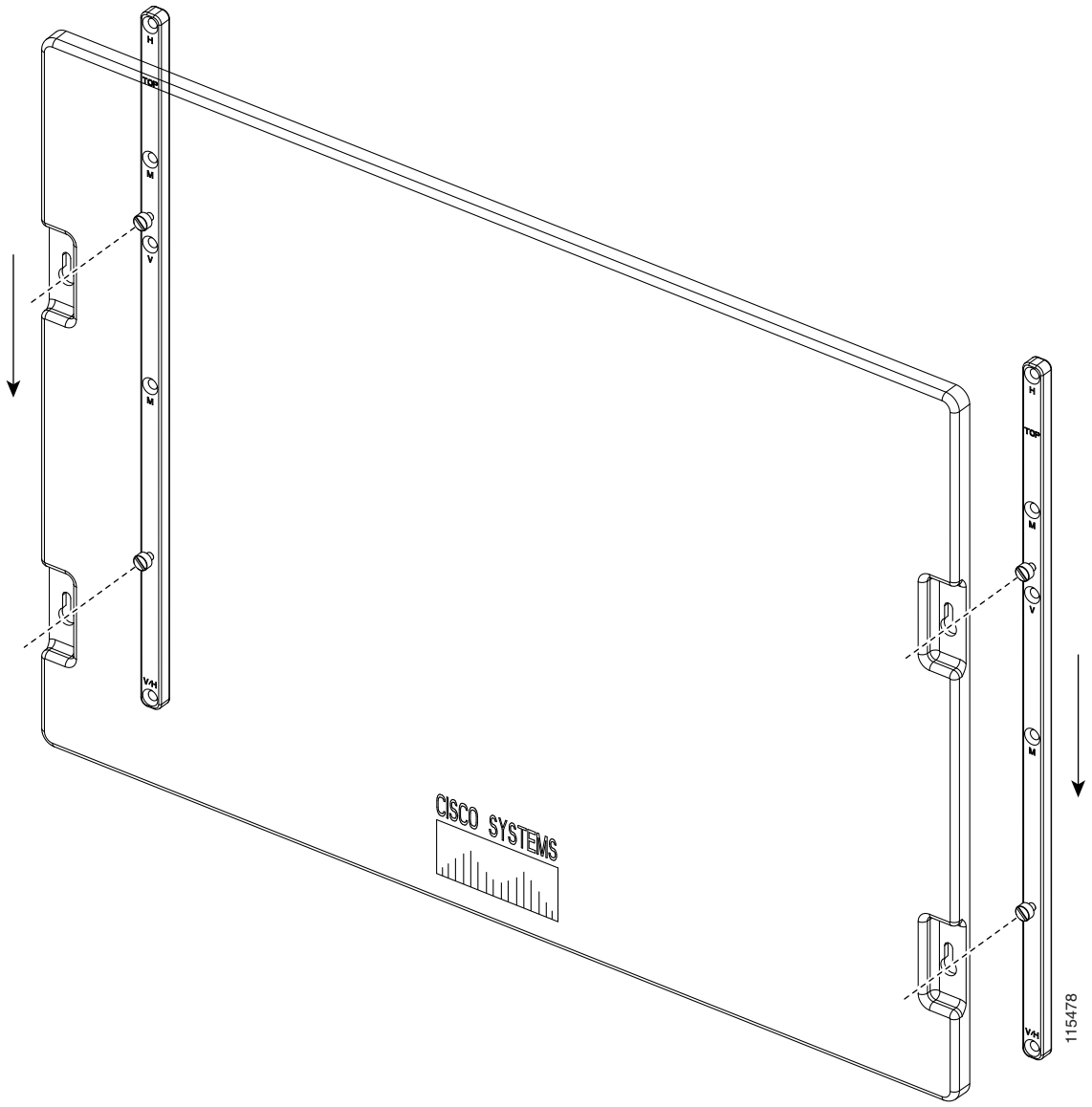
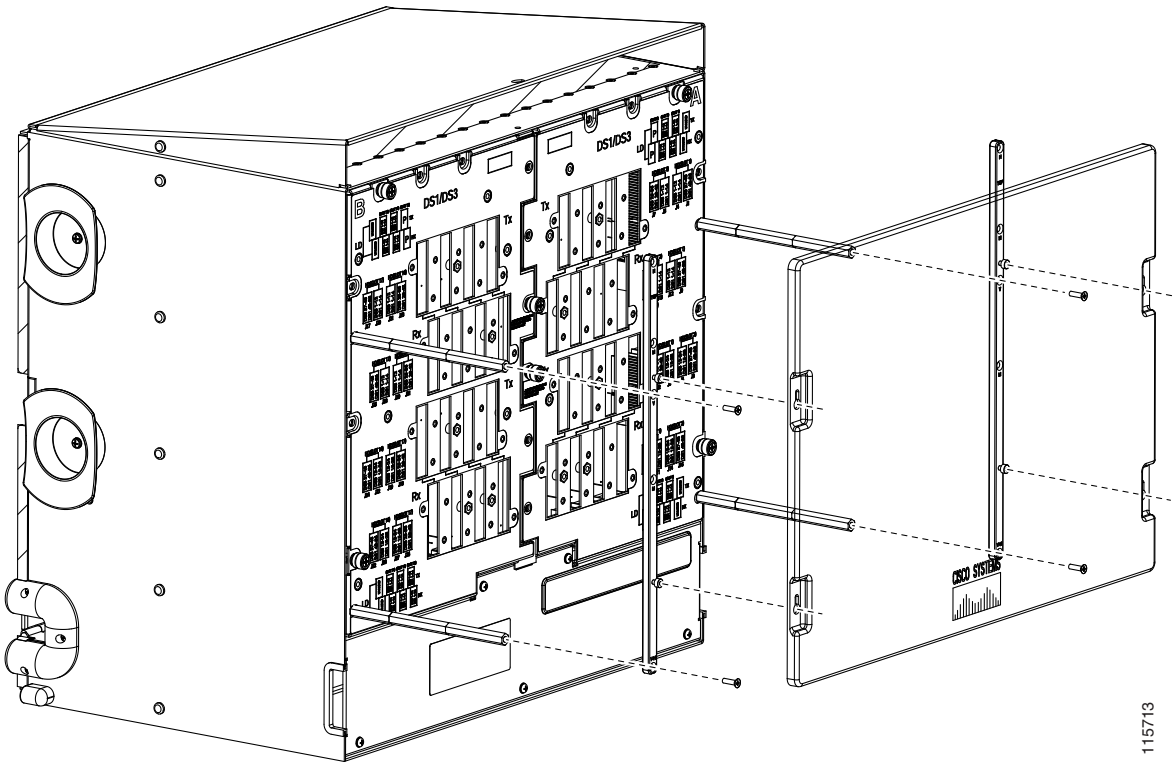


Figure 1-13 Installing the Rear Cover with Standoffs



Stop. You have completed this procedure.

NTP-A13 Perform the Shelf Installation Acceptance Test

Purpose	Use this procedure to perform a shelf installation acceptance test.
Tools/Equipment	Voltmeter
Prerequisite Procedures	Applicable procedures in Chapter 1
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **The covers are an integral part of the safety design of the product. Do not operate the unit without the covers installed.**

Step 1 Complete Table 1-5 by verifying that each applicable procedure was completed.

Table 1-5 Shelf Installation Task Summary

Description	Completed
NTP-A1 Unpack and Inspect the ONS 15454 Shelf Assembly, page 1-4	
NTP-A2 Install the Shelf Assembly, page 1-5	
NTP-A3 Open and Remove the Front Door, page 1-6	
NTP-A4 Remove the Backplane Covers, page 1-7	
NTP-A5 Install the EIAs, page 1-8	
NTP-A6 Install the Power and Ground, page 1-9	
NTP-A7 Install the Fan-Tray Assembly, page 1-11	
NTP-A119 Install the Alarm Expansion Panel, page 1-14	
NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-17	
NTP-A120 Install an External Wire-Wrap Panel to the AEP, page 1-18	
NTP-A9 Install the Electrical Card Cables on the Backplane, page 1-23	
NTP-A10 Route Electrical Cables, page 1-24	
NTP-A11 Install the Rear Cover, page 1-24	

Step 2 Complete the "DLP-A32 Inspect the Shelf Installation and Connections" task on page 17-36.

Step 3 Complete the "DLP-A33 Measure Voltage" task on page 17-36.

Step 4 Continue with Chapter 2, "Install Cards and Fiber-Optic Cable."

Stop. You have completed this procedure.

CHAPTER 2

Install Cards and Fiber-Optic Cable

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which maybe used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter explains how to install the Cisco ONS 15454 cards and fiber-optic cable.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A15 Install the Common Control Cards, page 2-2—Complete this procedure first before installing any other cards.
2. NTP-A16 Install Optical Cards and Connectors, page 2-8—Complete as needed.
3. NTP-A17 Install the Electrical Cards, page 2-11—Complete as needed.
4. NTP-A246 Install Ethernet Cards and Connectors, page 2-13—Complete as needed.
5. NTP-A274 Install the FC_MR-4 Card, page 2-15—Complete as needed.
6. NTP-A316 Install the Filler or Filler Plus Cards, page 2-17—Complete as needed.
7. NTP-A247 Install Fiber-Optic Cables, page 2-19—Complete this procedure to install fiber-optic cable on optical cards.
8. NTP-A245 Route Fiber-Optic Cables, page 2-22—Complete as needed.
9. NTP-A116 Remove and Replace a Card, page 2-23—Complete this procedure as needed to remove and replace a card, including deleting the card from Cisco Transport Controller (CTC) and changing an OC-N card without losing the card's provisioning.
10. NTP-A20 Replace the Front Door, page 2-24—If the front door was removed, complete this procedure to replace the front door and ground strap after installing cards and fiber-optic cable.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Filler cards serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards and faceplates are in place.** Statement 156

NTP-A15 Install the Common Control Cards

Purpose	This procedure describes how to install the common control cards.
Tools/Equipment	Redundant TCC2/TCC2P cards Redundant XCVT, XC10G, or XC-VXC-10G (cross-connect) cards AIC-I card (optional)
Prerequisite Procedures	NTP-A13 Perform the Shelf Installation Acceptance Test, page 1-31
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **During this procedure, wear grounding wrist straps to avoid electrostatic discharge (ESD) damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.** Statement 94

Warning **The intra-building ports of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 4) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.**

Warning **The intra-building ports of this card are suitable for connection only to shielded intra-building cabling grounded at both ends.**

Caution Always use the supplied ESD wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Caution If protective clips are installed on the backplane connectors of the cards, remove the clips before installing the cards.

Note If you install a card incorrectly, the FAIL LED flashes continuously.

Step 1 If you plan to install XCVT cards, review Table 2-1 to determine card/slot compatibility. If you plan to install XC10G or XC-VXC-10G cards, review Table 2-2 on page 2-5 to determine card/slot compatibility.

Step 2 Complete the "DLP-A36 Install the TCC2/TCC2P Cards" task on page 17-37.

Step 3 Complete the "DLP-A37 Install the XCVT, XC10G, or XC-VXC-10G Cards" task on page 17-40.

Step 4 Complete the "DLP-A41 Install the Alarm Interface Controller–International Card" task on page 17-42, as needed.

Note If you install the wrong card in a slot, see the "NTP-A116 Remove and Replace a Card" procedure on page 2-23.

Step 5 Install the traffic cards. To determine the appropriate procedure for a particular card, see the NTP list in the "Before You Begin" section on page 2-1.

In Table 2-1, X indicates that a card is supported in the slot. The multiservice (traffic) slots, Slots 1 to 6 and 12 to 17, include four slots (Slots 5, 6, 12, and 13) that have four times the bandwidth of the other multiservice slots.

Note The XC card is compatible with most cards but does not support features new to Release 5.0 and greater. See the *Cisco ONS 15454 Reference Manual* for more information about XC card compatibility.

Note For specific slot restrictions for a particular card, consult the card reference section for that card in the *Cisco ONS 15454 Reference Manual*.

Table 2-1 Card and Slot Compatibility for the XCVT Card

Slot	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Type	**MS**	**MS**	**MS**	**MS**	**MS**	**MS**	**TCC**	**XC**	**AIC-I**	**XC**	**TCC**	**MS**	**MS**	**MS**	**MS**	**MS**	**MS**
TCC2/TCC2P							X				X						
XCVT								X		X							
AIC-I									X								
DS1-14	X	X	X	X	X	X						X	X	X	X	X	X
DS1N-14[1]	X	X[3]	X	X[3]	X[3]	X[3]						X[3]	X[3]	X[3]	X	X[3]	X[3]
DS1/E1-56	X	X	X												X	X	X
DS3-12	X	X	X	X	X	X[2]						X[2]	X	X	X	X	X
DS3-12E	X	X	X	X	X	X[2]						X[2]	X	X	X	X	X
DS3N-12	X[3]	X[3]	X	X[3]	X[3]	X[3,2]						X[3,2]	X[3]	X[3]	X	X[3]	X[3]
DS3N-12E	X[3]	X[3]	X	X[3]	X[3]	X[3,2]						X[3,2]	X[3]	X[3]	X	X[3]	X[3]
DS3I-N-12[3]	X[3]	X[3]	X	X[3]	X[3]	X[3]						X[3]	X[3]	X[3]	X	X[3]	X[3]
DS3XM-6	X	X	X	X	X	X[2]						X[2]	X	X	X	X	X
DS3XM-12	X	X	X	X	X	X[2]						X[2]	X	X	X	X	X

Table 2-1 Card and Slot Compatibility for the XCVT Card (continued)

Slot	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Type	MS	MS	MS	MS	MS	MS	TCC	XC	AIC-I	XC	TCC	MS	MS	MS	MS	MS	MS
DS3/EC1-48	Not supported with XCVT cards. Requires XC10G or XC-VXC-10G cards.																
EC1-12	X	X	X	X	X	X[2]						X[6]	X	X	X	X	X
E100T-12	X	X	X	X	X	X						X	X	X	X	X	X
E1000-2	X	X	X	X	X	X						X	X	X	X	X	X
E100T-G	X	X	X	X	X	X						X	X	X	X	X	X
E1000-2-G	X	X	X	X	X	X						X	X	X	X	X	X
CE-100T-8	X	X	X	X	X	X						X	X	X	X	X	X
CE-1000-4					X	X						X	X				
CE-MR-10	X	X	X	X	X	X						X	X	X	X	X	X
G1K-4					X	X						X	X				
ML100-12					X	X						X	X				
ML1000-2					X	X						X	X				
ML100X-8	Not supported with XCVT cards. Requires XC10G or XC-VXC-10G cards.																
ML-MR-10	X	X	X	X	X	X						X	X	X	X	X	X
OC3 IR 4/STM1 SH 1310	X	X	X	X	X	X						X	X	X	X	X	X
OC3IR/STM1SH 1310-8	Not supported with XCVT cards. Requires XC10G or XC-VXC-10G cards.																
OC12 IR STM4 SH 1310	X	X	X	X	X	X						X	X	X	X	X	X
OC12 LR/STM4 LH 1310	X	X	X	X	X	X						X	X	X	X	X	X
OC12 LR/STM4 LH 1550	X	X	X	X	X	X						X	X	X	X	X	X
OC12 IR/STM4 SH 1310-4	Not supported with XCVT cards. Requires XC10G or XC-VXC-10G cards.																
OC48 LR 1550					X	X						X	X				
OC48 IR/STM16 SH AS 1310[4]					X	X						X	X				
OC48 LR/STM16 LH AS 1550[4]					X	X						X	X				
OC48-ELR/STM 16 EH 100 GHz					X	X						X	X				
OC48 ELR 200 GHz					X	X						X	X				
OC192 SR/STM64 IO 1310	Not supported with XCVT cards. Requires XC10G or XC-VXC-10G cards.																

Table 2-1 Card and Slot Compatibility for the XCVT Card (continued)

Slot	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Type	**MS**	**MS**	**MS**	**MS**	**MS**	**MS**	**TCC**	**XC**	**AIC-I**	**XC**	**TCC**	**MS**	**MS**	**MS**	**MS**	**MS**	**MS**
OC192 IR/STM64 SH 1550	Not supported with XCVT cards. Requires XC10G or XC-VXC-10G cards.																
OC192 LR/STM64 LH 1550	Not supported with XCVT cards. Requires XC10G or XC-VXC-10G cards.																
MRC-12	X	X	X	X	X	X						X	X	X	X	X	X
MRC-2.5G-4	X	X	X	X	X	X						X	X	X	X	X	X
OC192SR1/ STM64IO Short Reach and OC192/STM64 Any Reach (OC192-XFP cards)	Not supported with XCVT cards. Requires XC10G or XC-VXC-10G cards.																
FC_MR-4					X	X						X	X				
OC192 LR/STM64 LH ITU 15xx.xx	Not supported with XCVT cards. Requires XC10G or XC-VXC-10G cards.																

1. This identifies 1:N cards that operate as normal DS1 or DS3 cards when installed in certain slots.
2. This DS3 card cannot be used in this slot if used with a high-density electrical interface assembly (EIA) or in a 1:N configuration.
3. This card can only be used with the XCVT card, not the XC card.
4. The OC48AS will operate in Slots 5, 6, 12, and 13 with the XC/XCVT in R3.4 through R4.6, and the OC48AS will operate in Slots 5, 6, 12, and 13 with the XCVT in R5.0 and later. In Release R3.3 and earlier, OC48AS with XC/XCVT is not supported.

In Table 2-2, X indicates that a card is supported in the slot. The multiservice (traffic) slots, Slots 1 to 6 and 12 to 17, include four slots (Slots 5, 6, 12, and 13) that have four times the bandwidth of the other multiservice slots. The XC10G and XC-VXC-10G cards require the ANSI shelf (5454-SA-ANSI) or the high-density shelf (15454-SA-HD).

Note For specific slot restrictions for a particular card, consult the card reference section for that card in the *Cisco ONS 15454 Reference Manual*.

Table 2-2 Card and Slot Compatibility for the XC10G and XC-VXC-10G Cards

Slot	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Type	**MS**	**MS**	**MS**	**MS**	**MS**	**MS**	**TCC**	**XC**	**AIC-I**	**XC**	**TCC**	**MS**	**MS**	**MS**	**MS**	**MS**	**MS**
TCC2/TCC2P							X				X						
XC10G								X		X							
XC-VXC-10G								X		X							
AIC-I									X								

Table 2-2 Card and Slot Compatibility for the XC10G and XC-VXC-10G Cards (continued)

Slot	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Type	MS	MS	MS	MS	MS	MS	TCC	XC	AIC-I	XC	TCC	MS	MS	MS	MS	MS	MS
DS1-14	X	X	X	X	X	X						X	X	X	X	X	X
DS1N-14	X[1]	X[1]	X	X[1]	X[1]	X[1]						X[1]	X[1]	X[1]	X	X[1]	X[1]
DS1/E1-56	X	X	X												X	X	X
DS3-12	X	X	X	X	X	X						X	X	X	X	X	X
DS3-12E	X	X	X	X	X	X						X	X	X	X	X	X
DS3N-12	X[1]	X[1]	X	X[1]	X[1]	X[1]						X[1]	X[1]	X[1]	X	X[1]	X[1]
DS3N-12E	X[1]	X[1]	X	X[1]	X[1]	X[1]						X[1]	X[1]	X[1]	X	X[1]	X[1]
DS3XM-6	X	X	X	X	X	X						X	X	X	X	X	X
DS3XM-12	X	X	X	X	X	X						X	X	X	X	X	X
DS3/EC1-48	X	X	X												X	X	X
EC1-12	X	X	X	X	X	X						X	X	X	X	X	X
E100T-12	Not supported with the XC10G or XC-VXC-10G cards.																
E1000-2	Not supported with the XC10G or XC-VXC-10G cards.																
E100T-G	X	X	X	X	X	X						X	X	X	X	X	X
E1000-2-G	X	X	X	X	X	X						X	X	X	X	X	X
CE-100T-8	X	X	X	X	X	X						X	X	X	X	X	X
CE-1000-4	X	X	X	X	X	X						X	X	X	X	X	X
CE-MR-10	X	X	X	X	X	X						X	X	X	X	X	X
G1K-4	X	X	X	X	X	X						X	X	X	X	X	X
ML100-12	X	X	X	X	X	X						X	X	X	X	X	X
ML1000-2	X	X	X	X	X	X						X	X	X	X	X	X
ML100X-8	X	X	X	X	X	X						X	X	X	X	X	X
ML-MR-10	X	X	X	X	X	X						X	X	X	X	X	X
OC3 IR 4/STM1 SH 1310	X	X	X	X	X	X						X	X	X	X	X	X
OC3IR/STM1SH 1310-8	X	X	X	X										X	X	X	X
OC12 IR STM4 SH 1310	X	X	X	X	X	X						X	X	X	X	X	X
OC12 LR/STM4 LH 1310	X	X	X	X	X	X						X	X	X	X	X	X
OC12 IR/STM4 SH 1310-4	X	X	X	X										X	X	X	X
OC12 LR/STM4 LH 1550	X	X	X	X	X	X						X	X	X	X	X	X
OC48 LR 1550					X	X						X	X				

Table 2-2 Card and Slot Compatibility for the XC10G and XC-VXC-10G Cards (continued)

Slot	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Type	MS	MS	MS	MS	MS	MS	TCC	XC	AIC-I	XC	TCC	MS	MS	MS	MS	MS	MS
OC48 IR/STM16 SH AS 1310	X	X	X	X	X	X						X	X	X	X	X	X
OC48 LR/STM16 LH AS 1550	X	X	X	X	X	X						X	X	X	X	X	X
OC48-ELR/STM16 EH 100 GHz					X	X						X	X				
OC48 ELR 200 GHz					X	X						X	X				
OC192 SR/STM64 IO 1310					X	X						X	X				
OC192 IR/STM64 SH 1550					X	X						X	X				
OC192 LR/STM64 LH 1550					X	X						X	X				
OC192 LR/STM64 LH ITU 15xx.xx					X	X						X	X				
FC_MR-4	X	X	X	X	X	X						X	X	X	X	X	X
OC192SR1/ STM64IO Short Reach and OC192/STM64 Any Reach (OC192-XFP cards)					X	X						X	X				
MRC_12	X	X	X	X	X	X						X	X	X	X	X	X
MRC-2.5G-4	X	X	X	X	X	X						X	X	X	X	X	X

1. This identifies 1:N cards that operate as normal DS1 or DS3 cards when installed in certain slots.

Stop. You have completed this procedure.

NTP-A16 Install Optical Cards and Connectors

Purpose	This procedure describes how to install optical cards (OC-3, OC-12, OC-48, OC-192, MRC-12, and MRC-2.5G-4). The 15454_MRC-12 (multirate), MRC-2.5G-4, OC192SR1/STM64IO Short Reach, and OC192/STM64 Any Reach (known in CTC as OC192-XFP) cards require small form-factor pluggables (SFPs/XFPs) to provide the fiber interface to the cards. On all other optical cards, the fiber is plugged directly into the card. Install according to site plan, if available.
Tools/Equipment	OC-3, OC-12, OC-48, OC-192, MRC-2.5G-4, and MRC-12 cards (as applicable)
Prerequisite Procedures	NTP-A15 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.** Statement 94

Warning **Class I (CDRH) and Class 1M (IEC) laser products.** Statement 1055

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure.** Statement 1057

The following warning only applies to OC-192 cards with safety keys.

Warning **The laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

Caution Always use the supplied ESD wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Caution When TCC is rebooted after running the VxWorks command to delete database, perform the following steps:

1) I/O cards, OC3-8, OC12-4, OC48-AS (in low-speed slots),OC192, and MRC-12, need to be plugged out after running the VxWorks command to delete database and before rebooting TCC.

2) I/O cards, OC3-8, OC12-4, OC48-AS (in low-speed slots),OC192, and MRC-12, need to be plugged in after TCC comes to ACTIVE.

The above steps are applicable even in the power cycle of the NODE after running the VxWorks command to delete database on the TCC.

Note If protective clips are installed on the backplane connectors of the cards, remove the clips before installing the cards.

Note To simplify path protection to bidirectional line switched ring (BLSR) conversion and node addition, install optical cards according to a high-speed east (Slots 12 and 13) and west (Slots 5 and 6) configuration. This configuration is not mandatory.

Note During the boot process, an Out-of-Service (OOS) OC-N port will output a Line Alarm Indication Signal (AIS-L) to any In-Service (IS) far-end receivers. See the *Cisco ONS 15454 Troubleshooting Guide* for further information about the AIS-L condition.

Step 1 If you installed XCVT cards, review Table 2-1 on page 2-3 to determine card/slot compatibility. If you installed XC10G or XC-VXC-10G cards, review Table 2-2 on page 2-5 to determine card/slot compatibility.

Install higher-capacity cards first; for example, install an OC-192 card before installing an OC-48 card. Let each card completely boot before installing the next card.

Note "OC192SR1/STM64IO Short Reach" and "OC192/STM64 Any Reach" are the titles that appear on the faceplates of the OC192-XFP cards. In CTC, the cards are abbreviated as "OC192-XFP."

Before installing a MRC-12 card, review Table 2-3 for bandwidth limitations based on the slot where the card is installed and the type of cross-connect card installed in the shelf.

Table 2-3 Maximum Bandwidth by Shelf Slot for the MRC-12 in Different XC Configurations

XC Card Type	Maximum Bandwidth in Slots 1 through 4 and 12 through 17	Maximum Bandwidth in Slots 5, 6, 12, or 13
XCVT	OC-12	OC-48
XC10G/XC-VXC-10G	OC-48	OC-192

Before installing a MRC-2.5G-4 card, review Table 2-4 for bandwidth limitations based on the slot where the card is installed and the type of cross-connect card installed in the shelf.

Table 2-4 Maximum Bandwidth by Shelf Slot for the MRC-2.5G-4 in Different Cross-Connect Configurations

XC Card Type	Maximum Bandwidth in Slots 1 through 4 and 14 through 17	Maximum Bandwidth in Slots 5, 6, 12, or 13
XCVT	OC-12	OC-48
XC10G/XC-VXC-10G	OC-48	OC-48

Refer to the card's reference section in the "Optical Cards" chapter of the *Cisco ONS 15454 Reference Manual* for more information about slot and bandwidth restrictions.

Step 2 Open the card latches/ejectors.

Step 3 Use the latches/ejectors to firmly slide the optical card along the guide rails until the card plugs into the receptacle at the back of the slot. If you install a card incorrectly, the FAIL LED flashes continuously.

Note If you install the wrong card in a slot, complete the "NTP-A116 Remove and Replace a Card" procedure on page 2-23.

Step 4 Verify that the card is inserted correctly and close the latches/ejectors on the card. It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 5 Verify the LED activity:

- The red FAIL LED turns on for 20 to 30 seconds.
- The red FAIL LED blinks for 35 to 45 seconds.
- All LEDs blink once and turn off for 5 to 10 seconds.
- The ACT or ACT/STBY LED becomes amber. The signal fail (SF) LED can persist until all card ports connect to their far-end counterparts and a signal is present.

Step 6 If the card does not boot up properly, or the LED activity does not mimic Step 5, check the following:

- When a physical card type does not match the type of card provisioned for that slot in CTC, the card might not boot. If an optical card does not boot, open CTC and ensure that the slot is not provisioned for a different card type before assuming the card is faulty.
- If the red FAIL LED does not turn on, check the power.
- If you insert a card into a slot provisioned for a different card, all LEDs turn off.
- If the red FAIL LED is on continuously or the LEDs behave erratically, the card is not installed properly. Remove the card and repeat Steps 2 to 5.

Step 7 The MRC-12 card requires SFPs and the OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach (OC192-XFP) cards require XFPs to provide a fiber interface. If you installed any of these cards, complete the "DLP-A469 Install a GBIC or SFP/XFP Device" task on page 21-58. If you want to preprovision the SFPs or XFPs before installing them, complete the "DLP-A461 Preprovision an SFP or XFP Device" task on page 21-43.

Step 8 When you are ready to install fiber, continue with the "NTP-A247 Install Fiber-Optic Cables" procedure on page 2-19.

Stop. You have completed this procedure.

NTP-A17 Install the Electrical Cards

Purpose	This procedure describes how to install electrical cards (DS-1, DS-3, DS3XM, and EC-1).
Tools/Equipment	Electrical cards
Prerequisite Procedures	NTP-A15 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.** Statement 94

Warning **The intra-building ports of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 4) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.**

Warning **The intra-building ports of this card are suitable for connection only to shielded intra-building cabling grounded at both ends.**

Caution Always use the supplied ESD wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Caution Do not install low-density DS-1 cards in the same side of the shelf as DS3/EC1-48 cards.

Caution Do not install a DS3/EC1-48 card in Slots 1 or 2 if you have installed an MXP_2.5G_10G card in Slot 3. Likewise, do not install a DS3/EC1-48 in Slots 16 or 17 if you have installed an MXP_2.5G_10G card in Slot 15. If you do, the cards will interact and cause DS-3 bit errors.

Note When TCC is rebooted after running the VxWorks command to delete database, perform the following steps:

1. I/O card, DS3/EC1, need to be plugged out after running the VxWorks command to delete database and before rebooting TCC.
2. 2) I/O card, DS3/EC1, need to be plugged in after TCC comes to ACTIVE.

The above steps are applicable even in the power cycle of the NODE after running the VxWorks command to delete database on the TCC.

Note If protective clips are installed on the backplane connectors of the cards, remove the clips before installing the cards.

Note Install higher-capacity cards first; for example, install a DS-3 card before installing a DS-1 card. Let each card boot completely before installing the next card.

Note If you are installing OC-N, transponder (TXP), or muxponder (MXP) cards, Cisco recommends that you install these before you install electrical cards, as applicable.

Step 1 If you installed XC or XCVT cards, review Table 2-1 on page 2-3 to determine card/slot compatibility. If you installed XC10G or XC-VXC-10G cards, review Table 2-2 on page 2-5 to determine card/slot compatibility.

Step 2 Open the card latches/ejectors.

Step 3 Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot.

Note If you install the wrong card in a slot, complete the "NTP-A116 Remove and Replace a Card" procedure on page 2-23.

Step 4 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 5 Verify the LED activity:

- The red FAIL LED turns on for 10 to 15 seconds.
- The red FAIL LED blinks for 30 to 40 seconds.
- All LEDs blink once and turn off for 1 to 5 seconds.
- The ACT or ACT/STBY LED turns on. The SF LED can persist until all card ports connect to their far-end counterparts and a signal is present.

Step 6 If the card does not boot up properly, or the LED activity does not mimic Step 5, check the following:

- If the red FAIL LED does not turn on, check the power.
- If you insert a card into a slot provisioned for a different card, all LEDs turn off.
- If the red FAIL LED is on continuously or the LEDs behave erratically, the card is not installed properly. Remove the card and repeat Steps 2 to 5.

Step 7 Continue with the "NTP-A246 Install Ethernet Cards and Connectors" procedure on page 2-13, if necessary.

Stop. You have completed this procedure.

NTP-A246 Install Ethernet Cards and Connectors

Purpose	This procedure describes how to install the Ethernet cards (E100T-12, E100T-G, E1000-2, E1000-2-G, G1K-4, ML100T-12, ML1000-2, ML100X-8, ML-MR-10, CE-100T-8, CE-1000-4, and CE-MR-10).
Tools/Equipment	Ethernet cards
Prerequisite Procedures	NTP-A15 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.** Statement 94

Warning **Class I (CDRH) and Class 1M (IEC) laser products.** Statement 1055

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure.** Statement 1057

Warning **The intra-building ports of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 4) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.**

Warning **The intra-building ports of this card are suitable for connection only to shielded intra-building cabling grounded at both ends.**

Caution Always use the supplied ESD wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Note Ethernet interface on the ML-MR-10 Card needs to be shielded and grounded at both ends.

Note If protective clips are installed on the backplane connectors of the cards, remove the clips before installing the cards.

Note If you are installing OC-N, TXP, or MXP cards, Cisco recommends that you install these before you install Ethernet cards.

Step 1 If you installed XC or XCVT cards, review Table 2-1 on page 2-3 to determine card/slot compatibility. If you installed XC10G or XC-VXC-10G cards, review Table 2-2 on page 2-5 to determine card/slot compatibility.

Step 2 Complete the "DLP-A39 Install Ethernet Cards" task on page 17-41. Allow each card to boot completely before installing the next card.

Note If you install the wrong card in a slot, complete the "NTP-A116 Remove and Replace a Card" procedure on page 2-23.

Step 3 Complete the "DLP-A469 Install a GBIC or SFP/XFP Device" task on page 21-58 if you are using E1000-2, E1000-2-G, ML1000-2, ML100X-8, ML-MR-10, CE-1000-4, or CE-MR-10 cards.

Note If you need to remove a GBIC or SFP/XFP, complete the "DLP-A470 Remove GBIC or SFP/XFP Devices" task on page 21-60.

Step 4 Continue with the "NTP-A274 Install the FC_MR-4 Card" procedure on page 2-15 as needed.

Stop. You have completed this procedure.

NTP-A274 Install the FC_MR-4 Card

Purpose	This procedure installs the FC_MR-4 card, also known as the Fibre Channel card.
Tools/Equipment	FC_MR-4 card(s)
Prerequisite Procedures	NTP-A15 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.** Statement 94

Warning **Class I (CDRH) and Class 1M (IEC) laser products.** Statement 1055

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure.** Statement 1057

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Caution Always use the supplied ESD wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Note If protective clips are installed on the backplane connectors of the cards, remove the clips before installing the cards.

Step 1 If you installed XCVT cards, review Table 2-1 on page 2-3 to determine card/slot compatibility. If you installed XC10G or XC-VXC-10G cards, review Table 2-2 on page 2-5 to determine card/slot compatibility.

Step 2 Open the card latches/ejectors.

Step 3 Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot.

Note If you install the wrong card in a slot, complete the "NTP-A116 Remove and Replace a Card" procedure on page 2-23 and install the correct card.

Step 4 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 5 Verify the LED activity:

- The red FAIL LED turns on for 20 to 30 seconds. The ACT LED is amber for 3 to 5 seconds.
- The red FAIL LED blinks for up to 2 minutes.
- The FAIL and ACT LEDs blink once and turn off for 1 to 5 seconds.
- The ACT LED turns on green.

Note If the red FAIL LED does not turn on, check the power.

Note If you insert a card into a slot provisioned for a different card, all LEDs turn off.

Step 6 Complete the "DLP-A469 Install a GBIC or SFP/XFP Device" task on page 21-58 to install GBICs on the FC_MR-4 card.

Note If you need to remove a GBIC or SFP/XFP, complete the "DLP-A470 Remove GBIC or SFP/XFP Devices" task on page 21-60.

Step 7 Continue with the "NTP-A247 Install Fiber-Optic Cables" procedure on page 2-19.

Stop. You have completed this procedure.

NTP-A316 Install the Filler or Filler Plus Cards

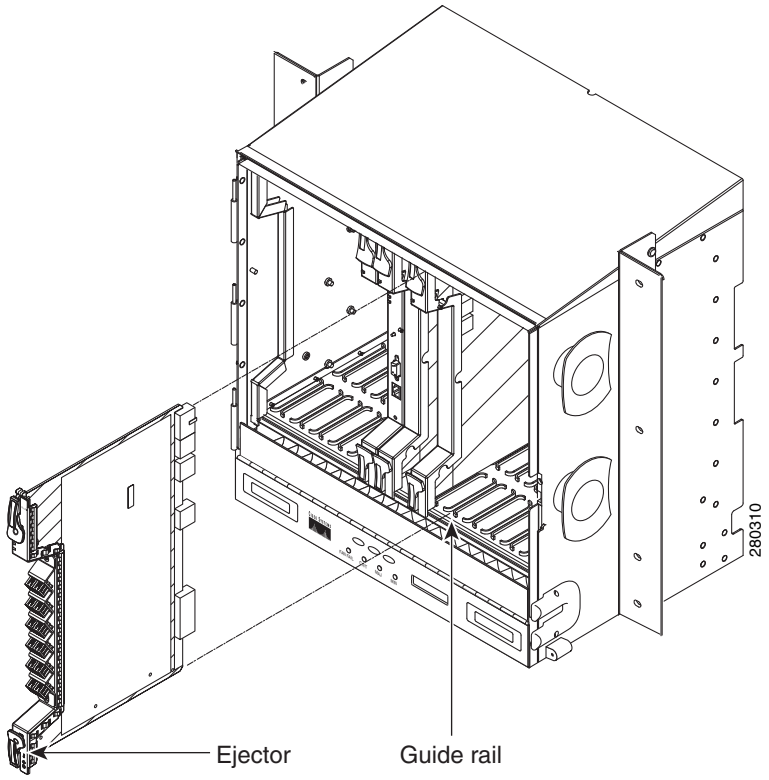
Purpose	This procedure explains how to install the filler or filler plus cards in any unused traffic or AIC-I card slots (Slots 1 through 6, 9, and 12 through 17). A filler or filler plus card consists of a card with a faceplate attached. **Note** There are two types of filler cards. One is not detectable by CTC and has no label on its faceplate. The other is detectable by CTC and has the label FILLER on its faceplate. Filler cards aid in maintaining proper air flow and electromagnetic interference (EMI) requirements.
Tools/Equipment	Filler cards Cisco P/N 15454-FILLER (detectable) Cisco P/N 15454-FILLER Plus (detectable) Cisco P/N 15454-BLANK (non-detectable)
Prerequisite Procedures	NTP-A15 Install the Common Control Cards, page 2-2 NTP-A16 Install Optical Cards and Connectors, page 2-8 NTP-A17 Install the Electrical Cards, page 2-11 NTP-A246 Install Ethernet Cards and Connectors, page 2-13 NTP-A274 Install the FC_MR-4 Card, page 2-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **Filler cards serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain EMI that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards and faceplates are in place.** Statement 156

Caution Always use the supplied ESD wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Figure 2-1 shows general card installation in an ONS 15454 SONET shelf.

Figure 2-1 Installing the Filler Plus Card in a ONS 15454 SONET Shelf



Step 1 Open the card ejectors.

Step 2 Slide the card along the guide rails into the correct slot.

Step 3 Close the ejectors.

Step 4 Repeat for any remaining unused card slots.

Step 5 When you log into CTC, verify that the detectable filler or filler plus card appears properly in CTC node view. A non-detectable filler card does not appear in CTC node view.

Stop. You have completed this procedure.

NTP-A247 Install Fiber-Optic Cables

Purpose	This procedure installs fiber-optic cables on optical cards according to topology. To attach fiber-optic cable to a GBIC, SFP, or XFP, see the "DLP-A469 Install a GBIC or SFP/XFP Device" task on page 21-58.
Tools/Equipment	Fiber-optic cables Fiber boot Fiber clips
Prerequisite Procedures	NTP-A16 Install Optical Cards and Connectors, page 2-8 NTP-A112 Clean Fiber Connectors, page 15-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **Class I (CDRH) and Class 1M (IEC) laser products.** Statement 1055

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure.** Statement 1057

The following warning only applies to OC-192 cards with safety keys.

Warning **The laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

Warning **Laser radiation presents an invisible hazard, so personnel should avoid exposure to the laser beam. Personnel must be qualified in laser safety procedures and must use proper eye protection before working on this equipment.** Statement 300

Caution To comply with the Telcordia GR-1089 NEBS, Issue 5 standard, do not use optical fibers with exposed metallic ferrules. Exposed metallic ferrules may result in ESD damage to the system and can be service affecting.

Caution Do not use fiber loopbacks with the OC192 LR/STM64 LH 1550 or OC192 LR/STM64 LH ITU 15xx.xx card unless you are using a 20-dB attentuator. Never connect a direct fiber loopback. Using fiber loopbacks causes irreparable damage to the OC192 LR/STM64 LH 1550 or OC192 LR/STM64 LH ITU 15xx.xx card.

Caution Do not use fiber loopbacks with the OC192 IR/STM64 SH 1550 card unless you are using a 5-dB attentuator. Never connect a direct, unattenuated fiber loopback. Using unattenuated fiber loopbacks causes irreparable damage to the OC192 IR/STM64 SH 1550 card.

Caution Always use the supplied ESD wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Note Fiber boots are not recommended for OC192 cards or OC48 AS cards because of the downward angle of the optical ports.

Note You can install the fiber-optic cable immediately after installing the cards, or wait until you are ready to turn up the network. See Chapter 5, "Turn Up a Network."

Step 1 Test the optical receive levels for the cards installed and attenuate accordingly. See Table 2-5 for the minimum and maximum levels.

Note The levels for the 15454_MRC-12, OC192SR1/STM64IO Short Reach, and OC192/STM64 Any Reach (OC192-XFP) cards are dependent on the particular SFP/XFP installed in a port. The SFPs/XFPs are shown in parentheses in Table 2-5 for these cards.

Table 2-5 Optical Card Transmit and Receive Levels

	Transmit		Receive	
Card	**Minimum**	**Maximum**	**Minimum**	**Maximum**
OC3 IR 4/STM1 SH 1310	–15 dBm	–8 dBm	–28 dBm	–8 dBm
OC3IR/STM1SH 1310-8	–15 dBm	–8 dBm	–28 dBm	–8 dBm
OC12 IR/STM4 SH 1310	–15 dBm	–8 dBm	–28 dBm	–8 dBm
OC12 LR/STM4 LH 1310	–3 dBm	+2 dBm	–28 dBm	–8 dBm
OC12 LR/STM4 LH 1550	–3 dBm	+2 dBm	–28 dBm	–8 dBm
OC12 IR/STM4 SH 1310-4	–15 dBm	–8 dBm	–30 dBm	–8 dBm
OC48 IR 1310	–5 dBm	0 dBm	–18 dBm	0 dBm
OC48 LR 1550	–2 dBm	+3 dBm	–28 dBm	–8 dBm

Table 2-5 Optical Card Transmit and Receive Levels (continued)

	Transmit		Receive	
Card	**Minimum**	**Maximum**	**Minimum**	**Maximum**
OC48 IR/STM16 SH AS 1310	–5 dBm	0 dBm	–18 dBm	0 dBm
OC48 LR/STM16 LH AS 1550	–2 dBm	+3 dBm	–28 dBm	–8 dBm
OC48 ELR/STM16 EH 100 GHz	–2 dBm	0 dBm	–27 dBm at 1E-12 BER	–9 dBm
OC48 ELR/STM16 EH 200 GHz	–2 dBm	0 dBm	–28 dBm	–8 dBm
OC192 SR/STM64 IO 1310	–6 dBm	–1 dBm	–11 dBm	–1 dBm
OC192 IR/STM64 SH 1550	–1 dBm	+2 dBm	–14 dBm	–1 dBm
OC192 LR/STM64 LH 1550	+7 dBm	+10 dBm	–19 dBm	–10 dBm
OC192 LR/STM64 LH ITU 15xx.xx	+3 dBm	+6 dBm	–22 dBm	–9 dBm
MRC-2.5G-4	–10 dBm	–3 dBm	–18 dBm	–3 dBm
15454_MRC-12 (ONS-SI-2G-S1)	–10 dBm	–3 dBm	–18 dBm	–3 dBm
15454_MRC-12 (ONS-SI-2G-I1)	–5 dBm	0 dBm	–18 dBm	0 dBm
15454_MRC-12 (ONS-SI-2G-L1)	–2 dBm	3 dBm	–27 dBm	–9 dBm
15454_MRC-12 (ONS-SI-2G-L2)	–2 dBm	3 dBm	–28 dBm	–9 dBm
15454_MRC-12 (ONS-SC-2G-30.3 through ONS-SC-2G-60.6)	0 dBm	4 dBm	–28 dBm	–9 dBm
15454_MRC-12 (ONS-SI-622-I1)	–15 dBm	–8 dBm	–28 dBm	–8 dBm
15454_MRC-12 (ONS-SI-622-L1)	–3 dBm	2 dBm	–28 dBm	–8 dBm
15454_MRC-12 (ONS-SI-622-L2)	–3 dBm	2 dBm	–28 dBm	–8 dBm
15454_MRC-12 (ONS-SE-622-1470 through ONS-SE-622-1610)	0 dBm	5 dBm	–28 dBm	–3 dBm
15454_MRC-12 (ONS-SI-155-I1)	–15 dBm	–8 dBm	–30 dBm	–8 dBm
15454_MRC-12 (ONS-SI-155-L1)	–5 dBm	0 dBm	–34 dBm	–10 dBm
15454_MRC-12 (ONS-SI-155-L2)	–5 dBm	0 dBm	–34 dBm	–10 dBm
15454_MRC-12 (ONS_SE-155-1470 through ONS-SE-155-1610)	0 dBm	5 dBm	–34 dBm	–3 dBm
15454_MRC_12 ONS-SI-155-I1-MM=	–9 dBm	–14 dBm	–14 dBm	–5 dBm
15454_MRC_12 ONS-SI-622-I1-MM=	–9 dBm	–14 dBm	–14 dBm	–5 dBm
15454_MRC_12 ONS-SC-Z3-1470 through ONS-SC-Z3-1610	0 dBm	5 dBm	–9 dBm	–5 dBm

Table 2-5 Optical Card Transmit and Receive Levels (continued)

Card	Transmit		Receive	
	Minimum	Maximum	Minimum	Maximum
15454_MRC_12 ONS-SE-Z1=	–5 dBm	0 dBm	–10 dBm 0 dBm –18 dBm 0 dBm 0 dBm	–23 dBm (OC-3) –23 dBm (OC-12) 0 dBm (OC-48) –21 dBm (FC) –22 dBm (GE)
OC192SR1/STM64IO Short Reach (ONS-XC-10G-S1)	–6 dBm	–1 dBm	–11 dBm	–1 dBm
OC192/STM64 Any Reach (ONS-XC-10G-S1)	–6 dBm	–1 dBm	–11 dBm	–1 dBm
OC192/STM64 Any Reach (ONS-XC-10G-I2)	–1 dBm	2 dBm	–14 dBm	2 dBm
OC192/STM64 Any Reach (ONS-XC-10G-L2)	0 dBm	4 dBm	–24 dBm	–7dBm

Step 2 As needed, complete the "DLP-A207 Install Fiber-Optic Cables on the LGX Interface" task on page 19-5.

Step 3 As needed, complete the "DLP-A428 Install Fiber-Optic Cables in a 1+1 Configuration" task on page 21-8.

Step 4 As needed, complete the "DLP-A43 Install Fiber-Optic Cables for Path Protection Configurations" task on page 17-43.

Step 5 As needed, complete the "DLP-A44 Install Fiber-Optic Cables for BLSR Configurations" task on page 17-46.

Step 6 Continue with the "NTP-A245 Route Fiber-Optic Cables" procedure on page 2-22.

Stop. You have completed this procedure.

NTP-A245 Route Fiber-Optic Cables

Purpose	This procedure describes how to route fiber-optic cables away from the ONS 15454 shelf, including installing fiber boots and fiber clips.
Tools/Equipment	None
Prerequisite Procedures	NTP-A247 Install Fiber-Optic Cables, page 2-19
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 As needed, complete the "DLP-A45 Install the Fiber Boot" task on page 17-48. Fiber boots are required for all OC-N cards except the OC-192,OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach (OC192-XFP), and OC-48 AS cards.

Step 2 Open the fold-down front door on the cable-management tray.

Step 3 Route the fiber-optic cable on the card faceplate through the fiber clip on the faceplate, if provided.

Step 4 If you installed a 15454_MRC-12 card, complete the "DLP-A443 Install the Fiber Clip on 15454_MRC-12 Cards" task on page 21-26. Fiber clips are factory-attached to the faceplate of optical cards except the 15454_MRC-12 cards. The 15454_MRC-12 cards are shipped with two versions of a fiber clip that plug into the faceplate.

Step 5 Route the fiber-optic cables into the cable-management tray.

Step 6 Route the fiber-optic cables out either side of the cable-management tray through the cutouts on each side of the shelf assembly. Use the reversible fiber guides to route cables out the desired side.

Step 7 Close the fold-down front door when all fiber-optic cables in the front compartment are properly routed.

Stop. You have completed this procedure.

NTP-A116 Remove and Replace a Card

Purpose	This procedure removes and replaces all cards housed in the ONS 15454 shelf and rack.
Tools/Equipment	None
Prerequisite Procedures	A card installation procedure
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 If you are not logged into CTC and you need to remove a card, remove the card as described in Step 3. When you log into CTC, troubleshoot the mismatched equipment alarm (MEA) with the *Cisco ONS 15454 Troubleshooting Guide*.

Step 2 If you are logged into CTC, complete one of the following:

- Complete the "DLP-A191 Delete a Card" task on page 18-64 and continue with Step 3.
- Complete the "DLP-A247 Change an OC-N Card" task on page 19-29 to delete a card and replace it with a different OC-N card while maintaining existing provisioning.

Step 3 Physically remove the card:

a. Open the card latches/ejectors.

b. Use the latches/ejectors to pull the card forward and away from the shelf.

Step 4 Insert the new card using one of the following procedures as applicable:

- NTP-A15 Install the Common Control Cards, page 2-2
- NTP-A16 Install Optical Cards and Connectors, page 2-8
- NTP-A17 Install the Electrical Cards, page 2-11
- NTP-A246 Install Ethernet Cards and Connectors, page 2-13
- NTP-A274 Install the FC_MR-4 Card, page 2-15

Step 5 As needed, continue with the "NTP-A247 Install Fiber-Optic Cables" procedure on page 2-19.

Stop. You have completed this procedure.

NTP-A20 Replace the Front Door

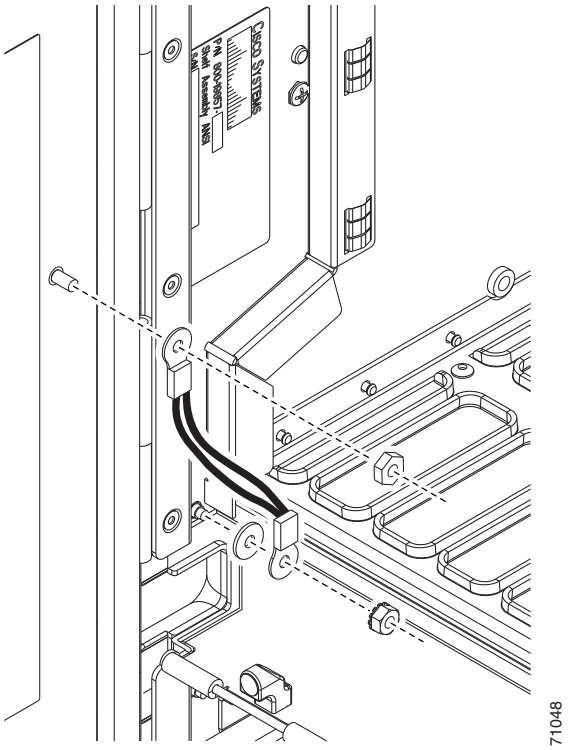
Purpose	This procedure replaces the front door and door ground strap after installing cards and fiber-optic cables.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	NTP-A3 Open and Remove the Front Door, page 1-6
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note Be careful not to crimp any fiber-optic cables that are connected to the optical cards. Some might not have the fiber boot attached.

Step 1 Insert the front door into the hinges on the shelf assembly.

Step 2 Attach one end of the ground strap terminal lug (72-3622-01) to the male stud on the inside of the door. Attach and tighten the #6 Kepnut (49-0600-01) using the open-end wrench (Figure 2-2).

Figure 2-2 Installing the Door Ground Strap Retrofit Kit



Step 3 Attach the other end of the ground strap to the longer screw on the fiber guide.

a. Attach the lock washer.

b. Attach the terminal lug.

c. Using the open-end wrench, attach and tighten the #4 Kepnut (49-0337-01) on the terminal lug.

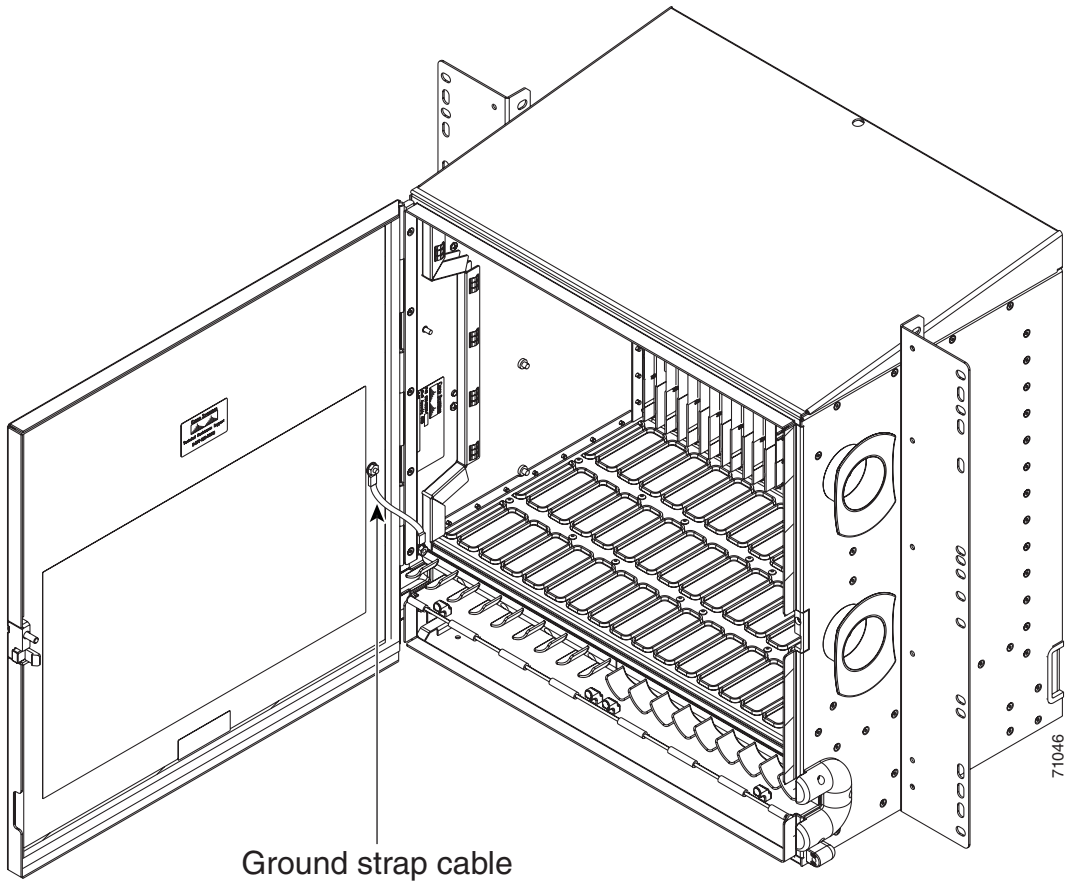
Note To avoid interference with the traffic (line) card, make sure the ground strap is in a flat position when the door is open. To move the ground strap into a flat position, rotate the terminal lug counterclockwise before tightening the Kepnut.

Step 4 Replace the left cable-routing channel.

Step 5 Using a Phillips screwdriver, insert and tighten the screws for the cable-routing channel.

Figure 2-3 shows the shelf assembly with the front door and ground strap installed.

Figure 2-3 Shelf Assembly with Door Ground Strap Retrofit Kit Installed



Step 6 Swing the door closed.

Note The ONS 15454 comes with a pinned hex key tool for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.

Stop. You have completed this procedure.

CHAPTER 3

Connect the PC and Log into the GUI

This chapter explains how to connect PCs and workstations to the Cisco ONS 15454 and how to log into Cisco Transport Controller (CTC) software, which is the ONS 15454 Operation, Administration, Maintenance and Provisioning (OAM&P) user interface. Procedures for connecting to the ONS 15454 using Transaction Language One (TL1) are provided in the *Cisco ONS SONET TL1 Reference Guide*.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A260 Set Up Computer for CTC, page 3-1—Complete this procedure if your PC or workstation has never been connected to an ONS 15454.
2. NTP-A234 Set Up CTC Computer for Local Craft Connection to the ONS 15454, page 3-3—Complete this procedure to set up your computer for an onsite craft connection to the ONS 15454.
3. NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454, page 3-5—Complete this procedure to set up your computer to connect to the ONS 15454 using a corporate LAN.
4. NTP-A236 Set Up a Remote Access Connection to the ONS 15454, page 3-6—Complete this procedure to set up your computer for remote modem access to the ONS 15454.
5. NTP-A23 Log into the ONS 15454 GUI, page 3-7—Complete this procedure to log into CTC.
6. NTP-A353 Use the CTC Launcher Application to Manage Multiple ONS Nodes, page 3-8—Complete this procedure to use the CTC launcher application.

NTP-A260 Set Up Computer for CTC

Purpose	This procedure configures your PC or UNIX workstation to run CTC.
Tools/Equipment	Cisco ONS 15454 Release 9.1, 9.2, or 9.2.1 software CD
Prerequisite Procedures	Chapter 1, “Install the Shelf and Backplane Cable”
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	None

Note JRE 5.0 is required to log into nodes running Software Release 8.5 and above (JRE 1.6 for Release 9.2 and later). To log into nodes running Release 4.5 or earlier, you must uninstall JRE 1.4.2 or 5.0 (JRE 1.6 for Release 9.2 and later) and install JRE 1.3.1_2. Complete the "DLP-A431 Change the JRE Version" task on page 21-9 as necessary.

Step 1 If your computer does not have an appropriate browser installed, complete the following:

- Download the supported browser from the Web:
  - Netscape 7.x
  - Mozilla 1.7 on a UNIX workstation
  - Internet Explorer 6.x on a PC (Internet Explorer 7.x or 8.x for Release 9.2 and later)
  - Safari for a Mac OS-X PC
- Choose Tools->options->security, uncheck Remember password for sites in the Mozilla Firefox browser.

Note Internet Explorer does not support IPv6 addressing. You can either use Netscape or Mozilla Firefox browser. The Mozilla Firefox browser is required to the access IPv6 addressing through CTC sessions from Windows or Linux machines.

Step 2 Complete the "DLP-A552 Adjust the Java Virtual Memory Heap Size" task on page 22-58 to increase the size of the JVM heap in order to improve the CTC performance.

Step 3 If your computer is a Windows PC, complete the "DLP-A337 Run the CTC Installation Wizard for Windows" task on page 20-25, then go to Step 5.

Step 4 If your computer is a UNIX workstation, complete the "DLP-A338 Run the CTC Installation Wizard for UNIX" task on page 20-28.

Step 5 When your PC or workstation is set up, continue with the setup procedure appropriate to your network:

- NTP-A234 Set Up CTC Computer for Local Craft Connection to the ONS 15454, page 3-3
- NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454, page 3-5
- NTP-A236 Set Up a Remote Access Connection to the ONS 15454, page 3-6

Note Cisco recommends that you configure your browser to disable the caching of user IDs/passwords on computers used to access Cisco optical equipment.

In Internet Explorer, choose **Tools > Internet Options > Content**. Click **Auto Complete** and uncheck the **User names and passwords on forms** option.

In Netscape 7.0, choose **Edit > Preferences > Privacy & Security > Forms** and uncheck the option to save form data. For passwords, choose **Edit > Preferences > Privacy & Security > Passwords** and uncheck the option to remember passwords. Note that passwords can be stored in an encrypted format. Netscape versions earlier than 6.0 do not cache user IDs and passwords.

In Mozilla Firefox browser, choose **Tools->options->security**, uncheck 'Remember password for sites'

Stop. You have completed this procedure.

NTP-A234 Set Up CTC Computer for Local Craft Connection to the ONS 15454

Purpose	This procedure explains how to set up a PC running Windows or a Solaris workstation for an onsite local craft connection to the ONS 15454.
Tools/Equipment	Network interface card (NIC), also referred to as an Ethernet card Straight-through (CAT 5) LAN cable
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Complete one of the CTC computer setup tasks shown in Table 3-1 based your CTC connection environment.

Table 3-1 CTC Computer Setup for Local Craft Connections to the ONS 15454

CTC Connection Environment	CTC Computer Setup Task
• You are connecting from a Windows PC. • All nodes that you will access run software earlier than Release 3.3. • You will connect to one ONS 15454. • You need to access non-ONS 15454 applications such as ping and tracert (trace route).	DLP-A50 Set Up a Windows PC for Craft Connection to an ONS 15454 on the Same Subnet Using Static IP Addresses, page 17-50
• You are connecting from a Windows PC. • The CTC computer is provisioned for Dynamic Host Configuration Protocol (DHCP). • The ONS 15454 has DHCP forwarding enabled. • The ONS 15454 is connected to a DHCP server. **Note** The ONS 15454 does not provide IP addresses. If DHCP is enabled, it passes DCHP requests to an external DHCP server.	DLP-A51 Set Up a Windows PC for Craft Connection to an ONS 15454 Using Dynamic Host Configuration Protocol, page 17-52 **Note** Do not use this task for initial node turn-up. Use the task only if DHCP forwarding is enabled on the ONS 15454. By default, DHCP is not enabled. To enable it, see the "NTP-A169 Set Up CTC Network Access" procedure on page 4-8.

Table 3-1 CTC Computer Setup for Local Craft Connections to the ONS 15454 (continued)

CTC Connection Environment	CTC Computer Setup Task
• You are connecting from a Windows PC. • All nodes that you will access run software Release 3.3 or later. • You will connect to ONS 15454s at different locations and times and do not wish to reconfigure your PC's IP settings each time. • You will not access or use non-ONS 15454 applications such as ping and tracert (trace route). • You will connect to the ONS 15454 TCC2/TCC2P Ethernet port or backplane LAN pins either directly or through a hub.	DLP-A52 Set Up a Windows PC for Craft Connection to an ONS 15454 Using Automatic Host Detection, page 17-54
• You are connecting from a Solaris workstation. • You will connect to one ONS 15454. • You need to access non-ONS 15454 applications such as ping and traceroute.	DLP-A565 Set Up a Solaris Workstation for a Craft Connection to an ONS 15454, page 22-79

Step 2 Connect a straight-through (CAT-5) LAN cable from the PC or Solaris workstation NIC to one of the following:

- RJ-45 (LAN) port on the active or standby TCC2/TCC2P card
- RJ-45 (LAN) port on a hub or switch to which the ONS 15454 is physically connected

Note For instructions on crimping your own straight-through (CAT-5) LAN cables, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Note For initial shelf turn-up, you should connect your PC directly to the LAN port on the TCC2/TCC2P card of the ONS 15454.

Step 3 After setting up your CTC computer, continue with the "NTP-A23 Log into the ONS 15454 GUI" procedure on page 3-7, if applicable.

Stop. You have completed this procedure.

NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454

Purpose	This procedure sets up your computer to access the ONS 15454 through a corporate LAN.
Tools/Equipment	Network interface card (NIC), also referred to as an Ethernet card Straight-through (CAT 5) LAN cable
Prerequisite Procedures	• NTP-A260 Set Up Computer for CTC, page 3-1 • The ONS 15454 must be provisioned for LAN connectivity, including IP address, subnet mask, default gateway. • The ONS 15454 must be physically connected to the corporate LAN. • The CTC computer must be connected to the corporate LAN that has connectivity to the ONS 15454.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 If your computer is already connected to the corporate LAN, go to Step 3. If you changed your computer's network settings for craft access to the ONS 15454, change the settings back to the corporate LAN access settings. This generally means:

- Set the IP Address on the TCP/IP dialog box back to **Obtain an IP address automatically** (Windows 98) or **Obtain an IP address from a DHCP server** (Windows NT 4.0, 2000, or XP).
- If your LAN requires that Domain Name System (DNS) or Windows Internet Naming Service (WINS) be enabled, change the setting on the DNS Configuration or WINS Configuration tab of the TCP/IP dialog box.

Step 2 Connect a straight-through (CAT-5) LAN cable from the PC or Solaris workstation NIC card to a corporate LAN port.

Step 3 If your computer is connected to a proxy server, disable proxy service or add the ONS 15454 nodes as exceptions. To disable proxy service, complete one of the following tasks, depending on the web browser that you use:

- DLP-A56 Disable Proxy Service Using Internet Explorer (Windows), page 17-57
- DLP-A57 Disable Proxy Service Using Netscape (Windows and UNIX), page 17-58
- DLP-A598 Disable Proxy Service Using Mozilla Firefox (Windows and UNIX), page 17-59

Step 4 Continue with the "NTP-A23 Log into the ONS 15454 GUI" procedure on page 3-7.

Stop. You have completed this procedure.

NTP-A236 Set Up a Remote Access Connection to the ONS 15454

Purpose	This procedure connects the CTC computer to an ONS 15454 using a LAN modem.
Tools/Equipment	Modem and modem documentation
Prerequisite Procedures	• NTP-A260 Set Up Computer for CTC, page 3-1 • A modem must be connected to the ONS 15454 • The modem must be provisioned for ONS 15454. To run CTC, the modem must be provisioned for Ethernet access.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Connect the modem to the RJ-45 (LAN) port on the TCC2/TCC2P card or to the LAN pins on the ONS 15454 backplane.

Step 2 While referring to the modem documentation, complete the following tasks to provision the modem for the ONS 15454:

- For CTC access, set the modem for Ethernet access.
- Assign an IP address to the modem that is on the same subnet as the ONS 15454.
- The IP address the modem assigns to the CTC computer must be on the same subnet as the modem and the ONS 15454.

Note For assistance on provisioning specific modems, contact the Cisco Technical Assistance Center (Cisco TAC). See the "Obtaining Documentation and Submitting a Service Request" section on page lxiv for more information.

Step 3 Continue with the "NTP-A23 Log into the ONS 15454 GUI" procedure on page 3-7.

Stop. You have completed this procedure.

NTP-A23 Log into the ONS 15454 GUI

Purpose	This procedure logs into CTC, the graphical user interface software used to manage the ONS 15454. This procedure includes optional node login tasks.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1 One of the following procedures: • NTP-A234 Set Up CTC Computer for Local Craft Connection to the ONS 15454, page 3-3 • NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454, page 3-5 • NTP-A236 Set Up a Remote Access Connection to the ONS 15454, page 3-6
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60.

Note For information about navigating in CTC, see Appendix A, "CTC Information and Shortcuts."

During network topology discovery, CTC polls each node in the network to determine which one contains the most recent version of the CTC software. If CTC discovers a node in the network that has a more recent version of the CTC software than the version you are currently running, CTC generates a message stating that a later version of CTC has been found in the network, and offers to install the CTC software upgrade. If you have network discovery disabled, CTC will not seek more recent versions of the software. Unreachable nodes are not included in the upgrade discovery.

Note Upgrading the CTC software will overwrite your existing software. You must restart CTC after the upgrade is complete.

Step 2 As needed, complete the "DLP-A61 Create Login Node Groups" task on page 17-63. Login node groups allow you to manage nodes that are not connected to the login node through data communication channels (DCC).

Step 3 As needed, complete the "DLP-A62 Add a Node to the Current Session or Login Group" task on page 17-64.

Step 4 As needed, complete the "DLP-A339 Delete a Node from the Current Session or Login Group" task on page 20-31.

Step 5 As needed, complete the "DLP-A372 Delete a Node from a Specified Login Node Group" task on page 20-56.

Step 6 As needed, complete the "DLP-A327 Configure the CTC Alerts Dialog Box for Automatic Popup" task on page 20-16.

Stop. You have completed this procedure.

NTP-A353 Use the CTC Launcher Application to Manage Multiple ONS Nodes

Purpose	This procedure uses the CTC Launcher to start a CTC session with an ONS NE that has an IP connection to the CTC computer; create TL1 tunnels to connect to ONS NEs on the other side of third-party, OSI-based GNEs; and view, manage, and delete TL1 tunnels using CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1 One of the following procedures: • NTP-A234 Set Up CTC Computer for Local Craft Connection to the ONS 15454, page 3-3 • NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note JRE 5.0 (JRE 1.6 for Release 9.2 and later) must be installed on the PC you are using with the CTC Launcher application.

Step 1 As needed, complete one of the following tasks to install the CTC Launcher:

- DLP-A566 Install the CTC Launcher Application from a Release 9.1, 9.2, or 9.2.1 Software CD, page 22-80
- DLP-A567 Install the CTC Launcher Application from a Release 9.1, 9.2, or 9.2.1 Node, page 22-81

Step 2 As needed, complete the "DLP-A568 Connect to ONS Nodes Using the CTC Launcher" task on page 22-81 to connect to an ONS network element with direct IP connectivity.

Step 3 As needed, complete the "DLP-A559 Install or Reinstall the CTC JAR Files" task on page 22-73 to install or reinstall the CTC JAR files.

Step 4 As needed, complete one of the following tasks to create a TL1 tunnel, which enables you to connect to an ONS network element residing behind OSI-based, third-party GNEs:

- DLP-A569 Create a TL1 Tunnel Using the CTC Launcher, page 22-83
- DLP-A570 Create a TL1 Tunnel Using CTC, page 22-84

Step 5 As needed, complete the "DLP-A571 View TL1 Tunnel Information" task on page 22-85.

Step 6 As needed, complete the "DLP-A572 Edit a TL1 Tunnel Using CTC" task on page 22-86.

Step 7 As needed, complete the "DLP-A573 Delete a TL1 Tunnel Using CTC" task on page 22-87.

Stop. You have completed this procedure.

CHAPTER 4

Turn Up a Node

This chapter explains how to provision a single Cisco ONS 15454 node and turn it up for service, including assigning a node name, date and time, timing references, network attributes such as IP address and default router, users and user security, and card protection groups.

Before You Begin

Complete the procedures applicable to your site plan from the following chapters:

- Chapter 1, “Install the Shelf and Backplane Cable”
- Chapter 2, “Install Cards and Fiber-Optic Cable”
- Chapter 3, “Connect the PC and Log into the GUI”

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A323 Verify Card Installation, page 4-2—Complete this procedure first.
2. NTP-A30 Create Users and Assign Security, page 4-4—Complete this procedure to create Cisco Transport Controller (CTC) users and assign their security levels.
3. NTP-A25 Set Up Name, Date, Time, and Contact Information, page 4-5—Continue with this procedure to set the node name, date, time, location, and contact information.
4. NTP-A261 Set Power Monitor Thresholds, page 4-7—Continue with this procedure to set the node battery power thresholds.
5. NTP-A169 Set Up CTC Network Access, page 4-8—Continue with this procedure to provision the IP address, default router, subnet mask, and network configuration settings.
6. NTP-A358 Set up the ONS 15454 in Secure Mode, page 4-9—Continue with this procedure to connect the CTC in secure mode.
7. NTP-A360 Enable EMS Secure Access, page 4-9—Continue with this procedure to enable EMS secure access and provide enhanced SFTP and SSH security.
8. NTP-A375 Set Up Secure Access to the ONS 15454 TL1, page 4-10—Continue with this procedure to enable secure access to TL1.
9. NTP-A27 Set Up the ONS 15454 for Firewall Access, page 4-10—Continue with this procedure if the ONS 15454 will be accessed behind firewalls.
10. NTP-A355 Create FTP Host, page 4-12—Continue with this procedure if to create FTP host for ENE database backup.

11. NTP-A28 Set Up Timing, page 4-13—Continue with this procedure to set up the node's SONET timing references.
12. NTP-A324 Create Protection Groups, page 4-13—Complete this procedure, as needed, to set up 1:1, 1:N, 1+1, or Y-cable protection groups for ONS 15454 electrical and optical cards.
13. NTP-A256 Set Up SNMP, page 4-16—Complete this procedure if Simple Network Management Protocol (SNMP) will be used for network monitoring.
14. NTP-A364 Provision Node for SNMPv3, page 4-18—Complete this procedure if Simple Network Management Protocol Version 3 (SNMPv3) will be used for network monitoring.
15. NTP-A318 Provision OSI, page 4-17—Complete this procedure if the ONS 15454 will be connected in networks with network elements (NEs) that are based on the Open System Interconnection (OSI) protocol stack. This procedure provisions the TID Address Resolution Protocol (TARP), OSI routers, manual area addresses, subnetwork points of attachment, and IP over OSI tunnels.

NTP-A323 Verify Card Installation

Purpose	This procedure verifies that an ONS 15454 node provisioned for SONET is ready for turn-up.
Tools/Equipment	An engineering work order, site plan, or other document specifying the ONS 15454 card installation.
Prerequisite Procedures	Chapter 1, "Install the Shelf and Backplane Cable" Chapter 2, "Install Cards and Fiber-Optic Cable"
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Verify that two TCC2/TCC2P cards are installed in Slots 7 and 11.

Step 2 Verify that the green ACT (active) LED is illuminated on one TCC2/TCC2P card and the amber STBY (standby) LED is illuminated on the second TCC2/TCC2P card.

Note If the TCC2/TCC2P cards are not installed, or if their LEDs are not operating as described, do not proceed. Repeat the "DLP-A36 Install the TCC2/TCC2P Cards" task on page 17-37, or refer to the *Cisco ONS 15454 Troubleshooting Guide* to resolve installation problems before proceeding to Step 3.

Step 3 Verify that cross-connect cards (XCVT, XC10G, or XC-VXC-10G) are installed in Slots 8 and 10. The cross-connect cards must be the same type.

Step 4 Verify that the green ACT (active) LED is illuminated on one cross-connect card and the amber STBY (standby) LED is illuminated on the second cross-connect card.

Note If the cross-connect cards are not installed, or if their LEDs are not operating as described, do not proceed. Repeat the "DLP-A37 Install the XCVT, XC10G, or XC-VXC-10G Cards" task on page 17-40, or refer to the *Cisco ONS 15454 Troubleshooting Guide* to resolve installation problems before proceeding to Step 5.

Step 5 If your site plan requires an AIC-I card, verify that it is installed in Slot 9 and its ACT (active) LED displays a solid green light.

Step 6 Verify that the DS-1, DS-3, EC-1, and DS3XM cards are installed in Slots 1 to 6 or 12 to 17 as designated by your installation plan.

Note The DS1/E1-56 and DS3/EC1-48 cards can only be installed in Slots 1 through 3 or 15 through 17.

Step 7 If Ethernet cards are installed, verify that the correct cross-connect cards are installed in Slots 8 and 10:

- E100T-12-G and E1000-2-G cards require XC10G or XC-VXC-10G cards.
- G1K-4, ML1000-2, ML100X-8, ML100T-12, and CE-1000-4 cards require XC10G or XC-VXC-10G cards if they are installed in Slots 1 to 6 or 12 to 17. If they are installed in Slots 5, 6, 11 and 12, any cross-connect card can be installed.
- ML-MR-10 cards require XC10G or XC-VXC-10G cards. The ML-MR-10 card is not compatible with the XCVT or XC card.
- CE-MR-10 cards can be installed in Slots 1 to 6 or 12 to 17, and can interoperate with any cross-connect card.

Step 8 If an E1000-2, E1000-2-G, G1K-4, ML100X-8, ML1000-2, CE-1000-4, CE-MR-10, or ML-MR-10 Ethernet card is installed, verify that it has a Gigabit Interface Converter (GBIC) or Small Form-Factor Pluggable (SFP) installed. If not, see the "DLP-A469 Install a GBIC or SFP/XFP Device" task on page 21-58.

Step 9 Verify that the OC-N cards (OC-3, OC-3-8, OC-12, OC-12-4, OC-48, OC-48 any slot [AS], OC-192, MRC-2.5G-4, and MRC-12) are installed in the slots designated by your site plan.

- OC-3, OC-12, OC-48 AS, MRC-2.5G-4, and MRC-12 cards can be installed in Slots 1 to 6 or 12 to 17.
- OC-3-8 and OC-12-4 cards can be installed in Slots 1 to 4 and 14 to 17.
- OC-192 cards can be installed in Slots 5, 6, 12, or 13.

Step 10 Verify that the correct cross-connect cards are installed in Slots 8 and 10:

- If an OC-192, OC-12-4, or OC-3-8 card is installed, an XC10G card must be installed.
- If an OC-48 AS card is installed in Slots 1 to 4 or 14 to 17, an XC10G card must be installed. If XC or XCVT cards are installed, the OC-48 AS can be installed only in Slots 5, 6, 12, or 13.

Step 11 Verify that all installed OC-N cards display a solid amber STBY LED.

Step 12 If transponder or muxponder cards are installed (TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_MR_2.5G, MXPP_MR_2.5G, MXP_2.5G_10G, TXP_MR_10E, TXP_MR_10E_L, TXP_MR_10E_C, MXP_2.5G_10E, MXP_2.5G_10E_C, MXP_2.5G_10E_L, MXP_MR_10DME_L, MXP_MR_10DME_C, ADM-10G, GE_XP, and 10GE_XP), verify that they are installed in Slots 1 to 6 or 12 to 17 and have GBIC or SFP connectors installed. For information about installing and provisioning TXP and MXP cards, refer to the *Cisco ONS 15454 DWDM Procedure Guide*.

Step 13 If Fibre Channel cards (FC-MR-4) are installed, verify one of the following:

- If XC10G cross-connect cards are installed, the FC-MR-4 is installed in Slots 1 to 6 or 12 to 17 and displays a solid green ACT (Active) LED.
- If XCVT cross-connect cards are installed, the FC-MR-4 is installed in Slots 5 to 6 or 12 to 13 and displays a solid green ACT (Active) LED.

Step 14 Verify that fiber-optic cables (fiber) are installed and connected to the locations indicated in the site plan. If the fiber is not installed, complete the "NTP-A247 Install Fiber-Optic Cables" procedure on page 2-19.

Step 15 Verify that fiber is routed correctly in the shelf assembly and fiber boots are installed properly. If the fiber is not routed on the shelf assembly, complete the "NTP-A245 Route Fiber-Optic Cables" procedure on page 2-22. If the fiber boots are not installed, complete the "DLP-A45 Install the Fiber Boot" task on page 17-48.

Step 16 Verify that the software release shown on the LCD matches the software release indicated in your site plan. If the release does not match, perform one of the following procedures:

- Perform a software upgrade using a Cisco ONS 15454 software CD. Refer to the release-specific software upgrade document for instructions.
- Replace the TCC2/TCC2P cards with cards containing the correct release. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Stop. **You have completed this procedure**.

NTP-A30 Create Users and Assign Security

Purpose	This procedure creates ONS 15454 users and assigns their security levels.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you need to create users. If you are already logged in, continue with Step 2.

Note You must log in as a Superuser to create additional users. The CISCO15 user provided with each ONS 15454 can be used to set up other ONS 15454 users. You can add up to 500 users to one ONS 15454.

Step 2 Complete the "DLP-A74 Create a New User on a Single Node" task on page 17-77 or the "DLP-A75 Create a New User on Multiple Nodes" task on page 17-78 as needed.

Note You must add the same user name and password to each node a user will access.

Step 3 As needed, complete the "DLP-A456 Configure the Node for RADIUS Authentication" task on page 21-37. Remote Authentication Dial in User Service (RADIUS) validates remote users trying to connect to the network.

Step 4 If you want to modify the security policy settings, including password aging and idle user timeout policies, complete the "NTP-A205 Modify Users and Change Security" procedure on page 11-7.

Stop. **You have completed this procedure**.

NTP-A25 Set Up Name, Date, Time, and Contact Information

Purpose	This procedure provisions identification information for the node, including the node name, a contact name and phone number, the location of the node, and the date, time, and time zone.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 for the node you will turn up. If you are already logged in, continue with Step 2.

Step 2 Click the **Provisioning > General** tabs.

Step 3 Enter the following information in the fields listed:

- Node Name/TID—Type a name for the node. For Transaction Language 1 (TL1) compliance, names must begin with an alpha character and have no more than 20 alphanumeric (a-z, A-Z, 0-9) characters.
- Contact—(Optional) Type the name of the node contact person and the phone number, up to 255 characters.
- Latitude—Enter the node latitude: N (North) or S (South), degrees, and minutes (optional).
- Longitude—Enter the node longitude: E (East) or W (West), degrees, and minutes (optional).

Tip You can drag and drop the node icon on the network view map to position nodes manually. To create the same network map visible for all ONS 15454 users, complete the "NTP-A172 Create a Logical Network Map" procedure on page 5-40.

Note The latitude and longitude values only indicate the geographical position of the nodes in the actual network and not the CTC node position.

- Description—Type a description of the node. The description can be a maximum of 255 characters.
- Use NTP/SNTP Server—When checked, CTC uses a Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) server to set the date and time of the node.

  If you do not use an SNTP or NTP server, complete the Date and Time fields. The ONS 15454 will use these fields for alarm dates and times. By default, CTC displays all alarms in the CTC computer time zone for consistency. To change the display to the node time zone, complete the "DLP-A112 Display Alarms and Conditions Using Time Zone" task on page 18-2.

Note Using an NTP or SNTP server ensures that all ONS 15454 network nodes use the same date and time reference. The server synchronizes the node's time after power outages or software upgrades.

If you check the Use NTP/SNTP Server check box, complete the following fields:

- Use NTP/SNTP Server—Type the IP address of the primary NTP/SNTP server connected to the ONS 15454 or of another ONS 15454/15600/15310-CL/15310-MA as GNE with NTP/SNTP enabled that is connected to the ONS 15454 ENE.
- Backup NTP/SNTP Server—Type the IP address of the secondary NTP/SNTP server connected to the ONS 15454 or of another ONS 15454/15600/15310-CL/15310-MA with NTP/SNTP enabled that is connected to the ONS 15454 ENE.

  When the primary NTP/SNTP server fails or is not reachable, the node uses the secondary NTP/SNTP server to synchronize its date and time. If both the primary and secondary NTP/SNTP servers fail or are not reachable, an SNTP-FAIL alarm is raised. The node checks for the availability of the primary or secondary NTP/SNTP server at regular intervals until it can get the time from any one of the NTP/SNTP servers. After the node gets the time from any one server, it synchronizes its date and time with the server's date and time and the SNTP-FAIL alarm is cleared. For each retry and resynchronization, the node checks the availability of the primary NTP/SNTP server first, followed by the secondary NTP/SNTP server. The node synchronizes its date and time every hour.

  Note You will not be able to identify which NTP/SNTP server is being used for synchronization.

If you check gateway network element (GNE) for the ONS 15454 SOCKS proxy server (see "DLP-A249 Provision IP Settings" task on page 19-30), external ONS 15454s must reference the gateway ONS 15454 for NTP/SNTP timing. For more information about the ONS 15454 gateway settings, refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual*.

Note In ONS 15454 Software Release 9.0 and later, you can configure an IPv6 address for an NTP/SNTP server, in addition to an IPv4 address.

Caution If you reference another ONS 15454 for the NTP/SNTP server, make sure the second ONS 15454 references an NTP/SNTP server and not the first ONS 15454 (that is, do not create an NTP/SNTP timing loop by having two ONS 15454 nodes reference each other).

- Date—If Use NTP/SNTP Server is not checked, type the current date (mm/dd/yyyy, for example, September 24, 2002 is 09/24/2002).
- Time—If Use NTP/SNTP Server is not checked, type the current time in the format hh:mm:ss, for example, 11:24:58. The ONS 15454 uses a 24-hour clock, so 10:00 PM is entered as 22:00:00.
- Time Zone—Click the field and choose a city within your time zone from the drop-down list. The list displays the 80 World Time Zones from –11 through 0 (GMT) to +14. Continental United States time zones are GMT-05:00 (Eastern), GMT-06:00 (Central), GMT-07:00 (Mountain), and GMT-08:00 (Pacific).

- Use Daylight Savings Time—Check this check box if the time zone that you chose uses Daylight Savings Time.
- Insert AIS-V on STS-1 SD-P—Check this check box if you want Alarm Indication Signal Virtual Tributary (AIS-V) conditions inserted on VT circuits carried by STS-1s when the STS-1 crosses its Signal Degrade Path (SD-P) bit error rate (BER) threshold. On protected circuits, traffic will be switched. If the switch cannot be performed, or if circuits are not protected, traffic will be dropped when the STS-1 SD-P BER threshold is reached.
- SD-P BER—If you selected Insert AIS-V, you can choose the SD-P BER level from the SD-P BER drop-down list.

Step 4 Click **Apply**.

Step 5 In the confirmation dialog box, click **Yes**.

Step 6 Review the node information. If you need to make corrections, repeat Steps 3 through 5 to enter the corrections. If the information is correct, continue with the "NTP-A261 Set Power Monitor Thresholds" procedure on page 4-7.

Stop. **You have completed this procedure**.

NTP-A261 Set Power Monitor Thresholds

Purpose	This procedure provisions extreme high extreme low, and low input battery power thresholds within a –48 volts direct current (VDC) environment. When the thresholds are crossed, the TCC2/TCC2P generates warning alarms in CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 for the node you will set up. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Provisioning > General > Power Monitor** tabs.

Step 3 To change the extreme low battery voltage threshold in 0.5 VDC increments, choose a voltage from the ELWBATVG(Vdc) drop-down list.

Step 4 To change the low battery voltage threshold in 0.5 VDC increments, choose a voltage from the LWBATVG(Vdc) drop-down list.

Step 5 To change the high battery voltage threshold in 0.5 VDC increments, choose a voltage from the HIBATVG(Vdc) drop-down list.

Step 6 To change the extreme high battery voltage threshold in 0.5 VDC increments, choose a voltage from the EHIBATVG(Vdc) drop-down list.

Step 7 Click **Apply**.

Stop. You have completed this procedure.

NTP-A169 Set Up CTC Network Access

Purpose	This procedure provisions network access for a node, including its subnet mask, default router, Dynamic Host Configuration Protocol (DHCP) server, IIOP (Internet Inter-Orb Protocol) listener port, SOCKS proxy server settings, dual IP address setting, static routes, Open Shortest Path First (OSPF) protocol, Routing Information Protocol (RIP), and designated SOCKS servers.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A249 Provision IP Settings" task on page 19-30 to provision the ONS 15454 IP address, subnet mask, default router, DHCP server, IIOP listener port, and SOCKS proxy server settings.

Tip If you cannot log into the node, you can change its IP address, default router, and network mask by using the LCD on the ONS 15454 fan-tray assembly (unless LCD provisioning is suppressed). See the "DLP-A64 Set the IP Address, Default Router, and Network Mask Using the LCD" task on page 17-65 for instructions. However, you cannot use the LCD to provision any other network settings.

Step 3 If you want to turn on the ONS 15454 secure mode, which allows two IP addresses to be provisioned for the node if TCC2P cards are installed, complete the "DLP-A433 Enable Node Secure Mode" task on page 21-10. Refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual* for information about secure mode.

Step 4 If static routes are needed, complete the "DLP-A65 Create a Static Route" task on page 17-67. Refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual* for further information about static routes.

Step 5 If the ONS 15454 is connected to a LAN or WAN that uses OSPF and you want to share routing information between the LAN/WAN and the ONS network, complete the "DLP-A250 Set Up or Change Open Shortest Path First Protocol" task on page 19-35.

Step 6 If the ONS 15454 is connected to a LAN or WAN that uses RIP, complete the "DLP-A251 Set Up or Change Routing Information Protocol" task on page 19-37.

Step 7 Complete the "DLP-A558 Provision the Designated SOCKS Servers" task on page 22-71 after the network is provisioned if SOCKS proxy is enabled and you are experiencing long login and NE discovery times. This can occur in large networks that have a high ENE-to-GNE ratio and a low number of ENEs with LAN connectivity.

If these conditions do not exist, you are completed with this procedure.

Stop. **You have completed this procedure**.

NTP-A358 Set up the ONS 15454 in Secure Mode

Purpose	This procedure provisions ONS 15454s and CTC computers for secure access.
Tools/Equipment	None
Prerequisite Procedures	NTP-A169 Set Up CTC Network Access, page 4-8
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > Security > Access** pane.

Step 2 Under the **EMS Access** area, change the **Access State** to **Secure**.

Step 3 Click **Apply**. The CTC disconnects and reconnects through a secure socket connection.

Step 4 To create a secure connection, enter **https://node-address**.

Note After setting up a CTC connection in secure mode, http requests are automatically redirected to https mode.

Step 5 A first time connection is authenticated by the **Website Certification is Not Known** dialog box. Accept the certificate and click **OK**. The **Security Error: Domain Name Mismatch** dialog box appears. Click **OK** to continue.

Stop. **You have completed this procedure**.

NTP-A360 Enable EMS Secure Access

Purpose	This procedure enables EMS secure access. This procedure enables enhanced SFTP and SSH security.
Tools/Equipment	None
Prerequisite Procedures	NTP-A169 Set Up CTC Network Access, page 4-8
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In shelf view, click the **Provisioning > Security > Access** pane.

Step 2 Under the **EMS Access** area, change the **Access State** to **Secure**.

Step 3 Click **Apply**. The CTC disconnects and reconnects through a secure socket connection.

Step 4 Set the listener port value by choosing "Other constant" radio button.

Stop. **You have completed this procedure**.

NTP-A375 Set Up Secure Access to the ONS 15454 TL1

Purpose	This procedure provisions ONS 15454s for secure access to TL1.
Tools/Equipment	None
Prerequisite Procedures	NTP-A169 Set Up CTC Network Access, page 4-8
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In the node view, click the **Provisioning > Security > Access** pane.

Step 2 Under the **TL1 Access** area, change the **Access State** to **Secure**.

Step 3 Click **Apply**.

Existing non-secure TL1 sessions, if any, are terminated.

Step 4 To create a secure TL1 connection, enter the following command at the UNIX or Linux prompt:

ssh -l *username node-ip* **-p** *port-number*

The port number for secure TL1 is 4083.

Note Use any SSH client on Windows.

Stop. You have completed this procedure.

NTP-A27 Set Up the ONS 15454 for Firewall Access

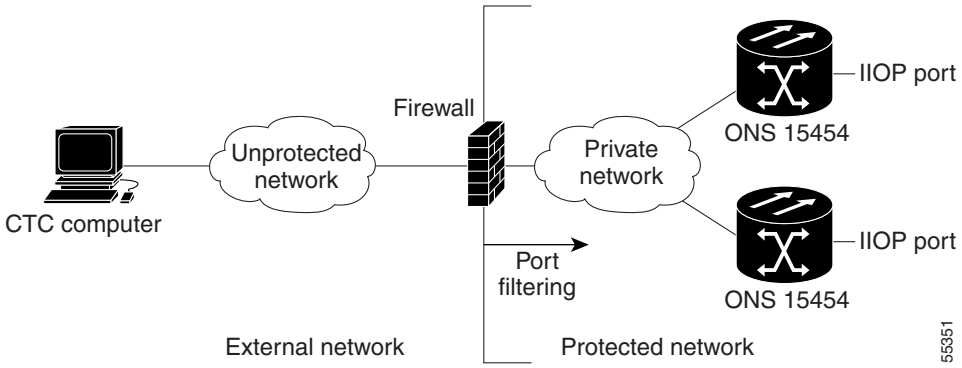
Purpose	This procedure provisions ONS 15454s and CTC computers for access through firewalls.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node that is behind the firewall. See the "DLP-A60 Log into CTC" task on page 17-60 for instructions. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A67 Provision the IIOP Listener Port on the ONS 15454" task on page 17-68.

Figure 4-1 shows an ONS 15454 in a protected network and the CTC computer in an external network. For the computer to access the ONS 15454s, you must provision the IIOP listener port specified by your firewall administrator on the ONS 15454.

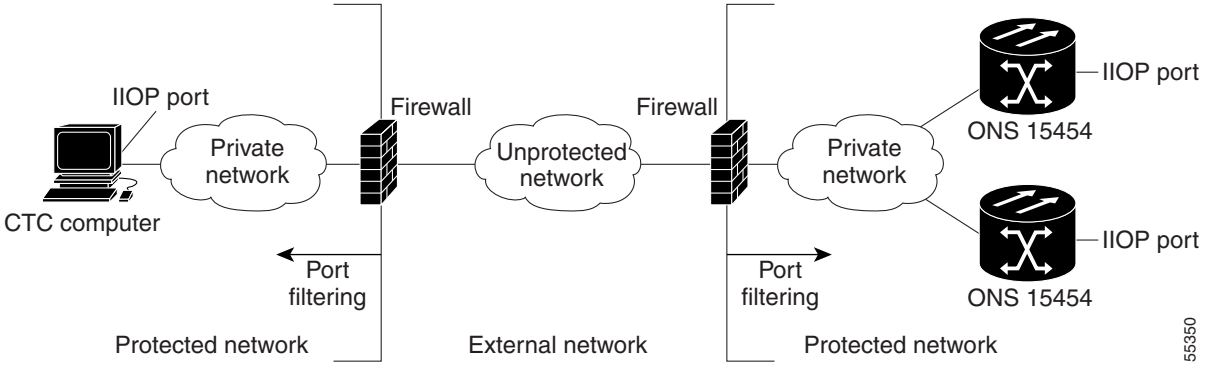
Figure 4-1 Nodes Behind a Firewall



Step 3 If the CTC computer resides behind a firewall, complete the "DLP-A68 Provision the IIOP Listener Port on the CTC Computer" task on page 17-69.

Figure 4-2 shows a CTC computer and ONS 15454 behind firewalls. For the computer to access the ONS 15454, you must provision the IIOP port on the CTC computer and on the ONS 15454.

Figure 4-2 CTC Computer and ONS 15454s Residing Behind Firewalls



Stop. You have completed this procedure.

NTP-A355 Create FTP Host

Purpose	This procedure provisions an FTP Host that you can use to perform database backup and restore or software download to an End Network Element (ENE) when proxy or firewall is enabled.
Tools/Equipment	None
Prerequisite Procedures	NTP-A169 Set Up CTC Network Access, page 4-8 NTP-A27 Set Up the ONS 15454 for Firewall Access, page 4-10
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 If you want to turn on the ONS 15454 secure mode, which allows two IPv4 addresses to be provisioned for the node if TCC2P cards are installed, complete the "DLP-A433 Enable Node Secure Mode" task on page 21-10. Refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual* for information about secure mode.

Step 3 In Node view, click the **Provisioning > Network > FTP Hosts** tabs.

Step 4 Click **Create**.

Step 5 Enter a valid IP address in the FTP Host Address field. A maximum of 12 host can be entered.

Note In ONS 15454 Software Release 9.0 and later, you can configure an IPv6 address for an FTP server, in addition to an IPv4 address.

Step 6 The Mask is automatically set according to the Net/Subnet Mask length specified in "DLP-A249 Provision IP Settings" section on page 19-30. To change the Mask, click the Up/Down arrows on the **Length** menu.

Step 7 Check the **FTP Relay Enable** radio button to allow FTP commands at the GNE relay. If you will enable the relay at a later time, go to Step 9. Certain TL1 commands executed on an ENE require FTP access into the Data Communication Network (DCN), the FTP relay on the GNE provides this access. The FTP hosts that you have configured in CTC can be used with the TL1 COPY-RFILE (for database backup and restore or software download) or COPY-IOSCFG (for Cisco IOS Configuration File backup and restore) commands.

Step 8 Enter the time, in minutes, that FTP Relay will be enabled. A valid entry is a number between 0 and 60. The number 0 disallows FTP command relay. After the specified time has elapsed the FTP Relay Enable flag is unset and FTP command relay is disallowed.

Step 9 Click OK.

Step 10 Repeat Step 4 through Step 9 to provision additional FTP Hosts.

Stop. **You have completed this procedure**.

NTP-A28 Set Up Timing

Purpose	This procedure provisions the ONS 15454 timing.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will set up timing. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A69 Set Up SONET External or Line Timing" task on page 17-69 if an external building integrated timing supply (BITS) source is available. This is the most common SONET timing setup procedure.

Step 3 If you cannot complete Step 2 (an external BITS source is not available), complete the "DLP-A70 Set Up Internal Timing" task on page 17-72. This task can only provide Stratum 3 timing.

Step 4 Complete the "DLP-A555 Set Up SDH External or Line Timing" task on page 22-68 if an external BITS source providing SDH timing (64 KHz, E1, or 2 MHz) is available. Use this task for a SONET shelf running on external SDH timing.

Note For information about SONET timing, refer to the "Timing" chapter in the *Cisco ONS 15454 Reference Manual* or to Telcordia GR-253-CORE.

Stop. **You have completed this procedure**.

NTP-A324 Create Protection Groups

Purpose	This procedure creates ONS 15454 card protection groups.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to create the protection group. If you are already logged in, continue with Step 2.

Table 4-1 describes the protection types available on the ONS 15454.

Table 4-1 Card Protection Types

Type	Cards	Description and Installation Requirements
1:1	DS1-14 DS3-12 DS3-12E DS3i-N-12 EC1-12 DS3XM-6 DS3XM-12 DS3/EC1-48	Pairs one working card with one protect card. The protect card should be installed in an odd-numbered slot and the working card in an even-numbered slot next to the protect slot towards the TCC2/TCC2P, for example: protect in Slot 1, working in Slot 2; protect in Slot 3, working in Slot 4; protect in Slot 15, working in Slot 14. 1:1 protection can be revertive or nonrevertive. For more information, refer to the "Card Protection" chapter and the card reference material specific to the card in the *Cisco ONS 15454 Reference Manual*.
1:N	DS1N-14 DS3N-12 DS3N-12E DS3i-N-12 DS3XM-12 DS3/EC1-48 DS1/E1-56	Assigns one protect card for several working cards. The maximum is 1:5. These protect cards must be installed in Slot 3 or 15 and the cards they protect must be on the same side of the shelf. Protect cards must match the cards they protect. For example, a DS1N-14 can only protect DS1-14 or DS1N-14 cards. If a failure clears, traffic reverts to the working card after the reversion time has elapsed. For more information, refer to the "Card Protection" chapter and the card reference material specific to the card in the *Cisco ONS 15454 Reference Manual*.
1+1	Any OC-N	Pairs a working OC-N card/port with a protect OC-N card/port. For multiport OC-N cards, the protect port must match the working port on the working card. For example, Port 1 of an OC-3 card can only be protected by Port 1 of another OC-3 card. The ports on multiport cards must be either working or protect. You cannot mix working and protect ports on the same card. Cards do not need to be in adjoining slots. 1+1 protection can be revertive or nonrevertive, bidirectional or unidirectional.
Optimized 1+1	OC-3-4 OC-3-8 MRC-2.5G-4 (in OC-3 configurations)	Ports must be provisioned to SDH. Optimized 1+1 protection is mainly used in networks that have linear 1+1 bidirectional protection schemes. Optimized 1+1 protection is a line-level protection scheme that includes two lines, working and protect. One of the two lines assumes the role of the primary channel, from which traffic gets selected, and the other port assumes the role of the secondary channel, which protects the primary channel. Traffic switches from the primary to the secondary channel based on either an external switching command or line conditions. After the line condition or the external switching command that was responsible for a switch clears, the roles of the two sides are reversed.

Table 4-1 Card Protection Types (continued)

Type	Cards	Description and Installation Requirements
Y Cable	MXP_2.5_10G MXP_2.5_10E MXP_2.5G_10E_C MXP_2.5G_10E_L MXP_MR_10DME_L MXP_MR_10DME_C TXP_MR_10G TXP_MR_10E TXP_MR_10E_L TXP_MR_10E_C MXP_2.5G_10E MXP_MR_2.5G GE_XP 10GE_XP	Pairs a working transponder or muxponder card/port with a protect transponder or muxponder card/port. The protect port must be on a different card than the working port and it must be the same card type as the working port. The working and protect port numbers must be the same, that is, Port 1 can only protect Port 1, Port 2 can only protect Port 2, etc. For more information, see the *Cisco ONS 15454 DWDM Procedure Guide*.
Splitter	TXPP_MR_2.5G MXPP_MR_2.5G	Splitter protection is automatically provided with the TXPP_MR_2.5G and MXPP_MR_2.5G cards. For more information, refer to the *Cisco ONS 15454 DWDM Procedure Guide*.
Unprotected	Any	Unprotected cards can cause signal loss if a card fails or incurs a signal error. However, because no card slots are reserved for protection, unprotected schemes maximize the service available for use on the ONS 15454. Unprotected is the default protection type.

Step 2 Complete one or more of the following tasks depending on the protection groups you want to create:

- "DLP-A71 Create a 1:1 Protection Group" task on page 17-73
- "DLP-A72 Create a 1:N Protection Group" task on page 17-75
- "DLP-A73 Create a 1+1 Protection Group" task on page 17-76
- DLP-A560 Create an Optimized 1+1 Protection Group, page 22-73

Note If a protect card is not installed, you can complete the "DLP-A332 Change Tunnel Type" task on page 20-20 and continue with the card protection provisioning.

Note A 1+1 protection group can only be provisioned between the same equipment type, using the same port number, and the same port rate. The MRC- 4 (MRC- 4 to MRC- 4 pairing) or MRC-12 (MRC-12 to MRC-12 pairing) cards can be in the same slot type or in different slot type; one in low speed-slot and one in high-speed slot.

Note To create Y-cable protection groups for TXP and MXP cards, refer to the *Cisco ONS 15454 DWDM Procedure Guide*.

Stop. You have completed this procedure.

NTP-A256 Set Up SNMP

Purpose	This procedure provisions the SNMP parameters so that you can use SNMP management software with the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	Required if SNMP is used at your installation.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to set up SNMP. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Provisioning** > **SNMP** tabs.

Step 3 In the Trap Destinations area, click **Create**.

Step 4 Complete the following in the Create SNMP Trap Destination dialog box (Figure 4-3):

- Destination IP Address—Type the IP address of your network management system. If the node you are logged into is an end network element (ENE), set the destination address to the GNE.

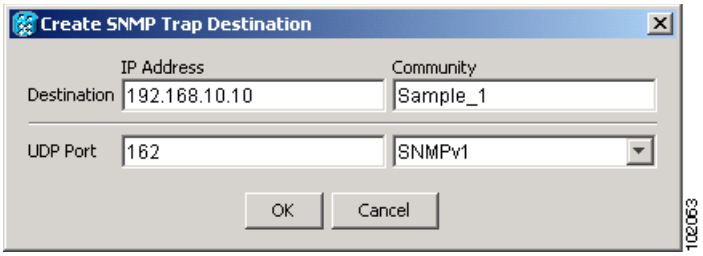
Note In ONS 15454 Software R9.0 and later, you can configure IPv6 addresses for SNMPv1/v2/v3 trap destinations, Get/Set requests and proxy targets, in addition to IPv4 addresses

- Community—Type the SNMP community name. For a description of SNMP community names, refer to the "SNMP" chapter in the *Cisco ONS 15454 Reference Manual*.

Note The community name is a form of authentication and access control. The community name assigned to the ONS 15454 is case-sensitive and must match the community name of the network management system (NMS).

- UDP Port—The default User Datagram Protocol (UDP) port for SNMP is 162. (More information about provisioning the UDP port is also given in the "DLP-A449 Set Up SNMP for a GNE" task on page 21-29 and the "DLP-A450 Set Up SNMP for an ENE" task on page 21-30.)
- Trap Version—Choose either SNMPv1 or SNMPv2. Refer to your NMS documentation to determine whether to use SNMPv1 or SNMPv2.

Figure 4-3 Creating an SNMP Trap



Step 5 Click **OK**. The node IP address of the node where you provisioned the new trap destination appears in the Trap Destinations area.

Step 6 Click the node IP address in the Trap Destinations area. Verify the SNMP information that appears in the Selected Destination list.

Step 7 If you want to set up SNMP remote monitoring (RMON) on GNEs and ENEs, complete the following tasks as required, depending on the protection groups you want to create:

- DLP-A449 Set Up SNMP for a GNE, page 21-29
- DLP-A450 Set Up SNMP for an ENE, page 21-30
- DLP-A451 Format and Enter NMS Community String for SNMP Command or Operation, page 21-32

Step 8 Click **Apply**.

Stop. **You have completed this procedure**.

NTP-A318 Provision OSI

Purpose	This procedure provisions the ONS 15454 so it can be networked with other vendor NEs that use the OSI protocol stack for data communications network (DCN) communications. This procedure provisions the TID TARP, OSI routers, manual area addresses, subnetwork points of attachment, and IP over OSI tunnels.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution This procedure requires an understanding of OSI protocols, parameters, and functions. Before you begin, review the OSI reference sections in the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual*.

Caution Do not begin this procedure until you know the role of the ONS 15454 within the OSI and IP network.

Note This procedure requires provisioning of non-ONS equipment including routers and third party network elements. Do not begin until you have the capability to complete that provisioning.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to provision the OSI routing mode. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the following tasks:

- DLP-A534 Provision OSI Routing Mode, page 22-42—Complete this task first.
- DLP-A535 Provision or Modify TARP Operating Parameters, page 22-43—Complete this task next.
- DLP-A536 Add a Static TID to NSAP Entry to the TARP Data Cache, page 22-45—Complete this task as needed.
- DLP-A538 Add a TARP Manual Adjacency Table Entry, page 22-46—Complete this task as needed.
- DLP-A539 Provision OSI Routers, page 22-47—Complete this task as needed.
- DLP-A540 Provision Additional Manual Area Addresses, page 22-48—Complete this task as needed.
- DLP-A541 Enable the OSI Subnet on the LAN Interface, page 22-48—Complete this task as needed.
- DLP-A542 Create an IP-Over-CLNS Tunnel, page 22-49—Complete this task as needed.

Stop. You have completed this procedure.

NTP-A364 Provision Node for SNMPv3

Purpose	This procedure provisions the node to allow SNMPv3 access.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 In node view, click the **Provisioning > SNMP > SNMP V3** tabs.

Step 3 Complete the following tasks as required:

- DLP-A584 Create an SNMPv3 User, page 22-94
- DLP-A586 Create Group Access, page 22-96

Note A group named default_group is defined in the initial configuration. The default group has read and notify access to the complete MIB tree.

- DLP-A585 Create MIB Views, page 22-95

Note A view named full_view is defined in the initial configuration. It includes the complete MIB tree supported on the node.

Stop. You have completed this procedure.

NTP-A365 Provision Node to Send SNMPv3 Traps

Purpose	This procedure provisions a node to send SNMP v3 traps.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 In node view, click the **Provisioning > SNMP > SNMP V3** tabs.

Step 3 Complete the following tasks as required:

- DLP-A584 Create an SNMPv3 User, page 22-94
- DLP-A586 Create Group Access, page 22-96
- DLP-A585 Create MIB Views, page 22-95
- DLP-A589 Create Notification Filters, page 22-98
- DLP-A587 Configure SNMPv3 Trap Destination, page 22-97. When you configure an SNMPv3 trap destination, use the IP address of the NMS, and the port number on which the NMS is listening for traps.

Stop. You have completed this procedure.

NTP-A366 Manually Provision a GNE/ENE to Manage an ENE using SNMPv3

Purpose	This procedure describes how to manually configure a GNE/ENE to allow the NMS to manage an ENE using SNMPv3.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 Go to network view.

Step 3 Double-click the ENE.

Step 4 Click **Provisioning > SNMP > SNMP V3 > General** and note the context engine ID. The context engine ID is required in Step 8.

Step 5 Double-click the GNE.

Step 6 Complete the "DLP-A584 Create an SNMPv3 User" task on page 22-94 to create an SNMPv3 user on the GNE.

Step 7 Complete the following tasks as needed on the ENE:

- DLP-A584 Create an SNMPv3 User, page 22-94
- DLP-A586 Create Group Access, page 22-96
- DLP-A585 Create MIB Views, page 22-95

Step 8 Complete the "DLP-A590 Manually Configure the SNMPv3 Proxy Forwarder Table" task on page 22-99. Use the context engine ID from Step 4, the local user details created in Step 6, and the remote user created in Step 7.

Stop. You have completed this procedure.

NTP-A367 Automatically Provision a GNE to Manage an ENE using SNMPv3

Purpose	This procedure describes how to automatically configure a GNE to allow an NMS to manage an ENE using SNMPv3.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 Go to network view.

Step 3 Double-click the GNE.

Step 4 Complete the "DLP-A584 Create an SNMPv3 User" task on page 22-94 to create an SNMPv3 user on the GNE.

Step 5 Complete the "DLP-A591 Automatically Configure the SNMPv3 Proxy Forwarder Table" task on page 22-100. Use the GNE user that you defined in Step 4 when you configure the Proxy Forwarder table.

Note When you use the automatic procedure, CTC automatically creates an ons_proxy user on the ENE, provides ENE user details for the proxy configuration, and the context engine ID of the ENE.

Stop. You have completed this procedure.

NTP-A368 Manually Provision a GNE/ENE to Send SNMPv3 Traps from an ENE using SNMPv3

Purpose	This procedure describes how to manually configure the GNE/ENE to allow an ENE to send SNMPv3 traps to the NMS.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 Go to network view.

Step 3 Double-click the GNE.

Step 4 Complete the "DLP-A584 Create an SNMPv3 User" task on page 22-94 to create an SNMPv3 user on the GNE.

Step 5 On the GNE, complete the "DLP-A587 Configure SNMPv3 Trap Destination" task on page 22-97. The target IP address must be the IPv4 or IPv6 address of the NMS. For the UDP Port number, use the port number on which the NMS is listening for traps. Use the user name configured in Step 4. Also, specify a target tag name.

Step 6 Double-click the ENE.

Step 7 Complete the "DLP-A584 Create an SNMPv3 User" task on page 22-94 to create an SNMPv3 user on the ENE.

Step 8 Complete the following tasks as required:

- DLP-A586 Create Group Access, page 22-96 to create a group on the ENE
- DLP-A585 Create MIB Views, page 22-95 to create a MIB view on the ENE
- DLP-A589 Create Notification Filters, page 22-98

Step 9 On the ENE, complete the "DLP-A587 Configure SNMPv3 Trap Destination" task on page 22-97. The target IP address should be the IP address of the GNE. The UDP port number is 161. Use the user name configured in Step 7.

Step 10 From the network view, click the **Provisioning > SNMPv3** tabs.

Step 11 Complete the "DLP-A592 Manually Configure the SNMPv3 Proxy Trap Forwarder Table" task on page 22-101.

The source of the trap must be the IP address of the ENE. For the context engine ID field, provide the context engine ID of the ENE. Also, you need to specify the target tag defined in Step 5, and the incoming user details configured in Step 7.

Stop. You have completed this procedure.

NTP-A369 Automatically Provision a GNE/ENE to Send SNMPv3 Traps from an ENE Using SNMPv3

Purpose	This procedure describes how to automatically configure the GNE/ENE to allow an ENE to send SNMPv3 traps to the NMS.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 Go to Network View.

Step 3 Double-click the GNE.

Step 4 Complete the task DLP-A584 Create an SNMPv3 User, page 22-94 to create an SNMPv3 user on the GNE.

Step 5 On the GNE, complete the following tasks:

- DLP-A587 Configure SNMPv3 Trap Destination, page 22-97. The target IP address must be the IPv4 or IPv6 address of the NMS. For the UDP Port number, use the port number on which the NMS is listening for traps. Also, specify a target tag name.
- DLP-A593 Automatically Configure the SNMPv3 Proxy Trap Forwarder Table, page 22-102. Use the target tag configured in Step 4. Use the IP address of the ENE as the source of trap. The following details are created automatically:
  - A user named ons_trap_user on the ENE
  - Trap destination on the ENE with an IP address of the GNE as the target IP and 161 as the UDP port number
  - Remote user details of the ENE on the GNE

Stop. You have completed this procedure.

CHAPTER 5

Turn Up a Network

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter explains how to turn up and test Cisco ONS 15454 networks, including point-to-point networks, linear add-drop multiplexers (ADMs), path protection configurations, and bidirectional line switched rings (BLSRs).

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A35 Verify Node Turn-Up, page 5-2—Complete this procedure before beginning network turn-up.
2. NTP-A124 Provision a Point-to-Point Network, page 5-3—Complete as needed.
3. NTP-A173 Point-to-Point Network Acceptance Test, page 5-4—Complete this procedure after you provision a point-to-point network.
4. NTP-A38 Provision a Linear ADM Network, page 5-6—Complete as needed.
5. NTP-A174 Linear ADM Network Acceptance Test, page 5-8—Complete this procedure after you provision a linear ADM.
6. NTP-A40 Provision BLSR Nodes, page 5-10—Complete this procedure to provision ONS 15454 nodes in a two-fiber or four-fiber BLSR.
7. NTP-A126 Create a BLSR, page 5-12—Complete this procedure after you provision the BLSR nodes.
8. NTP-A175 Two-Fiber BLSR Acceptance Test, page 5-13—Complete this procedure after you create a two-fiber BLSR.
9. NTP-A176 Four-Fiber BLSR Acceptance Test, page 5-15—Complete this procedure after you create a four-fiber BLSR.
10. NTP-A178 Provision a Traditional BLSR Dual-Ring Interconnect, page 5-17—As needed, complete this procedure after you provision a BLSR.

11. NTP-A179 Provision an Integrated BLSR Dual-Ring Interconnect, page 5-19—As needed, complete this procedure after you provision a BLSR.
12. NTP-A44 Provision Path Protection Nodes, page 5-20—Complete as needed.
13. NTP-A225 Open-Ended Path Protection Acceptance Test, page 5-33—Complete this procedure after you create a path protection.
14. NTP-A216 Provision a Traditional Path Protection Dual-Ring Interconnect, page 5-24—As needed, complete this procedure after you provision a path protection.
15. NTP-A217 Provision an Integrated Path Protection Dual-Ring Interconnect, page 5-26—As needed, complete this procedure after you provision a path protection.
16. NTP-A180 Provision a Traditional BLSR/Path Protection Dual-Ring Interconnect, page 5-27—As needed, complete this procedure after you provision a path protection and BLSR.
17. NTP-A209 Provision an Integrated BLSR/Path Protection Dual-Ring Interconnect, page 5-30—As needed, complete this procedure after you provision a path protection and BLSR.
18. NTP-A224 Provision an Open-Ended Path Protection Configuration, page 5-31—As needed, complete this procedure after you provision a path protection.
19. NTP-A225 Open-Ended Path Protection Acceptance Test, page 5-33—As needed, complete this procedure after you provision an open-ended path protection.
20. NTP-A46 Subtend a Path Protection Configuration from a BLSR, page 5-36—Complete as needed.
21. NTP-A47 Subtend a BLSR from a Path Protection Configuration, page 5-37—Complete as needed.
22. NTP-A48 Subtend a BLSR from a BLSR, page 5-38—Complete as needed.
23. NTP-A172 Create a Logical Network Map, page 5-40—Complete as needed.

NTP-A35 Verify Node Turn-Up

Purpose	This procedure verifies that an ONS 15454 is ready for network turn-up before adding it to a network.
Tools/Equipment	None
Prerequisite Procedures	Chapter 4, “Turn Up a Node”
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the “DLP-A60 Log into CTC” task on page 17-60 on the network you will test. If you are already logged in, continue with Step 2.

Step 2 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the “DLP-A227 Disable Alarm Filtering” task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 3 Verify that the SW Version and Defaults shown in the node view status area match the software version and NE defaults shown in your site plan. If either is not correct, complete the following procedures as needed:

- If the software is not the correct version, install the correct version from the Cisco ONS 15454 software CD. Upgrade procedures are located in a release-specific software upgrade document. TCC2/TCC2P cards can also be ordered with the latest software release.
- If the node defaults are not correct, import the network element defaults. Refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 4 Click the **Provisioning > General** tabs. Verify that all general node information settings match the settings of your site plan. If not, see the "NTP-A81 Change Node Management Information" procedure on page 11-2.

Step 5 Click the **Provisioning > Timing** tabs. Verify that timing settings match the settings of your site plan. If not, see the "NTP-A85 Change Node Timing" procedure on page 11-6.

Step 6 Click the **Provisioning > Network** tabs. Ensure that the IP settings and other CTC network access information is correct. If not, see the "NTP-A201 Change CTC Network Access" procedure on page 11-2.

Step 7 Click the **Provisioning > Protection** tabs. Verify that all protection groups have been created according to your site plan. If not, see the "NTP-A203 Modify or Delete Card Protection Settings" procedure on page 11-5.

Step 8 Click the **Provisioning > Security** tabs. Verify that all users have been created and their security levels and policies match the settings indicated by your site plan. If not, see the "NTP-A205 Modify Users and Change Security" procedure on page 11-7.

Step 9 If Simple Network Management Protocol (SNMP) is provisioned on the node, click the **Provisioning > SNMP** tabs. Verify that all SNMP settings match the settings of your site plan. If not, see the "NTP-A87 Change SNMP Settings" procedure on page 11-7.

Step 10 Provision the network using the applicable procedure shown in the "Before You Begin" section on page 5-1.

Stop. You have completed this procedure.

NTP-A124 Provision a Point-to-Point Network

Purpose	This procedure provisions two ONS 15454s in a 1+1 point-to-point (terminal) network.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 on an ONS 15454 in the network where you want to provision a point-to-point configuration. If you are already logged in, continue with Step 2.

Step 2 Click the **Provisioning > Protection** tabs. Verify that 1+1 protection is created for the OC-N cards. Complete the "DLP-A73 Create a 1+1 Protection Group" task on page 17-76 if protection has not been created.

Step 3 Repeat Steps 1 and 2 for the second point-to-point node.

Step 4 Verify that the working and protect cards in the 1+1 protection groups correspond to the physical fiber connections between the nodes, that is, verify that the working card in one node connects to the working card in the other node, and that the protect card in one node connects to the protect card in the other node.

Step 5 Complete the "DLP-A377 Provision Section DCC Terminations" task on page 20-69 for the working OC-N port on both point-to-point nodes. Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-A378 Provision Line DCC Terminations" task on page 20-71.

Note DCC terminations are not provisioned on the protect ports.

Note If the point-to-point nodes are not connected to a LAN, you will need to create the DCC terminations using a direct (craft) connection to the node. Remote provisioning is possible only after all nodes in the network have DCC terminations provisioned to in-service OC-N ports.

Step 6 Complete the "DLP-A214 Change the Service State for a Port" task on page 19-9 to put the protect card in-service.

Step 7 As needed, complete the "DLP-A380 Provision a Proxy Tunnel" task on page 20-77.

Step 8 As needed, complete the "DLP-A381 Provision a Firewall Tunnel" task on page 20-78.

Step 9 As needed, complete the "DLP-A367 Create a Provisionable Patchcord" task on page 20-51.

Step 10 Verify that timing is set up at both point-to-point nodes. If not, complete the "NTP-A28 Set Up Timing" procedure on page 4-13 for one or both of the nodes. If a node uses line timing, make its working OC-N card the timing source. The system will automatically choose the corresponding protect OC-N card as the protect timing source. This will be visible in the Maintenance > Timing tab.

Step 11 Complete the "NTP-A173 Point-to-Point Network Acceptance Test" procedure on page 5-4.

Stop. You have completed this procedure.

NTP-A173 Point-to-Point Network Acceptance Test

Purpose	This procedure tests a point-to-point network.
Tools/Equipment	Test set and cables appropriate to the test circuit you will create
Prerequisite Procedures	NTP-A124 Provision a Point-to-Point Network, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution This procedure might be service affecting if performed on a node carrying traffic.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at one of the point-to-point nodes. The node (default) view appears. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export alarm data.

Step 4 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

b. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the condition information.

Step 5 On the network map, double-click a point-to-point node to open it in node view.

Step 6 Create a test circuit from the login node to the other point-to-point node:

- For DS-1 circuits, complete the "NTP-A181 Create an Automatically Routed DS-1 Circuit" procedure on page 6-7. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-A184 Create an Automatically Routed DS-3 or EC-1 Circuit" procedure on page 6-19. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For OC-N circuits, complete the "NTP-A343 Create an Automatically Routed Optical Circuit" procedure on page 6-40. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 7 Configure the test set for the test circuit type you created:

- DS-1—If you are testing a DS-1 that is not multiplexed, you must have a DSX-1 panel or a direct DS-1 interface to the ONS 15454. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.
- DS3XM—If you are testing a DS-1 circuit on a DS3XM-6 or DS3XM-12 card you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for a multiplexed DS-3. Next, choose the DS-1 to test on the multiplexed DS-3. For information about configuring your test set, consult your test set user guide.
- OC-N—If you are testing an OC-N circuit, set the test set for the applicable circuit size. For information about configuring your test set, consult your test set user guide.

Step 8 Verify the integrity of all patch cables that will be used in this test by connecting one end to the test set transmit (Tx) connector the other to the test set receive (Rx) connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to Step 9.

Step 9 Create a physical loopback at the circuit destination card. To do so, attach one end of a patch cable to the destination port's Tx connector; attach the other end to the port's Rx connector.

Step 10 At the circuit source card:

a. Connect the Tx connector of the test set to the Rx connector on the circuit source card.

b. Connect the test set Rx connector to the circuit Tx connector on the circuit source card.

Step 11 Verify that the test set has a clean signal. If a clean signal is not present, repeat Steps 6 through 10 to make sure the test set and cabling are configured correctly.

Step 12 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

Step 13 Inject BIT errors from the test set. Verify that the errors appear at the test set, indicating a complete end-to-end circuit.

Step 14 Complete the "DLP-A356 TCC2/TCC2P Card Active/Standby Switch Test" task on page 20-40.

Step 15 Complete the "DLP-A255 Cross-Connect Card Side Switch Test" task on page 19-38.

Step 16 Complete the "DLP-A88 Optical 1+1 Protection Test" task on page 17-81.

Step 17 Set up and complete a bit error rate (BER) test. Use the existing configuration and follow your site requirements for the specified length of time. Record the test results and configuration.

Step 18 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete.

Step 19 From the View menu, choose **Go to Network View**.

Step 20 Click the **Alarms** tab.

- **a.** Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.
- **b.** Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.
- **c.** Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the alarms information.

Step 21 Repeat Steps 9 through 20 for the other point-to-point node.

Step 22 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

Step 23 Delete the test circuit. See the "DLP-A333 Delete Circuits" task on page 20-21.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application.

Stop. You have completed this procedure.

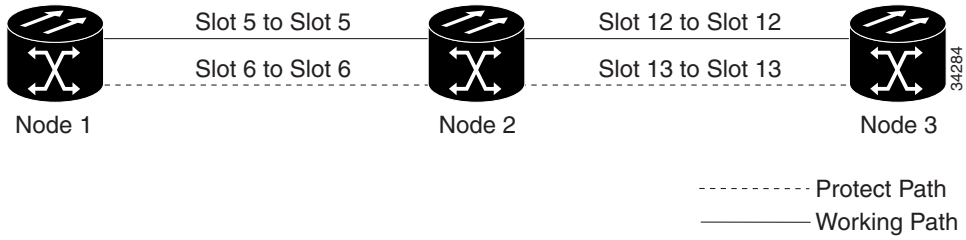
NTP-A38 Provision a Linear ADM Network

Purpose	This procedure provisions three or more ONS 15454s in a linear add-drop multiplexer (ADM) configuration.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at an ONS 15454 where you want to provision in a linear ADM network. If you are already logged in, continue with Step 2.

Figure 5-1 shows three ONS 15454s in a linear ADM configuration. In this example, working traffic flows from Slot 5/Node 1 to Slot 5/Node 2, and from Slot 12/Node 2 to Slot 12/Node 3. Slots 6 and 13 contain the protect OC-N cards. Slots 5 and 6 and Slots 12 and 13 are in 1+1 protection.

Figure 5-1 Linear ADM Configuration



Step 2 Click the **Provisioning > Protection** tabs. Verify that 1+1 protection is created for the OC-N cards at the node. If the protection group has not been created, complete the "DLP-A73 Create a 1+1 Protection Group" task on page 17-76.

Step 3 Repeat Steps 1 and 2 for all other nodes that you will include in the linear ADM.

Step 4 Verify that the working and protect cards in the 1+1 protection groups correspond to the physical fiber connections between the nodes, that is, working cards are fibered to working cards and protect cards are fibered to protect cards.

Step 5 Complete the "DLP-A377 Provision Section DCC Terminations" task on page 20-69 for the working OC-N ports on each linear ADM node. Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-A378 Provision Line DCC Terminations" task on page 20-71.

Note If linear ADM nodes are not connected to a LAN, you will need to create the DCC terminations using a direct (craft) connection to the node. Remote provisioning is possible only after all nodes without LAN connections have DCC terminations provisioned to in-service OC-N ports.

Note Terminating nodes (Nodes 1 and 3 in Figure 5-1) will have one DCC termination, and intermediate nodes (Node 2 in Figure 5-1) will have two DCC terminations (Slots 5 and 12 in the example).

Step 6 As needed, complete the "DLP-A380 Provision a Proxy Tunnel" task on page 20-77.

Step 7 As needed, complete the "DLP-A381 Provision a Firewall Tunnel" task on page 20-78.

Step 8 As needed, complete the "DLP-A367 Create a Provisionable Patchcord" task on page 20-51.

Step 9 Verify that the timing has been set up at each linear node. If not, complete the "NTP-A28 Set Up Timing" procedure on page 4-13. If a node is using line timing, use its working OC-N card as the timing source.

Step 10 Complete the "NTP-A174 Linear ADM Network Acceptance Test" procedure on page 5-8.

Stop. You have completed this procedure.

NTP-A174 Linear ADM Network Acceptance Test

Purpose	This procedure tests a linear ADM network.
Tools/Equipment	Test set and cables appropriate to the test circuit you will create.
Prerequisite Procedures	NTP-A38 Provision a Linear ADM Network, page 5-6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 on a node in the linear ADM network you are testing. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the alarm information.

Step 4 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

b. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the conditions information.

Step 5 On the network map, double-click the linear ADM node you are testing to open it in node view.

Step 6 Create a test circuit from that node to an adjacent linear ADM node.

- For DS-1 circuits, complete the "NTP-A181 Create an Automatically Routed DS-1 Circuit" procedure on page 6-7. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-A184 Create an Automatically Routed DS-3 or EC-1 Circuit" procedure on page 6-19. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For OC-N circuits, complete the "NTP-A343 Create an Automatically Routed Optical Circuit" procedure on page 6-40. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 7 Configure the test set for the test circuit type you created:

- DS-1 card—If you are testing a DS-1 that is not multiplexed, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15454. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15454. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.

- DS3XM—If you are testing a DS-1 circuit on a DS3XM-6 or DS3XM-12 card you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for a multiplexed DS-3, then choose the DS-1 to test on the multiplexed DS-3. For information about configuring your test set, consult your test set user guide.
- OC-N—If you are testing an OC-N circuit, set the test set for the applicable circuit size. For information about configuring your test set, consult your test set user guide.

Step 8 Verify the integrity of all patch cables that will be used in this test by connecting one end to the test set Tx connector and the other end to the test set Rx connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to the next step.

Step 9 Create a physical loopback at the circuit destination card. To do so, attach one end of a patch cable to the destination port's Tx connector; attach the other end to the destination port's Rx connector.

Step 10 At the circuit source card:

a. Connect the Tx connector of the test set to the circuit Rx connector.

b. Connect the test set Rx connector to the circuit Tx connector.

Step 11 Verify that the test set shows a clean signal. If a clean signal does not appear, repeat Steps 6 through 10 to make sure the test set and cabling are configured correctly.

Step 12 Inject BIT errors from the test set. Verify that the errors appear at the test set, indicating a complete end-to-end circuit.

Step 13 Complete the "DLP-A356 TCC2/TCC2P Card Active/Standby Switch Test" task on page 20-40.

Step 14 Complete the "DLP-A255 Cross-Connect Card Side Switch Test" task on page 19-38.

Step 15 Complete the "DLP-A88 Optical 1+1 Protection Test" task on page 17-81 to test the OC-N port protection group switching.

Step 16 Set up and complete a BER test. Use the existing configuration and follow your site requirements for length of time. Record the test results and configuration.

Step 17 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete.

Step 18 In network view, click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 19 Delete the test circuit. See the "DLP-A333 Delete Circuits" task on page 20-21.

Step 20 Repeat Steps 6 through 19 for the next linear ADM node you are testing.

Step 21 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application.

Stop. You have completed this procedure.

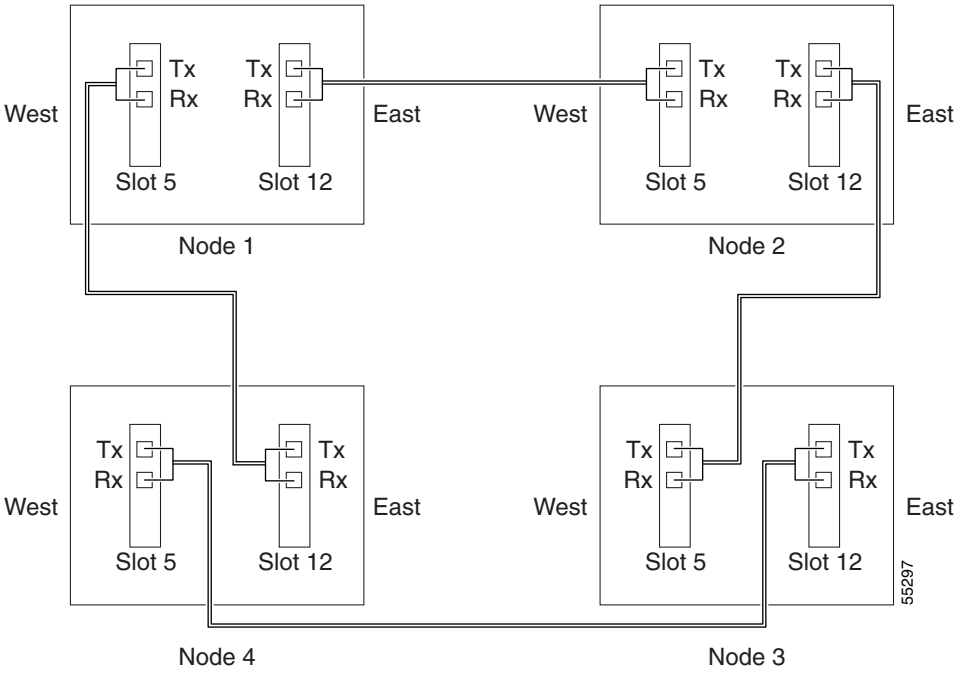
NTP-A40 Provision BLSR Nodes

Purpose	This procedure provisions ONS 15454 nodes for a BLSR.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A44 Install Fiber-Optic Cables for BLSR Configurations" task on page 17-46, verifying that the following rules are observed:

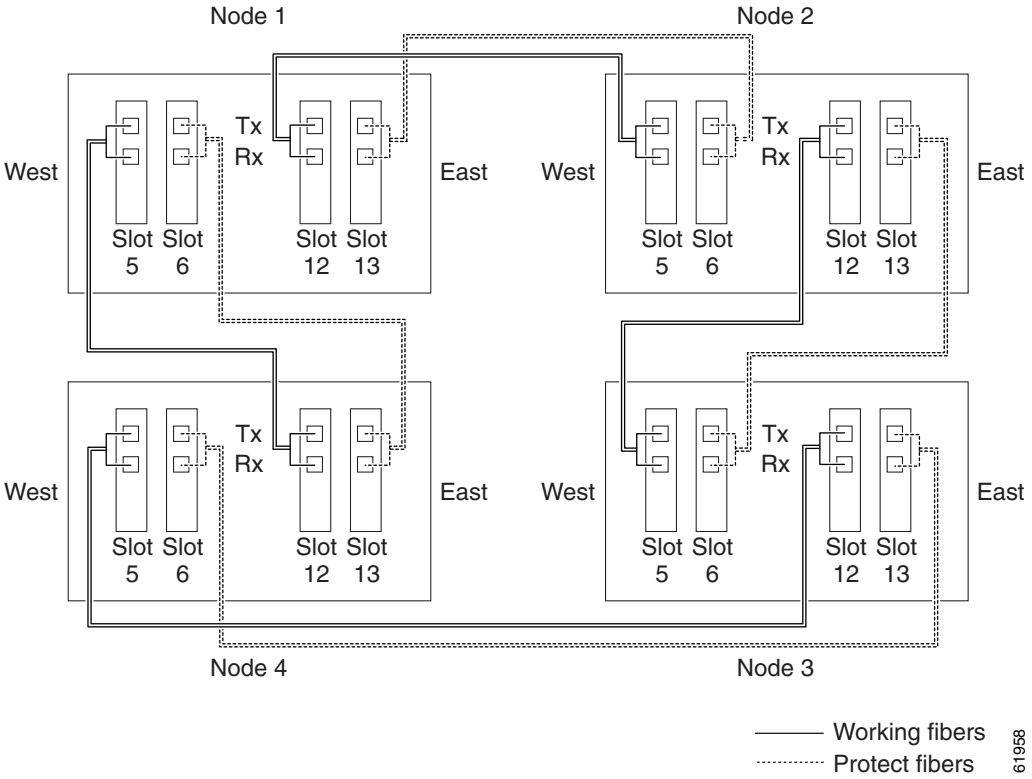
- Verify that the east port at one node is connected to the west port on an adjacent node, and this east-to-west port connection is used at all BLSR nodes, similar to Figure 5-2. In the figure, the OC-N drop card on the left side of the shelf is the west port, and the drop card on the right side of the shelf is considered the east port.

Figure 5-2 Four-Node, Two-Fiber BLSR Fiber Connection Example



- For four-fiber BLSRs, verify that the same east port to west port connection is used for the working and protect fibers, similar to Figure 5-3. Verify that the working and protect card connections are not mixed. The working cards are the cards where you will provision the DCC terminations.

Figure 5-3 Four-Node, Four-Fiber BLSR Fiber Connection Example



Step 2 Log into an ONS 15454 that you want to configure in a BLSR. See the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 3.

Step 3 Complete the "DLP-A377 Provision Section DCC Terminations" task on page 20-69. Provision the two ports/cards that will serve as the BLSR ports at the node. For four-fiber BLSRs, provision the DCC terminations on the OC-N cards that will carry the working traffic, but do not provision DCCs on the protect cards.

Note If an ONS 15454 is not connected to a corporate LAN, DCC provisioning must be performed through a direct (craft) connection to the node. Remote provisioning is possible only after all nodes in the network have DCCs provisioned to IS-NR OC-N ports.

Step 4 For four-fiber BLSRs, complete the "DLP-A214 Change the Service State for a Port" task on page 19-9 to put the protect OC-N cards/ports in service.

Step 5 Repeat Steps 2 through 4 at each node that will be in the BLSR. Verify that the EOC (DCC Termination Failure) and LOS (Loss of Signal) are cleared after DCCs are provisioned on all nodes in the ring.

Step 6 As needed, complete the "DLP-A380 Provision a Proxy Tunnel" task on page 20-77.

Step 7 As needed, complete the "DLP-A381 Provision a Firewall Tunnel" task on page 20-78.

Step 8 As needed, complete the "DLP-A367 Create a Provisionable Patchcord" task on page 20-51.

Step 9 If a BLSR span passes through third-party equipment that cannot transparently transport the K3 byte, complete the "DLP-A89 Remap the K3 Byte" task on page 17-82. This task is not necessary for most users.

Step 10 Complete the "NTP-A126 Create a BLSR" procedure on page 5-12.

Stop. You have completed this procedure.

NTP-A126 Create a BLSR

Purpose	This procedure creates a BLSR at each BLSR-provisioned node.
Tools/Equipment	None
Prerequisite Procedures	NTP-A40 Provision BLSR Nodes, page 5-10
Required/As Needed	As needed; required to complete BLSR provisioning
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node on the network where you will create the BLSR.

Step 2 Complete one of the following tasks:

- DLP-A328 Create a Two-Fiber BLSR Using the BLSR Wizard, page 20-17 – Use this task to create a two-fiber BLSR using the CTC BLSR wizard. The BLSR wizard checks to see that each node is ready for BLSR provisioning, then provisions all the nodes at once. Using the BLSR wizard is recommended.
- DLP-A362 Create a Four-Fiber BLSR Using the BLSR Wizard, page 20-46—Use this task to create a four-fiber BLSR using the CTC BLSR wizard. The BLSR wizard checks to see that each node is ready for BLSR provisioning, then provisions all the nodes at once. Using the BLSR wizard is recommended.
- DLP-A329 Create a Two-Fiber BLSR Manually, page 20-18— Use this task to provision a two-fiber BLSR manually at each node that will be in the BLSR.
- DLP-A363 Create a Four-Fiber BLSR Manually, page 20-47—Use this task to provision a four-fiber BLSR manually at each node that will be in the BLSR.

Step 3 Complete the "NTP-A175 Two-Fiber BLSR Acceptance Test" procedure on page 5-13 or the "NTP-A176 Four-Fiber BLSR Acceptance Test" procedure on page 5-15.

Stop. You have completed this procedure.

NTP-A175 Two-Fiber BLSR Acceptance Test

Purpose	This procedure tests a two-fiber BLSR.
Tools/Equipment	Test set and cables appropriate for the test circuit
Prerequisite Procedures	NTP-A40 Provision BLSR Nodes, page 5-10 NTP-A126 Create a BLSR, page 5-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This procedure requires that you create test circuits and perform ring switches around the ring. For clarity, "Node 1" refers to the login node where you begin the procedure. "Node 2" refers to the node connected to the east OC-N trunk (span) card of Node 1.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at one of the ONS 15454s on the BLSR you are testing. (This node will be called Node 1.) If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the alarm information.

Step 4 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

b. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the conditions information.

Step 5 On the network view, double-click Node 1.

Step 6 Complete the "DLP-A217 BLSR Exercise Ring Test" task on page 19-10.

Step 7 Create a test circuit from Node 1 to the node connected to the east OC-N trunk (span) card of Node 1. (This node will be called Node 2.)

- For DS-1 circuits, complete the "NTP-A181 Create an Automatically Routed DS-1 Circuit" procedure on page 6-7. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-A184 Create an Automatically Routed DS-3 or EC-1 Circuit" procedure on page 6-19. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For OC-N circuits, complete the "NTP-A343 Create an Automatically Routed Optical Circuit" procedure on page 6-40. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 8 Configure the test set for the test circuit type you created:

- DS-1—If you are testing a DS-1 that is not multiplexed, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15454. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15454. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.
- DS3XM—If you are testing a DS-1 circuit on a DS3XM-6 or DS3XM-12 card you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for a multiplexed DS-3, then choose the DS-1 to test on the multiplexed DS-3. For information about configuring your test set, consult your test set user guide.
- OC-N—If you are testing an OC-N circuit, set the test set for the applicable circuit size. For information about configuring your test set, consult your test set user guide.

Step 9 Verify the integrity of all patch cables that will be used in this test by connecting the test set Tx connector to the test set Rx connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to the next step.

Step 10 Create a physical loopback at the circuit destination card. To do so, attach one end of a patch cable to the destination port's Tx connector; attach the other end to the port's Rx connector.

Step 11 At the circuit source card:

a. Connect the Tx connector of the test set to the circuit Rx connector.

b. Connect the test set Rx connector to the circuit Tx connector.

Step 12 Verify that the test set shows a clean signal. If a clean signal does not appear, repeat Steps 7 through 11 to make sure the test set and cabling are configured correctly.

Step 13 Inject BIT errors from the test set. Verify that the errors appear at the test set, verifying a complete end-to-end circuit.

Step 14 Complete the "DLP-A356 TCC2/TCC2P Card Active/Standby Switch Test" task on page 20-40.

Step 15 Complete the "DLP-A255 Cross-Connect Card Side Switch Test" task on page 19-38.

Although a service interruption under 60 ms might occur, the test circuit should continue to work before, during, and after the switches. If the circuit stops working, do not continue. Contact your next level of support.

Step 16 Complete the "DLP-A91 BLSR Switch Test" task on page 17-83 at Node 1.

Step 17 Set up and complete a BER test on the test circuit. Use the existing configuration and follow your site requirements for length of time. Record the test results and configuration.

Step 18 Complete the "DLP-A333 Delete Circuits" task on page 20-21 for the test circuit.

Step 19 Repeating Steps 5 through 18 for Nodes 2 and higher, work your way around the BLSR, testing each node and span in the ring. Create test circuits between every two consecutive nodes.

Step 20 After you test the entire ring, remove any loopbacks and test sets from the nodes.

Step 21 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application. Continue with Chapter 6, "Create Circuits and VT Tunnels."

Stop. You have completed this procedure.

NTP-A176 Four-Fiber BLSR Acceptance Test

Purpose	This procedure tests a four-fiber BLSR.
Tools/Equipment	Test set and cables appropriate to the test circuit you will create
Prerequisite Procedures	NTP-A40 Provision BLSR Nodes, page 5-10 NTP-A126 Create a BLSR, page 5-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution This procedure might be service affecting if performed on a node carrying traffic.

Note This procedure requires that you create test circuits and perform a ring switch. For clarity, "Node 1" refers to the login node where you begin the procedure. "Node 2" refers to the node connected to the east OC-N trunk (span) card of Node 1, "Node 3" refers to the node connected to the east OC-N trunk card of Node 2, and so on.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 on the BLSR you are testing. (This node will be called Node 1.) If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the alarm information.

Step 4 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

b. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the conditions information.

Step 5 On the network map, double-click Node 1.

Step 6 Complete the "DLP-A92 Four-Fiber BLSR Exercise Span Test" task on page 17-86.

Step 7 Complete the "DLP-A217 BLSR Exercise Ring Test" task on page 19-10.

Step 8 Create a test circuit between Node 1 and Node 2.

- For DS-1 circuits, complete the "NTP-A181 Create an Automatically Routed DS-1 Circuit" procedure on page 6-7. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-A184 Create an Automatically Routed DS-3 or EC-1 Circuit" procedure on page 6-19. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

- For OC-N circuits, complete the "NTP-A343 Create an Automatically Routed Optical Circuit" procedure on page 6-40. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 9 Configure the test set for the test circuit type you created:

- DS-1—If you are testing a DS-1 that is not multiplexed, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15454. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15454. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.
- DS3XM—If you are testing a DS-1 circuit on a DS3XM-6 or DS3XM-12 card you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for a multiplexed DS-3, then choose the DS-1 to test on the multiplexed DS-3. For information about configuring your test set, consult your test set user guide.
- OC-N—If you are testing an OC-N circuit, set the test set for the applicable circuit size. For information about configuring your test set, consult your test set user guide.

Step 10 Verify the integrity of all patch cables that will be used in this test by connecting one end of the cable to the test set Tx connector and the other end of the cable to the test set Rx connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before continuing.

Step 11 Create a physical loopback at the circuit destination card. To do so, attach one end of a patch cable to the destination port's Tx connector; attach the other end to the port's Rx connector.

Step 12 At the circuit source card:

a. Connect the Tx connector of the test set to the circuit Rx connector.

b. Connect the test set Rx connector to the circuit Tx connector.

Step 13 Verify that the test set shows a clean signal. If a clean signal does not appear, repeat Steps 6 through 12 to make sure the test set and cabling are configured correctly.

Step 14 Inject global BIT errors from the test set. Verify that the errors appear at the test set, verifying a complete end-to-end circuit.

Step 15 Complete the "DLP-A356 TCC2/TCC2P Card Active/Standby Switch Test" task on page 20-40.

Step 16 Complete the "DLP-A255 Cross-Connect Card Side Switch Test" task on page 19-38.

Step 17 Complete the "DLP-A91 BLSR Switch Test" task on page 17-83 to test the BLSR protection switching at Node 1.

Step 18 Complete the "DLP-A93 Four-Fiber BLSR Span Switching Test" task on page 17-88 at Node 1.

Step 19 Set up and complete a BER test on the test circuit between Node 1 and 2. Use the existing configuration and follow your site requirements for length of time. Record the test results and configuration.

Step 20 Complete the "DLP-A333 Delete Circuits" task on page 20-21 for the test circuit.

Step 21 At Node 2, repeat Steps 5 through 20, creating a test circuit between Node 2 and the node connected to the east OC-N trunk (span) card of Node 2, which is Node 3. Work your way around the BLSR creating test circuits between every two consecutive nodes.

Step 22 After you test the entire ring, remove any loopbacks and test sets from the nodes.

Step 23 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the alarm information.

Step 24 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

b. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the conditions information.

Step 25 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application. Continue with Chapter 6, "Create Circuits and VT Tunnels."

Stop. You have completed this procedure.

NTP-A178 Provision a Traditional BLSR Dual-Ring Interconnect

Purpose	This procedure provisions BLSRs in a traditional dual-ring interconnect (DRI) topology. DRIs interconnect two or more BLSRs to provide an additional level of protection. Two-fiber and four-fiber BLSRs can be mixed in a traditional BLSR DRI network.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note To route circuits on the DRI, you must check the Dual Ring Interconnect check box during circuit creation.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Complete the following steps if you have not provisioned the BLSRs that you will interconnect in a BLSR DRI. If the BLSRs are created, go to Step 3.

a. Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 5-10 to provision the BLSRs.

b. Complete the "NTP-A126 Create a BLSR" procedure on page 5-12 to create the BLSRs.

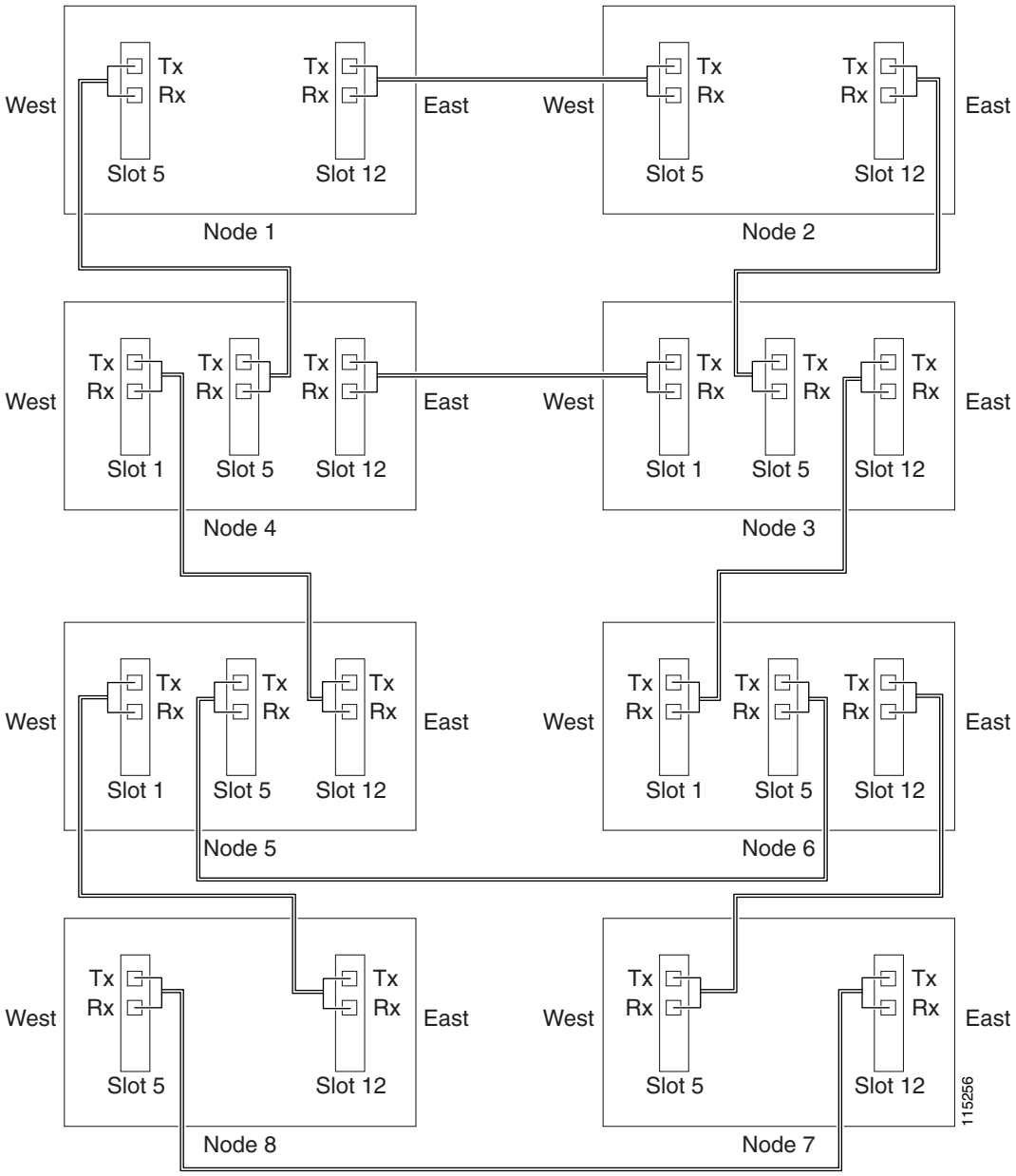
c. Complete the "NTP-A175 Two-Fiber BLSR Acceptance Test" procedure on page 5-13 to test two-fiber BLSRs.

d. Complete the "NTP-A176 Four-Fiber BLSR Acceptance Test" procedure on page 5-15 to test four-fiber BLSRs.

Step 3 Verify that the BLSR DRI interconnect nodes have OC-N cards installed and have fiber connections to the other interconnect nodes:

- The OC-N cards that will connect the BLSRs must be installed at the interconnect nodes.
- The interconnect nodes must have fiber connections. Figure 5-4 shows an example of fiber connections for a traditional two-fiber BLSR DRI.

Figure 5-4 Traditional Two-Fiber BLSR DRI Fiber Connection Example



Stop. You have completed this procedure.

NTP-A179 Provision an Integrated BLSR Dual-Ring Interconnect

Purpose	This procedure provisions BLSRs in an integrated DRI topology.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node in the BLSR DRI network. If you are already logged in, continue with Step 2.

Step 2 Complete the following steps if you have not provisioned the BLSRs that you will interconnect in a BLSR DRI. If the BLSRs are created, go to Step 3.

a. Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 5-10 to provision the BLSRs.

b. Complete the "NTP-A126 Create a BLSR" procedure on page 5-12 to create the BLSRs.

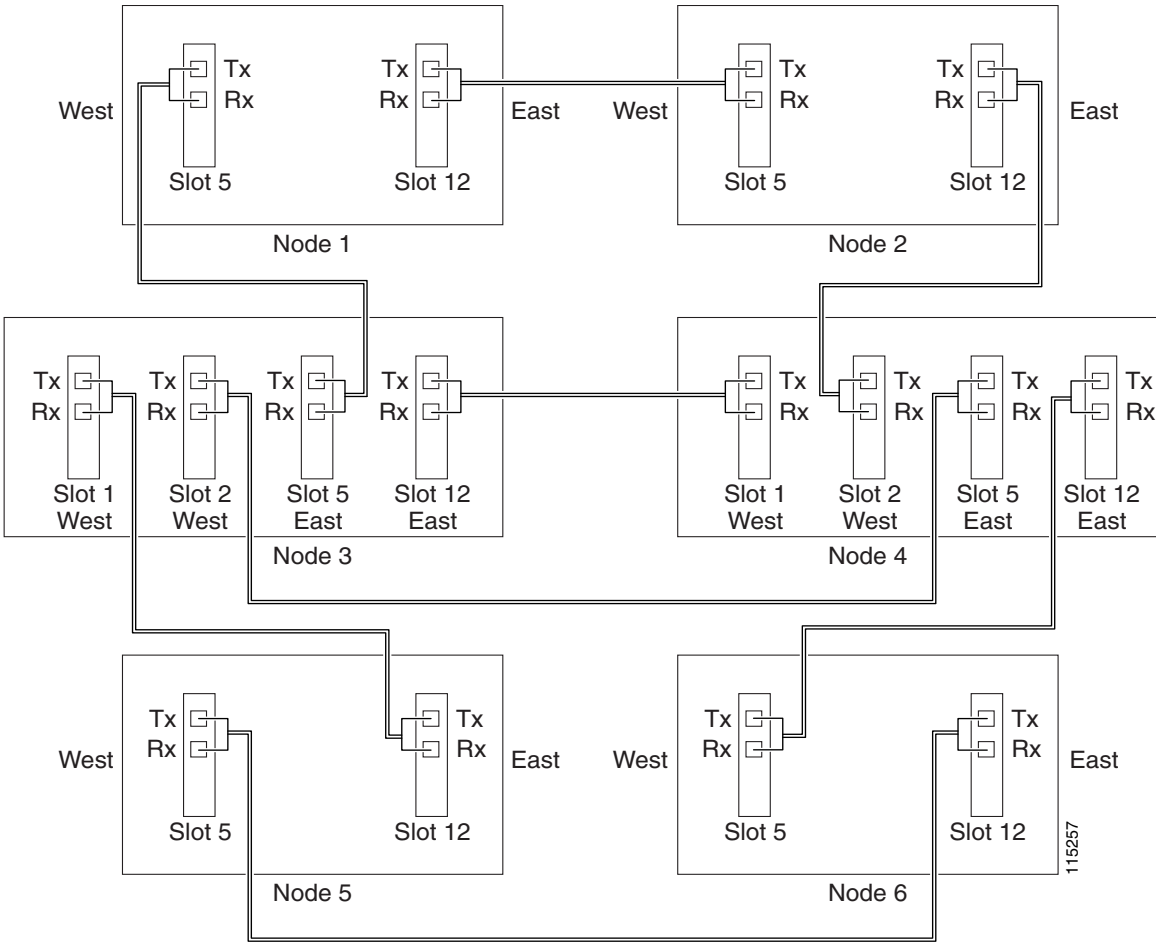
c. Complete the "NTP-A175 Two-Fiber BLSR Acceptance Test" procedure on page 5-13 to test two-fiber BLSRs.

d. Complete the "NTP-A176 Four-Fiber BLSR Acceptance Test" procedure on page 5-15 to test four-fiber BLSRs.

Step 3 Verify that the BLSR DRI node has OC-N cards installed and has fiber connections to the other interconnect node:

- The OC-N cards that will connect the BLSRs must be installed at the two interconnect nodes.
- The two interconnect nodes must have the correct fiber connections. Figure 5-5 shows an example of an integrated two-fiber BLSR DRI configuration.

Figure 5-5 Integrated Two-Fiber BLSR DRI Example



Stop. You have completed this procedure.

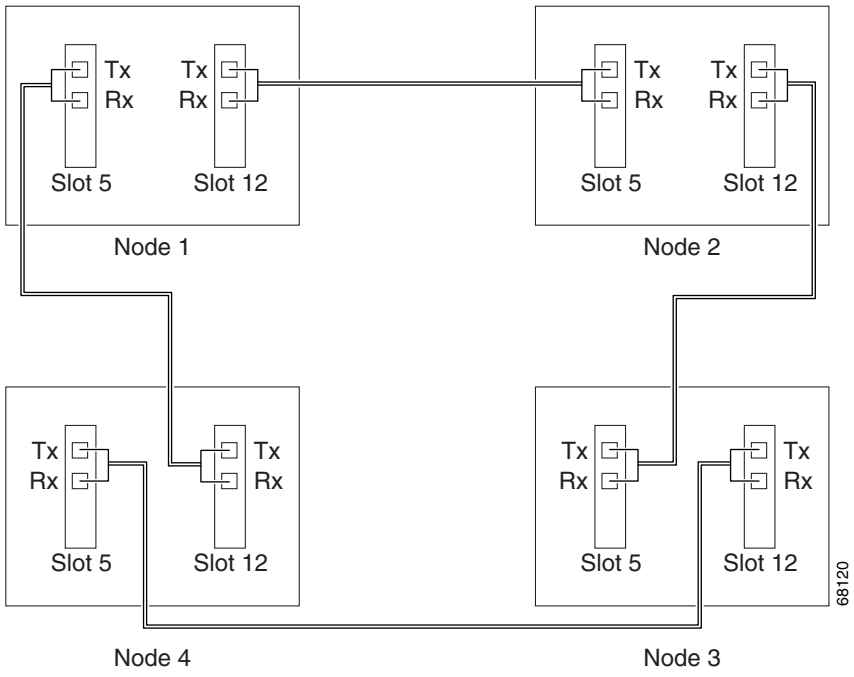
NTP-A44 Provision Path Protection Nodes

Purpose	This procedure provisions nodes for inclusion in a path protection configuration.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note Path protection is the default ONS 15454 topology. It is available as soon as you install the path protection OC-N cards, connect the OC-N fibers, and create the DCC terminations. Unlike the BLSRs, ONS 15454 path protection configurations do not require explicit setup.

Step 1 Verify that the fiber is correctly connected to the path protection trunk (span) OC-N cards similar to Figure 5-6. See the "DLP-A43 Install Fiber-Optic Cables for Path Protection Configurations" task on page 17-43.

Figure 5-6 Path Protection Fiber Connection Example



Step 2 Log into an ONS 15454 in the path protection you are turning up. See the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 3.

Step 3 Complete the "DLP-A377 Provision Section DCC Terminations" task on page 20-69 for the two cards/ports that will serve as the path protection ports on the node, for example, Slot 5 (OC-48)/Node 1 and Slot 12 (OC-48)/Node 1. (Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-A378 Provision Line DCC Terminations" task on page 20-71.)

Note If an ONS 15454 is not connected to a corporate LAN, DCC or LDCC provisioning must be performed through a direct (craft) connection. Remote provisioning is possible only after all nodes in the network have DCC or LDCC terminations provisioned to in-service OC-N ports.

Step 4 Repeat Steps 2 and 3 for each node in the path protection.

Step 5 As needed, complete the "DLP-A380 Provision a Proxy Tunnel" task on page 20-77.

Step 6 As needed, complete the "DLP-A381 Provision a Firewall Tunnel" task on page 20-78.

Step 7 As needed, complete the "DLP-A367 Create a Provisionable Patchcord" task on page 20-51.

Step 8 Complete the "NTP-A177 Path Protection Acceptance Test" procedure on page 5-22.

Stop. You have completed this procedure.

NTP-A177 Path Protection Acceptance Test

Purpose	This procedure tests a path protection configuration.
Tools/Equipment	Test set and cables appropriate to the test circuit you will create.
Prerequisite Procedures	NTP-A44 Provision Path Protection Nodes, page 5-20
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution This procedure might be service affecting if performed on a node carrying traffic.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at one of the ONS 15454s on the path protection configuration you are testing. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the alarm information.

Step 4 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

b. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the conditions information.

Step 5 On the network map, double-click the node that you logged into in Step 1.

Step 6 Create a test circuit from that node to the next adjacent path protection node.

- For DS-1 circuits, complete the "NTP-A181 Create an Automatically Routed DS-1 Circuit" procedure on page 6-7. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-A184 Create an Automatically Routed DS-3 or EC-1 Circuit" procedure on page 6-19. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For OC-N circuits, complete the "NTP-A343 Create an Automatically Routed Optical Circuit" procedure on page 6-40. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 7 Configure the test set for the test circuit type you created:

- DS-1—If you are testing a DS-1 that is not multiplexed, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15454. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15454. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.
- DS3XM—If you are testing a DS-1 circuit on a DS3XM-6 or a DS3XM-12 card you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for a multiplexed DS-3, then choose the DS-1 to test on the multiplexed DS-3. For information about configuring your test set, consult your test set user guide.
- OC-N—If you are testing an OC-N circuit, set the test set for the applicable circuit size. For information about configuring your test set, consult your test set user guide.

Step 8 Verify the integrity of all patch cables that will be used in this test by connecting one end to the test set Tx connector and the other end to the test set Rx connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before continuing.

Step 9 Create a physical loopback at the circuit destination card:

a. Attach one end of a patch cable to the destination port's Tx connector.

b. Attach the other end to the port's Rx connector.

Step 10 At the circuit source card:

a. Connect the Tx connector of the test set to the circuit Rx connector.

b. Connect the test set Rx connector to the circuit Tx connector.

Step 11 Verify that the test set has a clean signal. If a clean signal does not appear, repeat Steps 6 through 10 to make sure the test set and cabling are configured correctly.

Step 12 Inject BIT errors from the test set. To verify that you have a complete end-to-end circuit, verify that the errors appear at the test set.

Step 13 Complete the "DLP-A356 TCC2/TCC2P Card Active/Standby Switch Test" task on page 20-40.

Step 14 Complete the "DLP-A255 Cross-Connect Card Side Switch Test" task on page 19-38.

Step 15 From the View menu, choose **Go to Network View**.

Step 16 Click one of the two spans leaving the circuit source node.

Step 17 Complete the "DLP-A94 Path Protection Configuration Protection Switching Test" task on page 17-90 to test the path protection switching function on this span.

Step 18 In network view, click the other circuit source span and repeat Step 17.

Step 19 Set up and complete a BER test. Use the existing configuration and follow your site requirements for the length of time. Record the test results and configuration.

Step 20 Complete the "DLP-A333 Delete Circuits" task on page 20-21 for the test circuit.

Step 21 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete.

Step 22 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the alarm information.

Step 23 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

b. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the conditions information.

Step 24 Repeat Steps 5 through 23 for each node on the network.

Step 25 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application. Continue with Chapter 6, "Create Circuits and VT Tunnels."

Stop. You have completed this procedure.

NTP-A216 Provision a Traditional Path Protection Dual-Ring Interconnect

Purpose	This procedure provisions path protection configurations in a traditional DRI topology. DRIs interconnect two or more path protection configurations to provide an additional level of protection.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note To route circuits on the DRI, you must check the Dual Ring Interconnect check box during circuit creation.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Complete the following steps if you have not provisioned the path protection configurations that you will interconnect in a path protection DRI. If the path protection configurations are created, go to Step 3.

a. Complete the "NTP-A44 Provision Path Protection Nodes" procedure on page 5-20 to provision the path protection configurations.

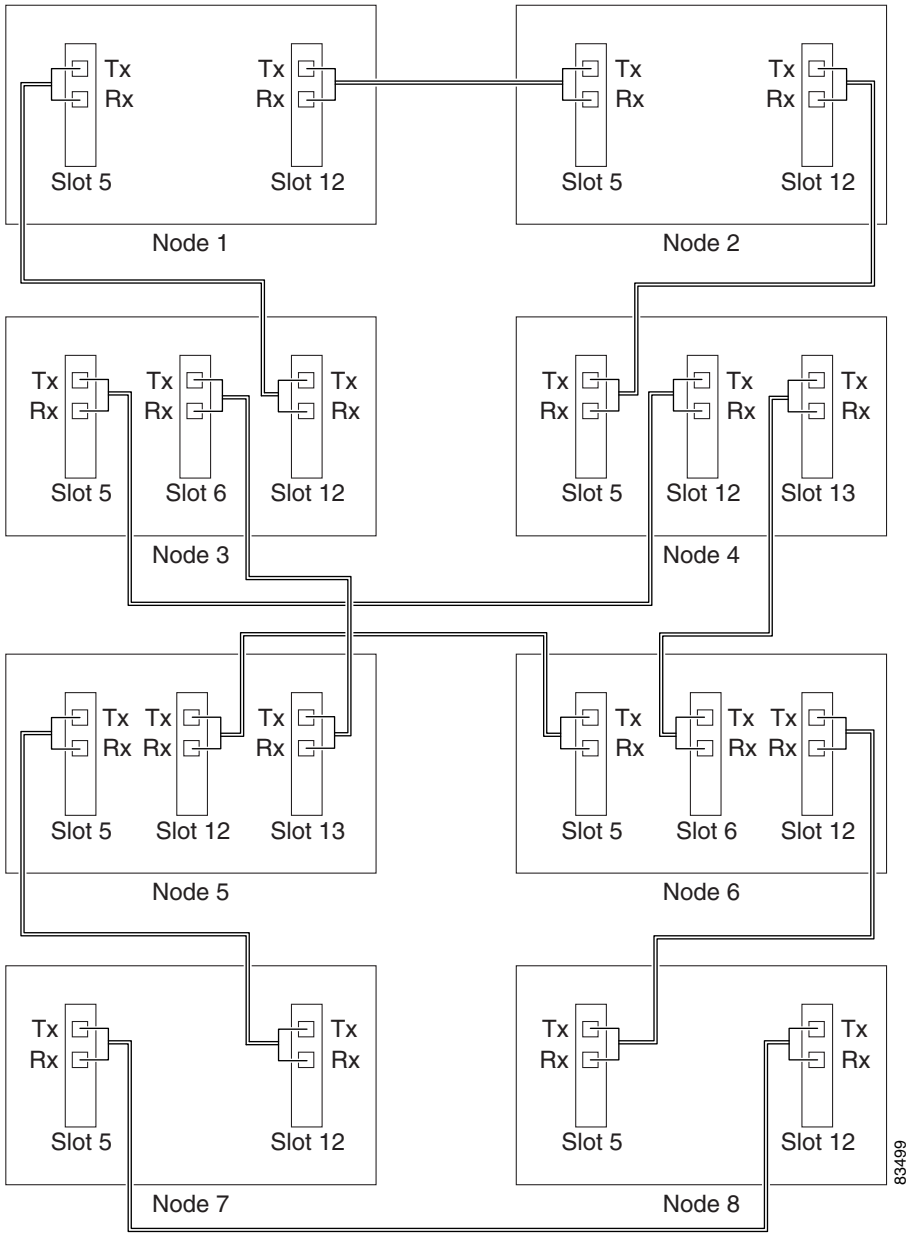
b. Complete the "NTP-A177 Path Protection Acceptance Test" procedure on page 5-22 to test the path protection configurations.

Note All path protection configurations that will be interconnected must have the same OC-N rate.

Step 3 Verify that the path protection DRI interconnect nodes have OC-N cards installed and have fiber connections to the other interconnect node:

- The OC-N cards that will connect the path protection must be installed at the interconnect nodes. The OC-N cards in the path protection nodes and the interconnect nodes must be the same type.
- The interconnect nodes must have fiber connections. An example is shown in Figure 5-7. This example shows a path protection DRI with two rings, Nodes 1 through 4 and 5 through 8. In the example, an additional OC-N is installed in Slot 13 at Node 4 and connected to an OC-N in Slot 6 at Node 6. Nodes 3 and 5 are interconnected with OC-N cards in Slot 6 (Node 3) and Slot 13 (Node 5).

Figure 5-7 Traditional Path Protection DRI Fiber Connection Example



Stop. You have completed this procedure.

NTP-A217 Provision an Integrated Path Protection Dual-Ring Interconnect

Purpose	This procedure provisions path protection configurations in an integrated DRI topology. In the integrated DRI, the path protection OC-N trunk cards for both path protection configurations are installed on the same shelf.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node in the path protection DRI network. If you are already logged in, continue with Step 2.

Step 2 Complete the following steps if you have not provisioned the path protection configurations that you will interconnect in a path protection DRI. If the path protection configurations are created, continue with Step 3.

a. Complete the "NTP-A44 Provision Path Protection Nodes" procedure on page 5-20 to provision the path protection configurations.

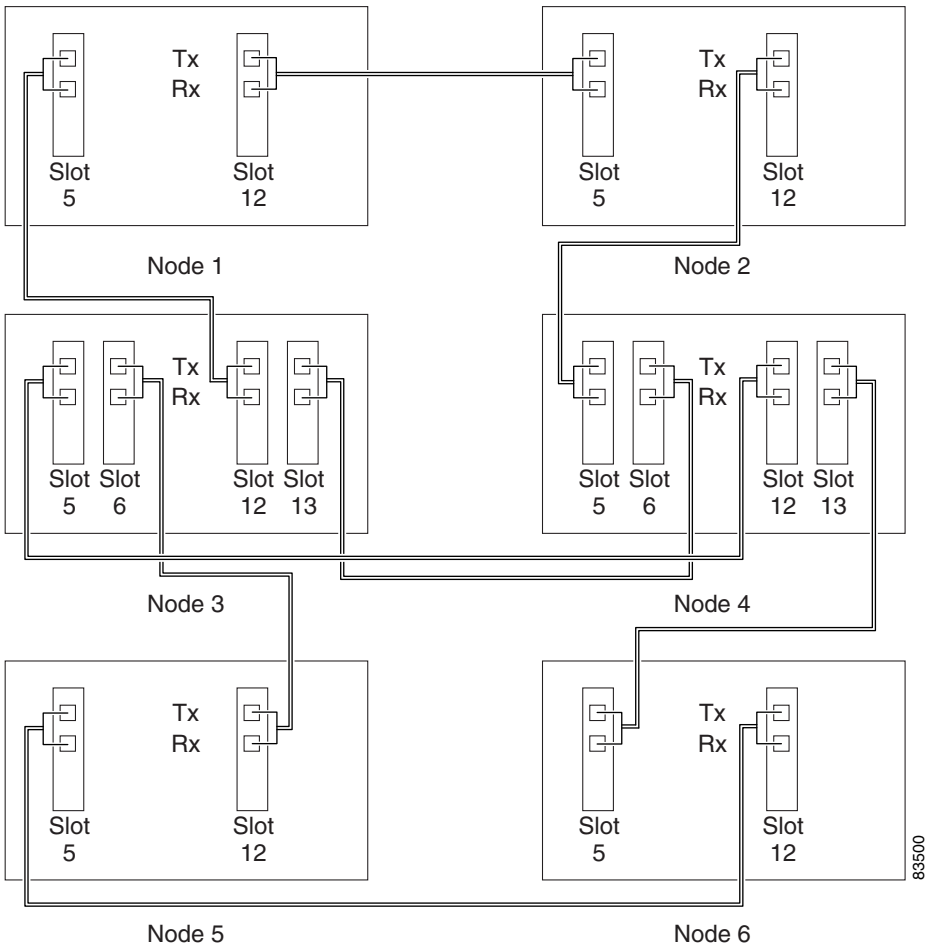
b. Complete the "NTP-A177 Path Protection Acceptance Test" procedure on page 5-22 to test the path protection configurations.

Note All path protection configurations that will be interconnected must have the same OC-N rate.

Step 3 Verify that the path protection DRI interconnect nodes have OC-N cards installed and have fiber connections to the other interconnect node:

- The OC-N cards that will connect the path protection configurations must be installed at the interconnect nodes. The OC-N cards in the path protection nodes and the interconnect nodes must be the same type.
- The interconnect nodes must have the correct fiber connections. An example is shown in Figure 5-8. This example shows a path protection DRI with two rings.

Figure 5-8 Integrated Path Protection DRI Example



Stop. You have completed this procedure.

NTP-A180 Provision a Traditional BLSR/Path Protection Dual-Ring Interconnect

Purpose	This procedure provisions a BLSR and a path protection in a traditional DRI topology. DRIs interconnect ring topologies to provide an additional level of protection.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note To route circuits on the DRI, you must check the Dual Ring Interconnect check box during circuit creation.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Complete the following steps if you have not provisioned the BLSR and path protection that you will interconnect in a traditional DRI. If the BLSR and path protection are created, go to Step 3.

a. To provision and test the BLSR, complete the following procedures:

- NTP-A40 Provision BLSR Nodes, page 5-10
- NTP-A126 Create a BLSR, page 5-12
- NTP-A175 Two-Fiber BLSR Acceptance Test, page 5-13
- NTP-A176 Four-Fiber BLSR Acceptance Test, page 5-15

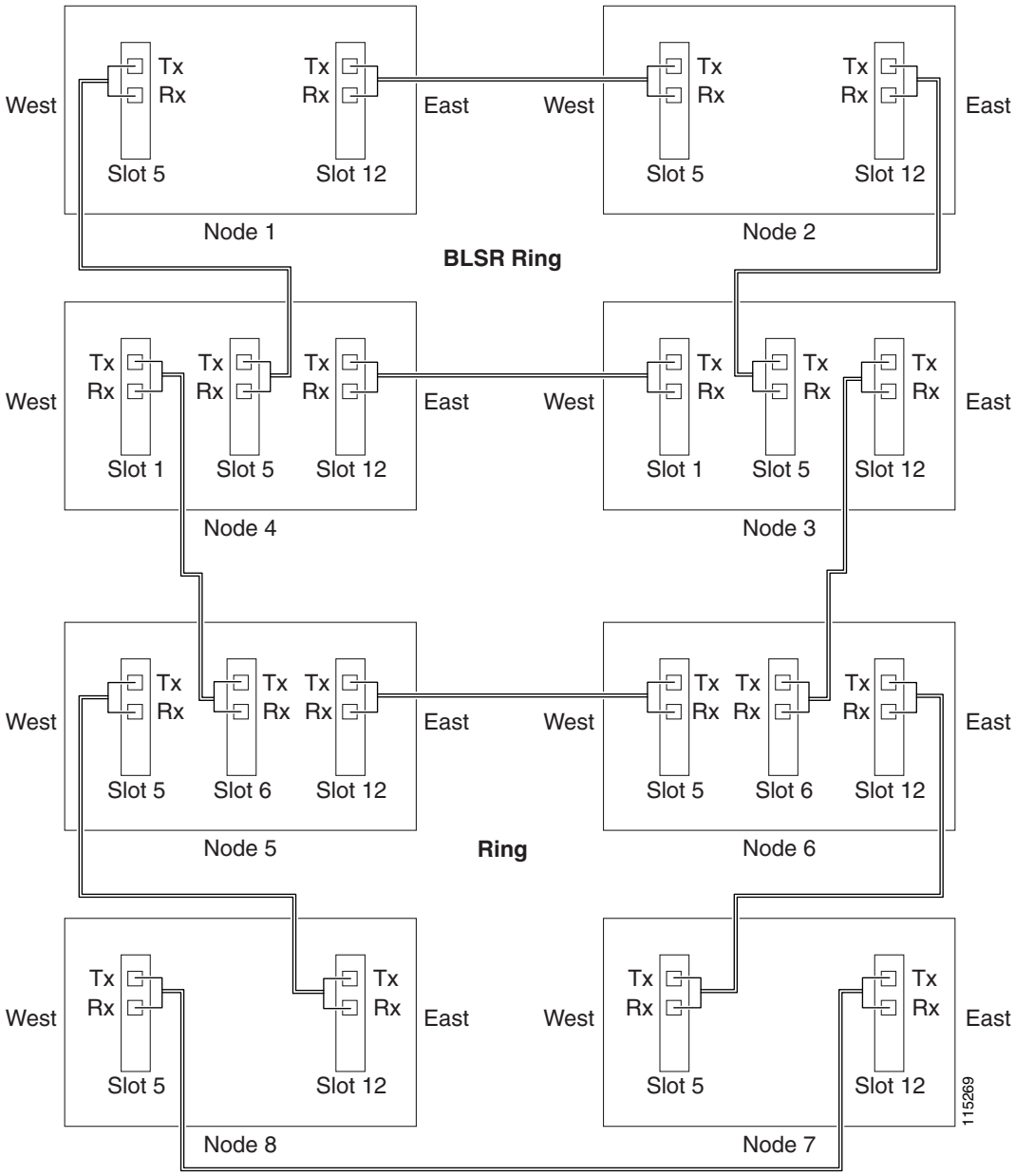
b. To provision and test the path protection, complete the following procedures:

- NTP-A44 Provision Path Protection Nodes, page 5-20
- NTP-A177 Path Protection Acceptance Test, page 5-22

Step 3 Verify that the DRI interconnect nodes have OC-N cards installed and have fiber connections to the other interconnect node:

- The OC-N cards that will connect the BLSR and path protection must be installed at the interconnect nodes. The OC-N cards in the path protection nodes and the interconnect nodes must be the same type.
- The interconnect nodes must have fiber connections. An example is shown in Figure 5-9.

Figure 5-9 Traditional BLSR to Path Protection DRI Fiber Connection Example



Stop. You have completed this procedure.

NTP-A209 Provision an Integrated BLSR/Path Protection Dual-Ring Interconnect

Purpose	This procedure provisions a BLSR and a path protection in an integrated DRI topology.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node in the BLSR and path protection DRI network. If you are already logged in, continue with Step 2.

Step 2 Complete the following steps if you have not provisioned the BLSR and path protection that you will interconnect in an integrated DRI. If the BLSR and path protection are created, continue with Step 3.

a. To provision and test the BLSR, complete the following procedures:

- NTP-A40 Provision BLSR Nodes, page 5-10
- NTP-A126 Create a BLSR, page 5-12
- NTP-A175 Two-Fiber BLSR Acceptance Test, page 5-13
- NTP-A176 Four-Fiber BLSR Acceptance Test, page 5-15

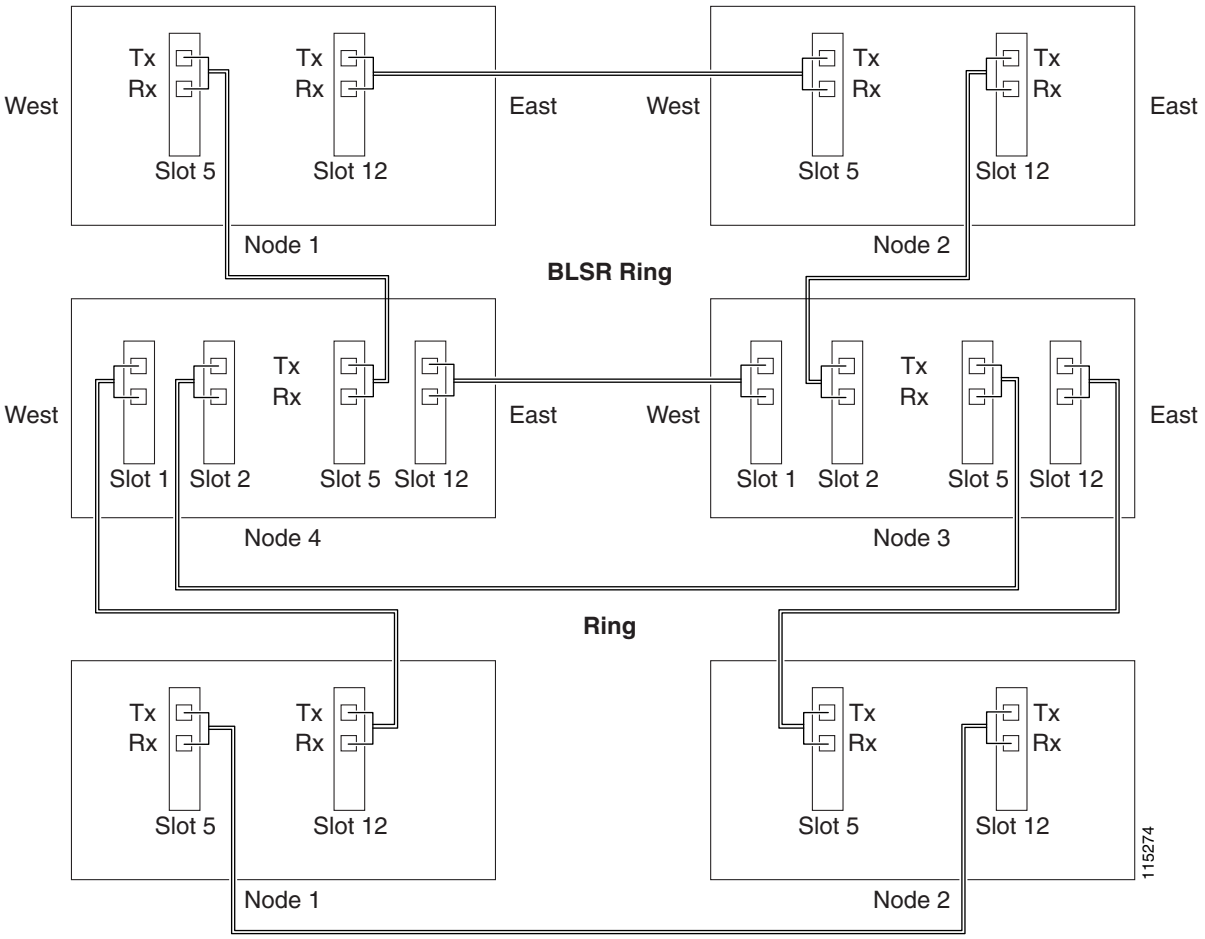
b. To provision and test the path protection, complete the following procedures:

- NTP-A44 Provision Path Protection Nodes, page 5-20
- NTP-A177 Path Protection Acceptance Test, page 5-22

Step 3 Verify that the BLSR and path protection DRI interconnect nodes have OC-N cards installed and have fiber connections to the other interconnect node:

- The OC-N cards that will connect the BLSR and path protection must be installed at the interconnect nodes. The OC-N cards in the path protection nodes and the interconnect nodes must be the same type.
- The interconnect nodes must have the correct fiber connections. An example is shown in Figure 5-10.

Figure 5-10 Integrated BLSR to Path Protection DRI Example



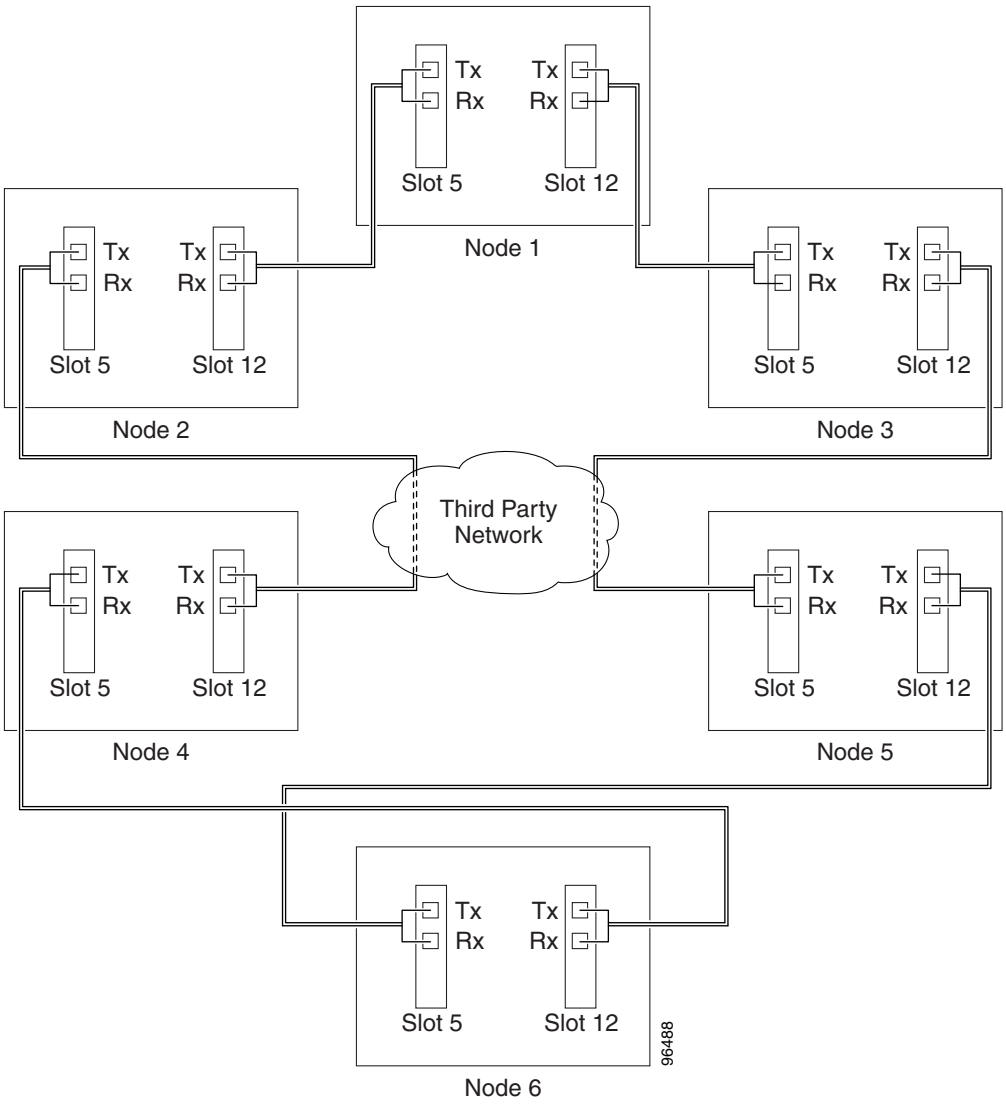
Stop. You have completed this procedure.

NTP-A224 Provision an Open-Ended Path Protection Configuration

Purpose	This procedure provisions ONS 15454 nodes in an open-ended path protection connected to a third-party vendor network. This topology allows you to route a circuit from one ONS 15454 network to another ONS 15454 network through the third-party network.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Verify that the fiber is correctly connected to the path protection trunk (span) OC-N cards at each open-ended path protection node. Figure 5-11 shows an example. Node 1 is connected to ONS 15454 Nodes 2 and 3 through Slots 12 and 5. Trunk cards at Nodes 2 and 3 are connected to the third-party vendor equipment.

Figure 5-11 ONS 15454 Open-Ended Path Protection Configurations Fiber Connection Example



Step 2 Verify that the third-party cards to which the ONS 15454 trunk cards are connected are the same OC-N rate as the ONS 15454 trunk cards. The third-party time slots must match the ONS 15454 card time slots to which they are connected. For example, if your trunk card is an OC-48, the third-party vendor card or unit must have STSs 1 to 48 available.

Step 3 Log into an ONS 15454 in the path protection you are turning up. See the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 4.

Step 4 Complete the "DLP-A377 Provision Section DCC Terminations" task on page 20-69 for the ONS 15454 cards/ports that are connected to another ONS 15454. (Alternatively, if additional bandwidth is needed for CTC management, complete the"DLP-A378 Provision Line DCC Terminations" task on page 20-71.) Do not create DCC or LDCC terminations for the card/port that connects to the third-party equipment. For example in Figure 5-11, DCC terminations are created at the following cards/ports:

- Nodes 1 and 6: Slot 5 and Slot 12
- Node 2 and 5: Slot 12
- Node 3 and 4: Slot 5

Note If an ONS 15454 is not connected to a corporate LAN, DCC or LDCC provisioning must be performed through a direct (craft) connection. Remote provisioning is possible only after all nodes in the network have DCC or LDCC terminations provisioned to in-service OC-N ports.

Step 5 Repeat Steps 3 and 4 for each node in the path protection.

Step 6 As needed, complete the "DLP-A380 Provision a Proxy Tunnel" task on page 20-77.

Step 7 As needed, complete the "DLP-A381 Provision a Firewall Tunnel" task on page 20-78.

Step 8 Following the documentation provided by the third-party vendor, provision the optical loop leading from the ONS 15454 connection at one end to the ONS 15454 connection at the other end. In other words, you will create an open-ended path protection using procedures for the third-party equipment.

Step 9 Complete the "NTP-A225 Open-Ended Path Protection Acceptance Test" procedure on page 5-33.

Stop. You have completed this procedure.

NTP-A225 Open-Ended Path Protection Acceptance Test

Purpose	This procedure tests an open-ended path protection configuration.
Tools/Equipment	Test set and cables appropriate to the test circuit you will create.
Prerequisite Procedures	NTP-A224 Provision an Open-Ended Path Protection Configuration, page 5-31
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution This procedure might be service affecting if performed on a node carrying traffic.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node that will be the source node for traffic traversing the third-party network. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the alarm information.

Step 4 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

b. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the conditions information.

Step 5 On the network map, double-click the node that you logged into in Step 1.

Step 6 Create a test circuit from that node to the OC-N trunk (span) cards on the nodes that connect to the third-party network. For example, in Figure 5-11, a circuit is created from Node 1 to the Slot 5 OC-N card at Node 2, and a secondary circuit destination is created on the Slot 12 OC-N card at Node 3. For circuit creation procedures, complete one of the following:

- For DS-1 circuits, complete the "NTP-A181 Create an Automatically Routed DS-1 Circuit" procedure on page 6-7. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-A184 Create an Automatically Routed DS-3 or EC-1 Circuit" procedure on page 6-19. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For OC-N circuits, complete the "NTP-A343 Create an Automatically Routed Optical Circuit" procedure on page 6-40. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 7 Create a circuit within the third-party network from ONS 15454 connection ports to the second set of ONS 15454 connection ports on both path protection spans. Refer to the third-party equipment documentation for circuit creation procedures.

Step 8 Repeat Step 6 to create a second circuit at the terminating node on the other side of the third-party network. In Figure 5-11, this is Node 6. However, this circuit will have two sources, one at Node 4/Slot 12, and one at Node 5/Slot 5. The destination will be a drop card on Node 6.

Step 9 Configure the test set for the test circuit type you created:

- DS-1—If you are testing a DS-1 that is not multiplexed, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15454. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15454. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.
- DS3XM—If you are testing a DS-1 circuit on a DS3XM-6 or DS3XM-12 card you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for a multiplexed DS-3, then choose the DS-1 to test on the multiplexed DS-3. For information about configuring your test set, consult your test set user guide.
- OC-N—If you are testing an OC-N circuit, set the test set for the applicable circuit size. For information about configuring your test set, consult your test set user guide.

Step 10 Verify the integrity of all patch cables that will be used in this test by connecting one end to the test set Tx connector and the other end to the test set Rx connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before continuing.

Step 11 Create a physical loopback at the circuit destination card:

a. Attach one end of a patch cable to the destination port's Tx connector.

b. Attach the other end to the port's Rx connector.

Step 12 At the circuit source card:

a. Connect the Tx connector of the test set to the circuit Rx connector.

b. Connect the test set Rx connector to the circuit Tx connector.

Step 13 Verify that the test set shows a clean signal. If a clean signal does not appear, repeat Steps 6 through 12 to make sure the test set and cabling are configured correctly.

Step 14 Inject BIT errors from the test set. To verify that you have a complete end-to-end circuit, verify that the errors appear at the test set.

Step 15 Complete the "DLP-A356 TCC2/TCC2P Card Active/Standby Switch Test" task on page 20-40.

Step 16 Complete the "DLP-A255 Cross-Connect Card Side Switch Test" task on page 19-38.

Although a service interruption under 60 ms might occur, the test circuit should continue to work before, during, and after the switches. If the circuit stops working, do not continue. Contact your next level of support.

Step 17 From the View menu, choose **Go to Network View**.

Step 18 Click one of the two spans leaving the circuit source node.

Step 19 Complete the "DLP-A94 Path Protection Configuration Protection Switching Test" task on page 17-90 to test the path protection switching function on this span.

Step 20 In network view, click the other circuit source span and repeat Step 19.

Step 21 Set up and complete a BER test. Use the existing configuration and follow your site requirements for the length of time. Record the test results and configuration.

Step 22 Complete the "DLP-A333 Delete Circuits" task on page 20-21 for the test circuit.

Step 23 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete.

Step 24 In network view, click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the alarm information.

Step 25 In network view, click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

b. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export the conditions information.

Step 26 Repeat Steps 6 through 25 for each node that will be a source or destination for circuits traversing the third-party network.

Step 27 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application. Continue with Chapter 6, "Create Circuits and VT Tunnels."

Stop. You have completed this procedure.

NTP-A46 Subtend a Path Protection Configuration from a BLSR

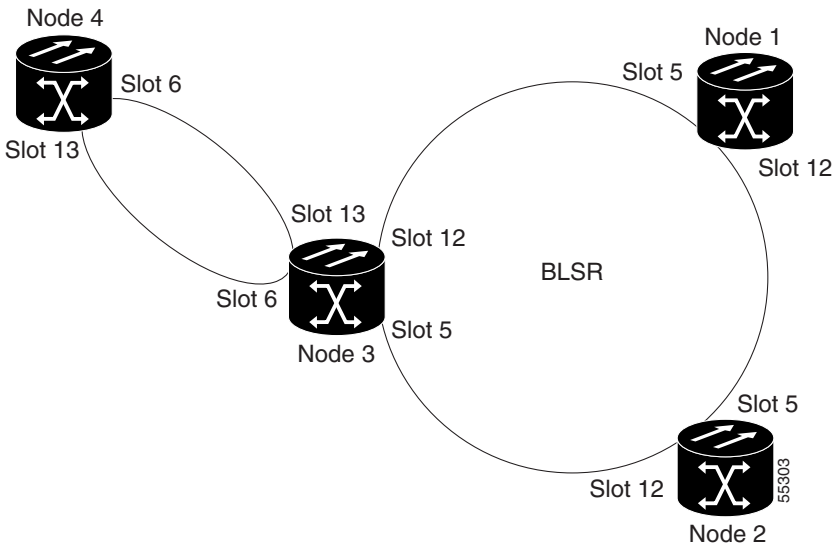
Purpose	This procedure subtends a path protection configuration from an existing BLSR.
Tools/Equipment	One BLSR node must have OC-N cards and fibers to carry the path protection.
Prerequisite Procedures	NTP-A175 Two-Fiber BLSR Acceptance Test, page 5-13 or NTP-A176 Four-Fiber BLSR Acceptance Test, page 5-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note Path protection is the default ONS 15454 topology. It is available as soon as you install the path protection OC-N cards, connect the OC-N fibers, and create the DCC terminations. Unlike the BLSRs, ONS 15454 path protection configurations do not require explicit setup.

Step 1 In the node that will subtend the path protection configuration (Node 3 in Figure 5-12), install the two OC-N cards that will serve as the path protection trunk (span) cards (Node 3, Slots 6 and 13). See the "NTP-A16 Install Optical Cards and Connectors" procedure on page 2-8. If they are already installed, continue with Step 2.

Step 2 Attach fibers from these cards to the path protection trunk cards on the neighbor path protection node or nodes. In Figure 5-12, Node 3/Slot 6 connects to Node 4/Slot 13, and Node 3/Slot 13 connects to Node 4/Slot 6.

Figure 5-12 Path Protection Subtended from a BLSR



Step 3 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the ONS 15454 that will subtend the path protection configuration (Node 3 in the example).

Step 4 Complete the "DLP-A377 Provision Section DCC Terminations" task on page 20-69 for each OC-N card that will carry the path protection configuration. Alternatively, if additional bandwidth is needed for CTC management, complete the"DLP-A378 Provision Line DCC Terminations" task on page 20-71.

Step 5 Log into a path protection node that connects to the node in Step 3. (In Figure 5-12, Node 4 is the only other node in the path protection configuration.)

Step 6 Complete the "DLP-A377 Provision Section DCC Terminations" task on page 20-69 for each OC-N card that will carry the path protection configuration. Alternatively, if additional bandwidth is needed for CTC management, complete the"DLP-A378 Provision Line DCC Terminations" task on page 20-71.

Step 7 Repeat Step 6 for each node in the path protection configuration.

Step 8 As needed, complete the "DLP-A380 Provision a Proxy Tunnel" task on page 20-77.

Step 9 As needed, complete the "DLP-A381 Provision a Firewall Tunnel" task on page 20-78.

Step 10 From the View menu, choose **Go To Network View** to view the subtending rings.

Step 11 Complete the "NTP-A177 Path Protection Acceptance Test" procedure on page 5-22.

Stop. You have completed this procedure.

NTP-A47 Subtend a BLSR from a Path Protection Configuration

Purpose	This procedure subtends a BLSR from an existing path protection configuration.
Tools/Equipment	One path protection node must have OC-N cards and fibers to carry the BLSR
Prerequisite Procedures	NTP-A177 Path Protection Acceptance Test, page 5-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In the path protection node that will subtend the BLSR, install the two OC-N cards that will serve as the BLSR trunk (span) cards (in Figure 5-12, Node 3, Slots 5 and 12). See the "NTP-A16 Install Optical Cards and Connectors" procedure on page 2-8.f

Step 2 Attach fibers from the cards in Step 1 to the BLSR trunk cards on another BLSR node or nodes. In Figure 5-12, Slot 5/Node 3 connects to Slot 12/Node 2, and Slot 12/Node 3 connects to Slot 5/Node 1.

Step 3 Log into the ONS 15454 that will subtend the BLSR (the node in Step 1). See the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 4.

Step 4 Create the DCCs on both OC-N trunk cards (east and west) that will carry the BLSR. See the "DLP-A377 Provision Section DCC Terminations" task on page 20-69. Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-A378 Provision Line DCC Terminations" task on page 20-71.

Step 5 Create the subtending BLSR:

a. Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 5-10 for each node that will be in the BLSR. If you have already provisioned the BLSR, perform this procedure for the subtending node only.

b. Complete the "NTP-A126 Create a BLSR" procedure on page 5-12. Include the node in Step 3 (the node that will subtend the BLSR) in the BLSR.

Step 6 From the View menu, choose **Go to the Network View** to see the subtending ring.

Stop. You have completed this procedure.

NTP-A48 Subtend a BLSR from a BLSR

Purpose	This procedure subtends a BLSR from an existing BLSR.
Tools/Equipment	One BLSR node must have OC-N cards and fibers needed to carry the second BLSR.
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

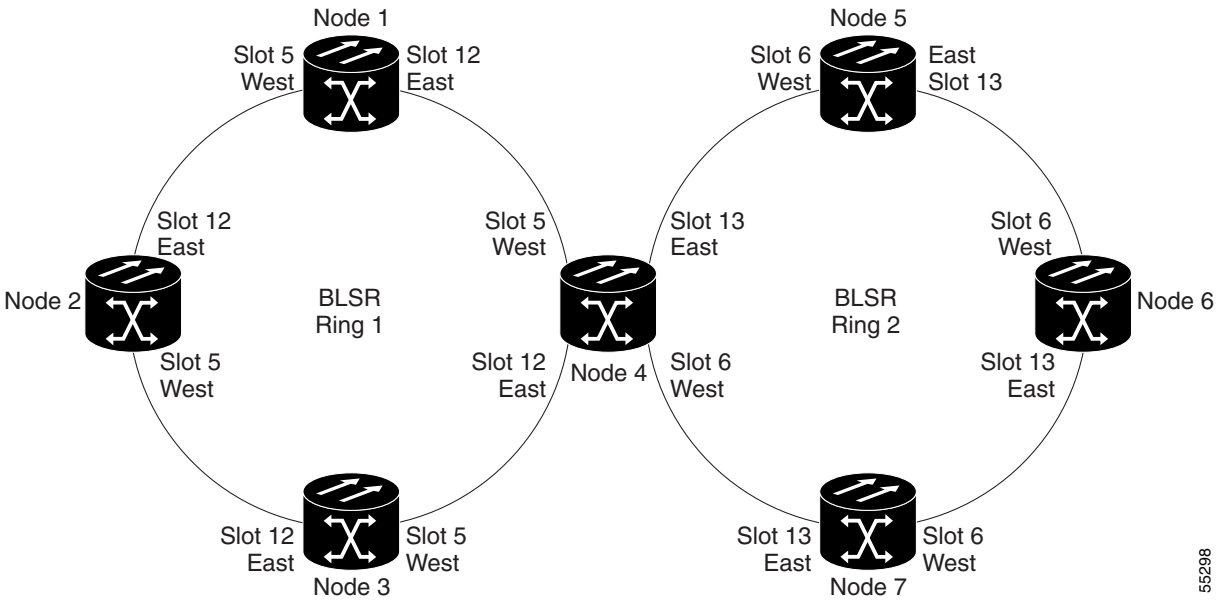
Note This procedure assumes that all nodes are configured for the BLSR. If you need to add a node to a BLSR, see the "NTP-A350 Add a BLSR Node" procedure on page 14-2.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node that will subtend the BLSR (Node 4 in Figure 5-13). If you are already logged in, continue with Step 2.

Step 2 Install the OC-N cards that will serve as the BLSR trunk (span) cards if they are not already installed. See the "NTP-A16 Install Optical Cards and Connectors" procedure on page 2-8.

Figure 5-13 shows two BLSRs shared by one ONS 15454. Ring 1 runs on Nodes 1, 2, 3, and 4. Ring 2 runs on Nodes 4, 5, 6, and 7 and represents the subtending ring added by this procedure. Two BLSR rings, Ring 1 and Ring 2, are provisioned on Node 4. Ring 1 uses cards in Slots 5 and 12, and Ring 2 uses cards in Slots 6 and 13.

Figure 5-13 BLSR Subtended from a BLSR



Step 3 Attach fibers from the trunk cards in the subtending node to the BLSR trunk cards on its two neighboring BLSR nodes. In Figure 5-13, Node 4/Slot 6 connects to Node 7/Slot 13, and Node 4/Slot 13 connects to Node 5/Slot 6. See the "DLP-A44 Install Fiber-Optic Cables for BLSR Configurations" task on page 17-46.

Step 4 Create the DCCs on the first OC-N card that will carry the BLSR. See the "DLP-A377 Provision Section DCC Terminations" task on page 20-69. Alternatively, if additional bandwidth is needed for CTC management, complete the"DLP-A378 Provision Line DCC Terminations" task on page 20-71.

Step 5 Repeat Step 4 for the second OC-N trunk card that will carry the BLSR.

Step 6 Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 5-10 for each node that will be in the BLSR. If you have already provisioned the BLSR, perform this procedure for the subtending node only.

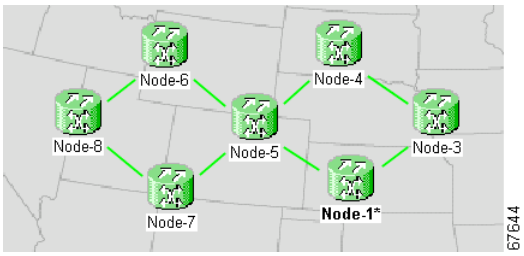
Step 7 If the subtending BLSR is not already created, complete the "NTP-A126 Create a BLSR" procedure on page 5-12 to provision the new BLSR. The subtending BLSR must have a ring name that differs from the ring name of the first BLSR.

Note The subtending node can have one Node ID that is used in both BLSRs, or a different Node ID for each BLSR. For example, the same node can be Node 4 in BLSR 1 and Node 2 in BLSR 2.

Step 8 From the View menu, choose **Go to Network View** to see the subtending ring.

Figure 5-14 shows an example of two subtending BLSRs.

Figure 5-14 Subtended BLSRs on the Network Map



Stop. You have completed this procedure.

NTP-A172 Create a Logical Network Map

Purpose	This procedure positions nodes in the network view and allows a Superuser to create a consistent network view for all nodes on the network.
Tools	None
Prerequisite Procedures	This procedure assumes that network turn-up is complete.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 on an ONS 15454 on the network where you want to create the network map. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Change the position of the nodes in the network view according to your site plan.

- **a.** Click a node to select it, then press the **Ctrl** key while you drag and drop a node icon to a new location.
- **b.** Deselect the previously selected node by clicking on any blank part of the network map area.
- **c.** Repeat Step a for each node you need to position.

Step 4 On the network view map, right-click and choose **Save Node Position**.

Step 5 Click **Yes** in the Save Node Position dialog box.

CTC displays a progress bar and saves the new node positions.

Note Retrieve, Provisioning, and Maintenance users can move nodes on the network map, but only Superusers can save new network map configurations. To restore the view to a previously saved version of the network map, right-click on the network view map and choose Reset Node Position.

Stop. You have completed this procedure.

CHAPTER 6

Create Circuits and VT Tunnels

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter explains how to create Cisco ONS 15454 electrical circuits, tunnels, optical circuits, Ethernet circuits, and virtual concatenated (VCAT) circuits. For additional information about ONS 15454 circuits, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A127 Verify Network Turn Up, page 6-5—Complete this procedure before you create any circuits.
2. NTP-A181 Create an Automatically Routed DS-1 Circuit, page 6-7—Complete as needed.
3. NTP-A182 Create a Manually Routed DS-1 Circuit, page 6-12—Complete as needed.
4. NTP-A183 Create a Unidirectional DS-1 Circuit with Multiple Drops, page 6-15—Complete as needed.
5. NTP-A184 Create an Automatically Routed DS-3 or EC-1 Circuit, page 6-19—Complete as needed.
6. NTP-A185 Create a Manually Routed DS-3 or EC-1 Circuit, page 6-24—Complete as needed.
7. NTP-A186 Create a Unidirectional DS-3 or EC-1 Circuit with Multiple Drops, page 6-27—Complete as needed.
8. NTP-A133 Create an Automatically Routed VT Tunnel, page 6-30—Complete as needed.
9. NTP-A134 Create a Manually Routed VT Tunnel, page 6-33—Complete as needed.
10. NTP-A187 Create a VT Aggregation Point, page 6-35—Complete as needed.
11. NTP-A135 Test Electrical Circuits, page 6-38—Complete this procedure after you create an electrical circuit.

12. NTP-A343 Create an Automatically Routed Optical Circuit, page 6-40—Complete as needed.
13. NTP-A344 Create a Manually Routed Optical Circuit, page 6-45—Complete as needed.
14. NTP-A314 Create a Unidirectional Optical Circuit with Multiple Drops, page 6-48—Complete as needed.
15. NTP-A62 Test Optical Circuits, page 6-51—Complete this procedure after you create an optical circuit.
16. NTP-A139 Create a Half Circuit on a BLSR or 1+1 Node, page 6-53—Complete this procedure as needed to create a half circuit using an OC-N or G-Series card as a destination in a bidirectional line switched ring (BLSR) or 1+1 topology.
17. NTP-A140 Create a Half Circuit on a Path Protection Node, page 6-55—Complete as needed to create a half circuit using an OC-N or G-Series card as a destination in a path protection configuration.
18. NTP-A191 Create an E-Series EtherSwitch Circuit (Multicard or Single-Card Mode), page 6-57—Complete as needed.
19. NTP-A192 Create a Circuit for an E-Series Card in Port-Mapped Mode, page 6-60—Complete as needed.
20. NTP-A142 Create an E-Series Shared Packet Ring Ethernet Circuit, page 6-62—Complete as needed.
21. NTP-A143 Create an E-Series Hub-and-Spoke Ethernet Configuration, page 6-65—Complete as needed.
22. NTP-A144 Create an E-Series Single-Card EtherSwitch Manual Cross-Connect, page 6-67—Complete as needed.
23. NTP-A145 Create an E-Series Multicard EtherSwitch Manual Cross-Connect, page 6-70—Complete as needed.
24. NTP-A146 Test E-Series Circuits, page 6-73—Complete this procedure after creating E-Series SONET circuits.
25. NTP-A148 Create a Manual Cross-Connect for a G-Series or E-Series Card in Port-Mapped Mode, page 6-74—Complete as needed.
26. NTP-A241 Provision G-Series Ports for Transponder Mode, page 6-76—Complete as needed.
27. NTP-A149 Test G-Series Circuits, page 6-79—Complete this procedure after creating G-Series SONET circuits.
28. NTP-A264 Create an Automatically Routed VCAT Circuit, page 6-81—Complete as needed.
29. NTP-A265 Create a Manually Routed VCAT Circuit, page 6-86—Complete as needed.
30. NTP-A194 Create Overhead Circuits, page 6-89—Complete as needed to create data communications channel (DCC) tunnels or IP-encapsulated tunnels, provision orderwire, or create user data channel (UDC) circuits.
31. NTP-A167 Create an STS Test Circuit around the Ring, page 6-90—Complete as needed.
32. NTP-A326 Create a Server Trail, page 6-93—Complete as needed.
33. NTP-A327 Create an Automatically Routed Open-Ended Path Protection Circuit, page 6-94—Complete as needed to create an open-ended path protection circuit.
34. NTP-A361 Create an Overlay Ring Circuit, page 6-98—Complete as needed.
35. NTP-A362 Create an Ethernet Drop and Continue Circuit, page 6-101—Complete as needed.
36. NTP-A363 Create a Dual Source, Single Destination Circuit, page 6-104—Complete as needed.

Table 6-1 defines ONS 15454 circuit creation terms and options.

Table 6-1 ONS 15454 Circuit Options

Circuit Option	Description
Source	The circuit source is where the circuit enters the ONS 15454 network.
Destination	The circuit destination is where the circuit exits an ONS 15454 network.
Automatic circuit routing	Cisco Transport Controller (CTC) routes the circuit automatically on the shortest available path based on routing parameters and bandwidth availability.
Manual circuit routing	Manual routing allows you to choose a specific path, not just the shortest path chosen by automatic routing. You can choose a specific synchronous transport signal (STS) or Virtual Tributary (VT) for each circuit segment and create circuits from work orders prepared by an operations support system (OSS) like the Telcordia Trunk Information Record Keeping System (TIRKS).
VT tunnel	VT tunnels allow VT1.5 circuits to pass through an ONS 15454 without utilizing cross-connect card (XC, XCVT, XC10G, XC-VXC-10G) resources. VT circuits using VT tunnels use cross-connect capacity only at the source and destination nodes. One VT tunnel can carry 28 VT1.5 circuits or 21 VT2 circuits.
VT aggregation point	VT aggregation points (VAPs) allow VT circuits to be aggregated into an STS for handoff to non-ONS 15454 networks or equipment, such as interoffice facilities (IOFs), switches, or digital access and cross-connect systems (DACS). VAPs reduce VT matrix resource utilization at the node where the VTs are aggregated onto the STS. This node is called the STS grooming end. The STS grooming end requires an EC1, DS3, DS3E, DS3/EC1-48, DS3XM-6, DS3XM-12, or OC-N card. VAPs can be created on BLSR, 1+1, or unprotected nodes, but cannot be created on path protection nodes.

ONS 15454 circuits are either VT or STS circuits. Table 6-2 shows the circuit source and destination options for VT circuits.

Table 6-2 CTC Circuit Source and Destination Options for VT Circuits

Card	Ports	STSs	VTs	DS-1s
DS1-14, DS1N-14	—	—	—	14
DS3XM-6	6	—	—	28 per port
DS3XM-12	12	—	—	28 per port
DS3/EC1-48	48	—	—	28 per port
EC1-12	12	—	28 VT1.5s per port, 21 VT2s per port	—
DS1/E1-56	56	—	—	56
OC3 IR 4/STM1 SH 1310	4	3 per port	28 VT1.5s per STS, 21 VT2s per port	—
OC3 IR/STM1 SH 1310-8	8	3 per port	28 VT1.5s per STS, 21 VT2s per port	—

Table 6-2 CTC Circuit Source and Destination Options for VT Circuits (continued)

Card	Ports	STSs	VTs	DS-1s
OC12 IR/STM4 SH 1310 OC12 LR/STM4 LH 1310 OC12 LR/STM4 LH 1550	—	12	28 VT1.5s per STS, 21 VT2s per port	—
OC12 IR/STM4 SH 1310-4	4	12 per port	28 VT1.5s per STS, 21 VT2s per port	—
All OC-48 cards (does not include the ML-Series card)	—	48	28 VT1.5s per STS, 21 VT2s per port	—
All OC-192 cards	—	192	28 VT1.5s per STS, 21 VT2s per port	—
ML-MR-10	10	48 or 192[1]	—	—
CE-MR-10	10	48 or 192[2]	24 VT1.5s per STS	—
FC_MR-4	4	—	—	—
MRC-4	4	3 or 12 per port[3]	28 VT1.5s per STS	—
MRC-12	12	3, 12, or 48 per port[3]	28 VT1.5s per STS, 21 VT2s per port	—

1. The ML-MR-10 card supports 48 STSs when it is installed in Slot 1 to 4 or 14 to 17, and supports 192 STSs when it is installed in Slot 5, 6, 12, or 13.
2. The CE-MR-10 card supports 48 STSs when it is installed in Slot 1 to 4 or 14 to 17, and supports 192 STSs when it is installed in Slot 5, 6, 12, or 13.
3. Dependent on the SFP used in a port, the available backplane width, and existing provisioned lines. For more details, refer to the "Optical Cards" chapter in the *Cisco ONS 15454 Reference Manual*.

Table 6-3 shows the shows the circuit source and destination options for STS circuits.

Table 6-3 CTC Circuit Source and Destination Options for STS Circuits

Card	Ports	STSs
DS1-14, DS1N-14[1]	—	—
DS3-12, DS3N-12, DS3-12E, DS3N-12E	12	—
DS3XM-6	6	—
DS3XM-12	12, or 6 to 12 "portless"[2]	—
DS3i-N-12	12	1 per port
DS3/EC1-48	48	1 per port
EC1-12	12	—
DS1/E1-56	56	—
OC3 IR 4/STM1	4	3 per port

Table 6-3 CTC Circuit Source and Destination Options for STS Circuits (continued)

Card	Ports	STSs
OC3-8	8	3 per port
OC12 IR/STM4 SH 1310 OC12 LR/STM4 LH 1310 OC12 LR/STM4 LH 1550	—	12
OC12 IR/STM4 SH 1310-4	4	12 per port
All OC-48 cards (includes ML-Series card)	—	48
All OC-192 cards (includes ML-MR-10 card)	—	192
CE-MR-10	10	48 or 192[3]
ML-MR-10	10	48 or 192[4]
FC_MC-4	4	—
MRC-4	4	3 or 12 per port[5]
MRC-12	12	3, 12, or 48 per port[5]

1. You can route one STS circuit on a DS1 card to carry all 14 ports within the STS. However, 14 VT1.5s are not utilized.
2. The number of "portless" interfaces depends on the system configuration. For XCVT drop slots, a maximum of 6 portless transmultiplexing interfaces are supported. For XCVT trunk slots and for the XC10G and XC-VXC-10G any slot, a maximum of 12 portless transmultiplexing interfaces are supported.
3. The CE-MR-10 card supports 48 STSs when it is installed in Slot 1 to 4 or 14 to 17, and supports 192 STSs when it is installed in Slot 5, 6, 12, or 13.
4. The CE-MR-10 card supports 48 STSs when it is installed in Slot 1 to 4 or 14 to 17, and supports 192 STSs when it is installed in Slot 5, 6, 12, or 13.
5. Dependent on the SFP used in a port, the available backplane width, and existing provisioned lines. For more details, refer to the "Optical Cards" chapter in the *Cisco ONS 15454 Reference Manual*.

NTP-A127 Verify Network Turn Up

Purpose	This procedure verifies that the ONS 15454 network is ready for circuit provisioning.
Tools/Equipment	None
Prerequisite Procedures	Chapter 5, "Turn Up a Network"
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**. Wait for all the nodes that are part of the network to appear on the network map. (Large networks might take several minutes to display all the nodes.)

Note If this is the first time your computer has connected to this ONS 15454 network, the node icons are stacked on the left side of the graphic area, possibly out of view. Use the scroll bar under the network map to display the icons. To separate the icons, drag and drop the icon to the new location. Repeat until all the nodes are visible on the graphic area.

Step 3 Verify node accessibility. In network view, all node icons must be either green, yellow, orange, or red.

If all network nodes do not appear after a few minutes, or if a node icon is gray with "Unknown" under it, do not continue. Look at the Net box in the lower right corner of the window. If it is gray, log in again, making sure not to check the Disable Network check box in the CTC Login dialog box. If problems persist, see Chapter 5, "Turn Up a Network" to review the network turn-up procedure appropriate for your network topology, or refer to the *Cisco ONS 15454 Troubleshooting Guide* for troubleshooting procedures.

Step 4 Verify DCC connectivity. All nodes must be connected by green lines. If lines are missing or gray in color, do not continue. See Chapter 5, "Turn Up a Network" and follow the network turn-up procedure appropriate for your network topology. Verify that all nodes have DCC connectivity before continuing.

Step 5 Click the **Alarms** tab to view alarm descriptions. Investigate and resolve, if necessary, all critical (red node icon) or major (orange node icon) alarms. Refer to the *Cisco ONS 15454 Troubleshooting Guide* to resolve alarms before continuing.

Step 6 From the View menu, choose **Go to Home View**. Verify that the node is provisioned according to your site or engineering plan:

a. View the cards in the shelf map. Verify that the ONS 15454 cards appear in the specified slots.

b. Click the **Provisioning > General** tabs. Verify that the node name, contacts, date, time, and Network Time Protocol/Simple Network Time Protocol (NTP/SNTP) server IP address (if used) are correctly provisioned. If needed, make corrections using the "NTP-A25 Set Up Name, Date, Time, and Contact Information" procedure on page 4-5.

c. Click the **Network** tab. Verify that the IP address, Subnet Mask, Default Router, Prevent LCD IP Config, and Gateway Settings are correctly provisioned. If not, make corrections using the "NTP-A169 Set Up CTC Network Access" procedure on page 4-8.

d. Click the **Protection** tab. Verify that protection groups are created as specified in your site plan. If the protection groups are not created, complete the "NTP-A324 Create Protection Groups" procedure on page 4-13.

e. If the node is in a BLSR, click the **BLSR** tab. (If the node is not in a BLSR, continue with Step f.) Verify that the following items are provisioned as specified in your site plan:

- BLSR type (2-fiber or 4-fiber)
- BLSR ring ID and node IDs
- Ring reversion time
- East and west card assignments
- 4-fiber BLSRs: Span reversion and east/west protect card assignments

If you need to make corrections, see the "NTP-A40 Provision BLSR Nodes" procedure on page 5-10 for instructions.

f. Click the **Security** tab. Verify that the users and access levels are provisioned as specified. If not, see the "NTP-A30 Create Users and Assign Security" procedure on page 4-4 to correct the information.

g. If Simple Network Management Protocol (SNMP) is used, click the **SNMP** tab and verify the trap and destination information. If the information is not correct, see the "NTP-A87 Change SNMP Settings" procedure on page 11-7 to correct the information.

h. Click the **Comm Channels** tab. Verify that DCCs were created to the applicable OC-N slots and ports (time-division multiplexing [TDM] nodes) or optical service channel (OSC) slots and ports (dense wavelength division multiplexing [DWDM] nodes). If DCCs were not created for the appropriate OC-N or OSC slots and ports, see Chapter 5, "Turn Up a Network" and complete the turn-up procedure appropriate for your network topology. To provision OSC ports, refer to the *Cisco ONS 15454 DWDM Procedure Guide*

i. Click the **Timing** tab. Verify that timing is provisioned as specified. If not, use the "NTP-A85 Change Node Timing" procedure on page 11-6 to make the changes.

j. Click the **Alarm Profiles** tab. If you provisioned optional alarm profiles, verify that the alarms are provisioned as specified. If not, see the "NTP-A71 Create, Download, and Assign Alarm Severity Profiles" procedure on page 8-6 to change the information.

k. Verify that the network element (NE) defaults listed in the status area of the node view window are correct.

Step 7 Repeat Step 6 for each node in the network.

Step 8 Complete the appropriate circuit creation procedure from the NTP list in the "Before You Begin" section on page 6-1.

Stop. You have completed this procedure.

NTP-A181 Create an Automatically Routed DS-1 Circuit

Purpose	This procedure creates an automatically routed DS-1 circuit, meaning that CTC chooses the circuit route based on the parameters you specify and on the software version.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **VT** or **STS**. VT cross-connects will carry the DS-1 circuit across the ONS 15454 network.
- Number of Circuits—Enter the number of DS-1 circuits that you want to create. The default is 1. If you are creating multiple circuits with the same slot and sequential port numbers, you can use Auto-ranged to create the circuits automatically.
- Auto-ranged—This check box is automatically selected if you enter more than 1 in the Number of Circuits field. Auto-ranging creates identical (same source and destination) sequential circuits automatically. Uncheck the box if you do not want CTC to create sequential circuits automatically.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-1):

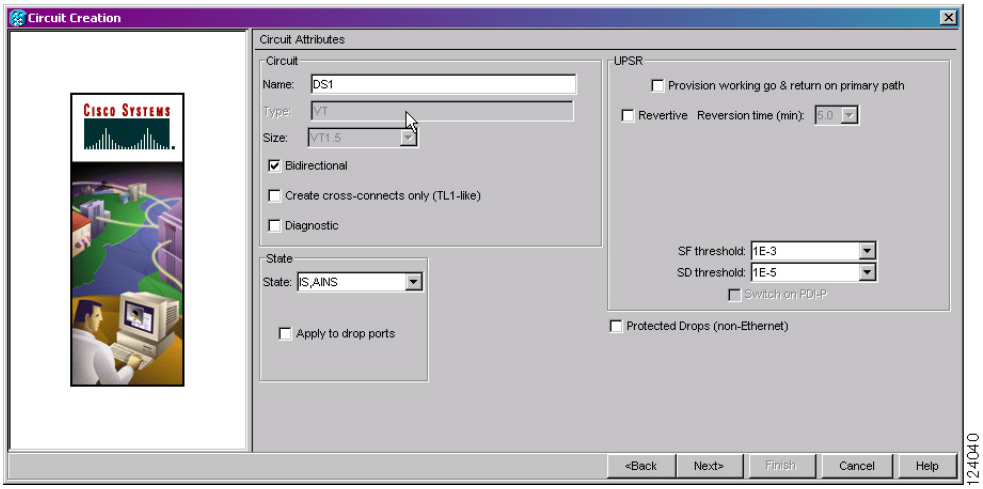
- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters, (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—If the circuit type is VT, choose **VT1.5**. If the circuit type is STS, choose **STS-1**.
- Bidirectional—Leave checked for this circuit (default).
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, VT tunnels and Ethergroup sources and destinations are unavailable.
- Diagnostic—Leave unchecked.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Puts the circuit cross-connects in the In-Service and Normal (IS-NR) service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. Traffic is not passed on the circuit.
  - IS,AINS—Puts the circuit cross-connects in the Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS) service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.

- Protected Drops—Check this box if you want the circuit routed on protected drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, 1+1, or optimized 1+1 protection. If you check this box, CTC displays only protected cards and ports as source and destination choices.

Figure 6-1 Setting Circuit Attributes for a DS-1 Circuit



Step 8 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12. Otherwise, continue with the next step.

Step 9 Click **Next**.

Step 10 Complete the "DLP-A95 Provision a DS-1 Circuit Source and Destination" task on page 17-91.

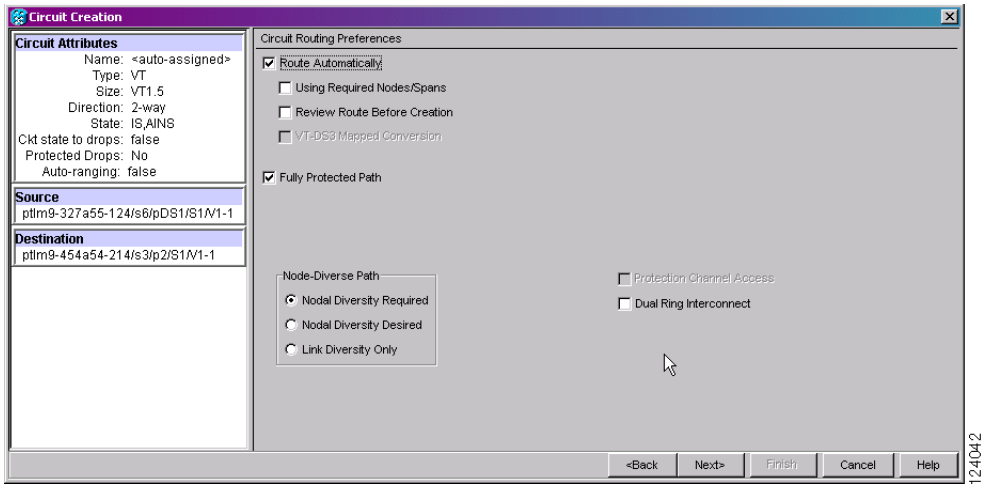
Step 11 In the Circuit Routing Preferences area (Figure 6-2), choose **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- Using Required Nodes/Spans—Check this check box if you want to specify nodes and spans to include or exclude in the CTC-generated circuit route.

  Including nodes and spans for a circuit ensures that those nodes and spans are in the working path of the circuit (but not the protect path). Excluding nodes and spans ensures that the nodes and spans are not in the working or protect path of the circuit.

- Review Route Before Creation—Check this check box if you want to review and edit the circuit route before the circuit is created.

Figure 6-2 Setting Circuit Routing Preferences for a DS-1 Circuit



Step 12 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. CTC creates a fully protected circuit route based on the path diversity option you choose. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 15.

Caution Circuits routed on BLSR protection channels are not protected. They are preempted during BLSR switches.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection configuration, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a BLSR or path protection dual-ring interconnect (DRI), check the **Dual Ring Interconnect** check box.

Step 15 If you checked Using Required Nodes/Spans in Step 11 or Dual Ring Interconnect for a path protection configuration in Step 14, complete the following substeps. If you checked Dual Ring Interconnect for a BLSR, skip this step and continue with Step 16. If you did not select any of these options, continue with Step 17.

a. In the Circuit Constraints for Automatic Routing area, click a node or span on the circuit map.

b. Click **Include** to include the node or span in the circuit. Click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans is the order in which the circuit is routed. Click spans twice to change the circuit direction.

c. Repeat Step b for each node or span you wish to include or exclude.

d. Review the circuit route. To change the circuit routing order, choose a node in the Required Nodes/Lines or Excluded Nodes Links lists and click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 16 Complete the "DLP-A563 Configure an Automatically Routed BLSR DRI" task on page 22-76.

Step 17 Click **Next**. If you are creating VT circuits, in the Create area of the VT Matrix Optimization page choose one of the following options. If not, continue with Step 18.

- Create VT tunnel on transit nodes—This option is available if the DS-1 circuit passes through a node that does not have a VT tunnel, or if an existing VT tunnel is full. VT tunnels allow VT circuits to pass through ONS 15454s without consuming cross-connect card resources. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the *Cisco ONS 15454 Reference Manual* for more information.
- Create VT aggregation point—This option is available if the DS-1 circuit source or destination is on an EC1, DS3, DS3E, DS3i-N-12, DS3/EC1-48, DS3XM-6, DS3XM-12, or OC-N port on a BLSR, 1+1, or unprotected node. VAPs collect DS-1s on an STS for handoff to non-ONS 15454 networks or equipment, such as an IOF, switch, or DACS. It allows VT1.5 circuits to be routed through the node using one STS connection on the cross-connect card matrix rather than multiple VT connections on the cross-connect card VT matrix. If you want to aggregate the DS-1 circuit you are creating with others onto an STS for transport outside the ONS 15454 network, choose one of the following:
  - STS grooming node is *source node,* VT grooming node is *destination node*—Creates the VAP on the DS-1 circuit source node. This option is available only if the DS-1 circuit originates on an EC1, DS3, DS3E, DS3i-N-12, DS3/EC1-48, DS3XM-6, DS3XM-12, or OC-N card.
  - STS grooming node is *destination node*, VT grooming node is *source node*—Creates the VAP on the DS-1 circuit destination node. This option is available only if the DS-1 circuit terminates on an EC1, DS3, DS3E, DS3i-N-12, DS3/EC1-48, DS3XM-6, DS3XM-12, or OC-N card.
- None—Choose this option if you do not want to create a VT tunnel or a VAP. This is the only available option if CTC cannot create a VT tunnel or VAP.

Step 18 If you selected Review Route Before Creation in Step 11, complete the following substeps. If not, continue with Step 19.

a. Click **Next**.

b. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the "NTP-A182 Create a Manually Routed DS-1 Circuit" procedure on page 6-12.

Step 19 Click **Finish**. One of the following results occurs if you entered more than one circuit in the Number of Circuits field on the Circuit Creation dialog box.

- If you chose Auto-ranged, CTC automatically creates the number of circuits entered in the Number of Circuits field. If auto-ranging cannot complete all the circuits, for example, because sequential ports are unavailable at the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto-ranging. After completing the circuits, the Circuits window appears.
- If you did not choose Auto-ranged, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 5 through 18 for each additional circuit. After completing the circuits, the Circuits window appears.

Step 20 In the Circuits window, verify that the new circuits appear in the circuits list.

Step 21 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 6-38. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-A182 Create a Manually Routed DS-1 Circuit

Purpose	This procedure creates a DS-1 circuit and allows you to provision the circuit route.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **VT** or **STS**. VT cross-connects will carry the DS-1 circuit across the ONS 15454 network.
- Number of Circuits—Enter the number of DS-1 circuits that you want to create. The default is 1.
- Auto-ranged—(Automatically routed circuits only) If you entered more than 1 in the Number of Circuits field on the Circuit Creation dialog box, uncheck this box. (The box is unavailable if only one circuit is entered in the Number of Circuits field.)

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-1 on page 6-9):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.

- Size—If the circuit type is VT, choose **VT1.5**. If the circuit type is STS, choose **STS-1**.
- Bidirectional—Leave checked for this circuit (default).
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, VT tunnels and Ethergroup sources and destinations are unavailable.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Puts the circuit cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

  Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.

- Protected Drops—Check this box if you want the circuit routed on protected drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, 1+1, or optimized 1+1 protection. If you check this box, CTC shows only protected cards and ports as source and destination choices.

Step 8 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12. Otherwise, continue with the next step.

Step 9 Click **Next**.

Step 10 Complete the "DLP-A95 Provision a DS-1 Circuit Source and Destination" task on page 17-91.

Step 11 In the Circuit Routing Preferences area (Figure 6-2 on page 6-10), uncheck **Route Automatically**.

Step 12 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 16.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path,** check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 16.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection configuration, choose a Node-Diverse Path option:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired— Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection DRI or BLSR DRI, check the **Dual Ring Interconnect** check box.

Step 15 Click **Next**. In the Create area of the VT Matrix Optimization page, choose one of the following:

- Create VT tunnel on transit nodes—This option is available if the DS-1 circuit passes through a node that does not have a VT tunnel, or if an existing VT tunnel is full. VT tunnels allow VT circuits to pass through ONS 15454s without consuming cross-connect card resources. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the *Cisco ONS 15454 Reference Manual* for more information.
- Create VT aggregation point—This option is available if the DS-1 circuit source or destination is on an EC1, DS3, DS3E, DS3i-N-12, DS3/EC1-48, DS3XM-6, DS3XM-12, or OC-N port on a BLSR, 1+1, or unprotected node. VAPs collect DS-1s on an STS for handoff to non-ONS 15454 networks or equipment, such as an IOF, switch, or DACS. It allows VT1.5 circuits to be routed through the node using one STS connection on the cross-connect card matrix rather than multiple VT connections on the cross-connect card VT matrix. If you want to aggregate the DS-1 circuit you are creating with others onto an STS for transport outside the ONS 15454 network, choose one of the following:
  - STS grooming node is *source node*, VT grooming node is *destination node*—Creates the VAP on the DS-1 circuit source node. This option is available only if the DS-1 circuit originates on an EC1, DS3, DS3E, DS3i-N-12, DS3XM-6, DS3XM-12, or OC-N card.
  - STS grooming node is *destination node*, VT grooming node is *source node*—Creates the VAP on the DS-1 circuit destination node. This option is available only if the DS-1 circuit terminates on an EC1, DS3, DS3E, DS3i-N-12, DS3XM-6, DS3XM-12, or OC-N card.
- None—Choose this option if you do not want to create a VT tunnel or a VAP. This is the only available option if CTC cannot create a VT tunnel or VAP.

Step 16 Click **Next**. In the Route Review/Edit area, node icons appear for you to route the circuit manually. If you checked Dual Ring Interconnect for BLSR, continue with Step 17. If not, continue with Step 16.

Step 17 Complete the "DLP-A564 Configure a Manually Routed BLSR DRI" task on page 22-78.

Step 18 Complete the "DLP-A96 Provision a DS-1 or DS-3 Circuit Route" task on page 17-92 for the DS-1 circuit you are creating.

Step 19 Click **Finish**. CTC compares your manually provisioned circuit route with the specified path diversity option you chose in Step 13. If the path does not meet the specified path diversity requirement, CTC displays an error message and allows you to change the circuit path.

Step 20 If you entered more than 1 in the Number of Circuits field on the Circuit Creation dialog box, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 5 through 19 for each additional circuit.

Step 21 When all the circuits are created, the main Circuits window appears. Verify that the circuits you created are correct.

Step 22 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 6-38. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-A183 Create a Unidirectional DS-1 Circuit with Multiple Drops

Purpose	This procedure creates a unidirectional DS-1 circuit with multiple drops (destinations).
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **VT** or **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable when the Number of Circuits field is 1.

Step 6 Click **Next**.

Step 7 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—If the circuit type is VT, choose **VT1.5**. If the circuit type is STS, choose **STS-1**.
- Bidirectional—Uncheck for this circuit.

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, VT tunnels and Ethergroup sources and destinations are unavailable.
- Diagnostic—Leave unchecked.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Puts the circuit cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

  Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.
- Protected Drops—Check this box if you want the circuit routed to protect drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, 1+1, or optimized 1+1 protection. If you check this box, CTC displays only protected cards as source and destination choices.

Step 8 Click **Next**.

Step 9 Complete the "DLP-A95 Provision a DS-1 Circuit Source and Destination" task on page 17-91.

Step 10 In the Circuit Routing Preferences area, uncheck **Route Automatically**. When Route Automatically is not selected, the Using Required Nodes/Spans and Review Route Before Circuit Creation check boxes are unavailable.

Step 11 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 12. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 17.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 17.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 12 If you selected Fully Protected Path in Step 11 and the circuit will be routed on a path protection configuration, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 13 If you selected Fully Protected Path in Step 11 and the circuit will be routed on a BLSR DRI or path protection DRI, click the **Dual Ring Interconnect** check box.

Step 14 Click **Next**. In the Create area of the VT Matrix Optimization page, choose one of the following:

- Create VT tunnel on transit nodes—This option is available if the DS-1 circuit passes through a node that does not have a VT tunnel, or if an existing VT tunnel is full. VT tunnels allow VT circuits to pass through ONS 15454s without consuming cross-connect card resources. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the *Cisco ONS 15454 Reference Manual* for more information.
- Create VT aggregation point—This option is available if the DS-1 circuit source or destination is on an EC1, DS3, DS3E, DS3i-N-12, DS3/EC1-48, DS3XM-6, DS3XM-12, or OC-N port on a BLSR, 1+1, or unprotected node. VAPs collect DS-1s on an STS for handoff to non-ONS 15454 networks or equipment, such as an IOF, switch, or DACS. It allows VT1.5 circuits to be routed through the node using one STS connection on the cross-connect card matrix rather than multiple VT connections on the cross-connect card VT matrix. If you want to aggregate the DS-1 circuit you are creating with others onto an STS for transport outside the ONS 15454 network, choose one of the following:
  - STS grooming node is *source node*, VT grooming node is *destination node*—Creates the VAP on the DS-1 circuit source node. This option is available only if the DS-1 circuit originates on an EC1, DS3, DS3E, DS3i-N-12, DS3XM-6, DS3XM-12, or OC-N card.
  - STS grooming node is *destination node*, VT grooming node is *source node*—Creates the VAP on the DS-1 circuit destination node. This option is available only if the DS-1 circuit terminates on an EC1, DS3, DS3E, DS3i-N-12, DS3XM-6, DS3XM-12, or OC-N card.
- None—Choose this option if you do not want to create a VT tunnel or a VAP. This is the only available option if CTC cannot create a VT tunnel or VAP.

Step 15 Click **Next**. In the Route Review/Edit area, node icons appear for you to route the circuit manually. If you checked Dual Ring Interconnect for BLSR, continue with Step 16. If not, continue with Step 17.

Step 16 Complete the "DLP-A564 Configure a Manually Routed BLSR DRI" task on page 22-78.

Step 17 Complete the "DLP-A96 Provision a DS-1 or DS-3 Circuit Route" task on page 17-92 for the DS-1 circuit you are creating.

Step 18 Click **Finish**. CTC completes the circuit and the Circuits window appears.

Step 19 In the Circuits window, click the circuit that you want to route to multiple drops. The Delete, Edit, and Search buttons become active.

Step 20 Click **Edit** (or double-click the circuit row). The Edit Circuit window appears with the General tab selected.

All nodes in the DCC network appear on the network map. Circuit source and destination information appears under the source and destination nodes. To see a detailed view of the circuit, click **Show Detailed Map**. To rearrange a node icon, select the node, press **Ctrl**, then drag and drop the icon to the new location.

Step 21 In the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops appears.

Step 22 Click **Create**.

Step 23 In the Define New Drop dialog box, create the new drop:

a. Node—Choose the target node for the circuit drop.

b. Slot—Choose the target card and slot.

c. Port, STS, VT, or DS1—Choose the port, STS, VT, or DS-1 from the Port, STS, VT, or DS1 drop-down lists. The card you chose in Step b determines the fields that appear. See Table 6-2 on page 6-3 for a list of options.

d. The routing preferences for the new drop match those of the original circuit. However, if the following options are available, you can modify them:

- If the original circuit was routed on a protected path protection path, you can change the nodal diversity options: Nodal Diversity Required, Nodal Diversity Desired, or Link Diversity Only. See Step 12 for the option descriptions.
- If the original circuit was not routed on a protected path, the Protection Channel Access option is available. See Step 11 for a description of the PCA option.

e. If you want to change the circuit state, choose the circuit state from the Target Circuit Admin State drop-down list. The state chosen applies to the entire circuit.

f. Check **Apply to drop ports** if you want to apply the state chosen in the Target Circuit Admin State to the circuit source and destination drops. For the requirements necessary to apply a service state to drop ports, refer to the *Cisco ONS 15454 Reference Manual*.

g. Click **Finish**. The new drop appears in the Drops list.

Step 24 If you need to create additional drops for the circuit, repeat Steps 22 and 23 to create the additional drops.

Step 25 Click **Close**. The Circuits window appears.

Step 26 Verify that the new drops appear in the Destination column for the circuit you edited. If they do not appear, repeat Steps 5 through 25, making sure all options are provisioned correctly.

Step 27 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 6-38. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-A184 Create an Automatically Routed DS-3 or EC-1 Circuit

Purpose	This procedure creates an automatically routed DS-3 or EC-1 circuit and also gives you the option of creating a circuit over a pair of portless transmultiplexing interfaces. CTC routes the circuit automatically based on circuit creation parameters and the software version.
Tools/Equipment	For portless transmultiplexing configurations, a DS3XM-12 must be installed on a node through which the circuit will be routed. For VT2 circuits, the following cards must be installed at the circuit source and destination nodes: XC-VXC-10G and EC1.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **VT** or **STS**. STS cross-connects will carry the DS-3 or EC-1 circuit across the ONS 15454 network.
- Number of Circuits—Enter the number of DS-3 or EC-1 circuits that you want to create. The default is 1. If you are creating multiple circuits with sequential source and destination ports, you can use Auto-ranged to create the circuits automatically.
- Auto-ranged—This box is automatically selected if you enter more than 1 in the Number of Circuits field. Leave selected if you are creating multiple DS-3 or EC-1 circuits with the same source and destination and you want CTC to create the circuits automatically. Uncheck the box if you do not want CTC to create sequential circuits automatically.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-3):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—For circuits on the DS3i-N-12 card, choose **STS-3c**. This sets a port group for Ports 1, 4, 7, and 10 using three ports at any given time. For VT2 circuits on the EC1 card, choose **VT2**. For all other circuits, choose **STS-1**.

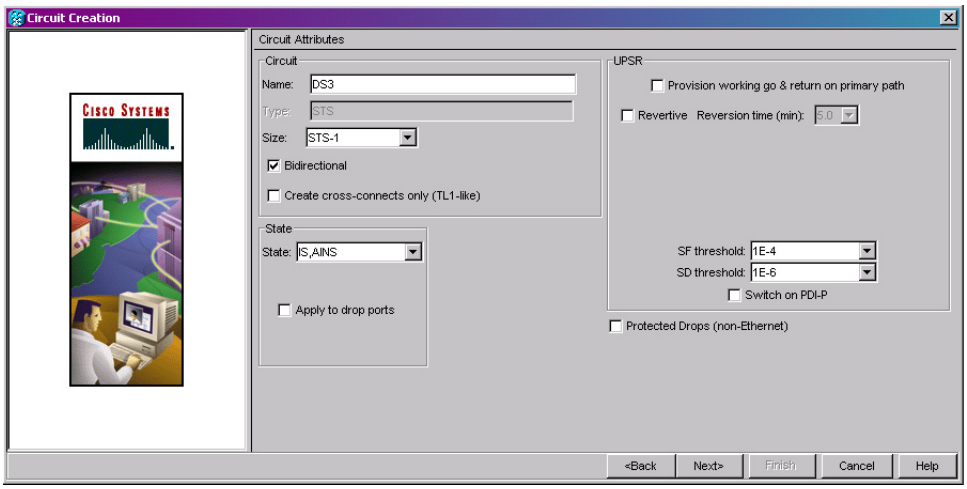
- Bidirectional—Leave checked for this circuit (default).
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, VT tunnels and Ethergroup sources and destinations are unavailable.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Puts the circuit cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 5454 Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.

- Protected Drops—Check this box if you want the circuit routed on protected drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, 1+1, or optimized 1+1 protection. If you check this box, CTC provides only protected cards and ports as source and destination choices.

Figure 6-3 Setting Circuit Attributes for a DS-3 or EC-1 Circuit



Step 8 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12.

Step 9 Click **Next**.

Step 10 Complete the "DLP-A510 Provision a DS-3 Circuit Source and Destination" task on page 22-4.

Step 11 In the Circuit Routing Preferences area (Figure 6-4), choose **Route Automatically**. Three options are available; choose based on your preferences:

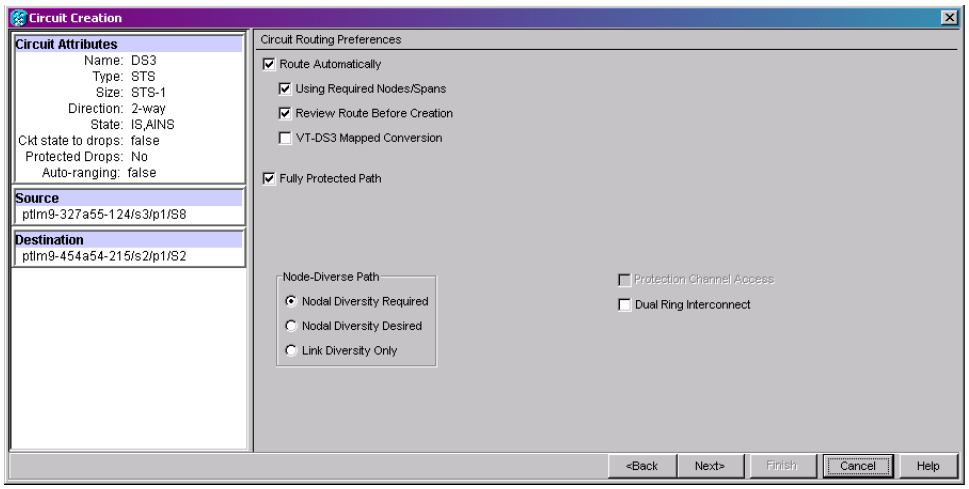
- Using Required Nodes/Spans—Check this check box to specify nodes and spans to include or exclude in the CTC-generated circuit route.

  Including nodes and spans for a circuit ensures that those nodes and spans are in the working path of the circuit (but not the protect path). Excluding nodes and spans ensures that the nodes and spans are not in the working or protect path of the circuit.

- Review Route Before Creation—Check this check box to review and edit the circuit route before the circuit is created.

- VT-DS3 Mapped Conversion—Check this check box to create a circuit using the portless transmultiplexing interface of the DS3XM-12 card.

Figure 6-4 Setting Circuit Routing Preferences for a DS-3 or EC-1 Circuit



Step 12 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. CTC creates a fully protected circuit route based on the path diversity option you choose. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 15.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection configuration, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a BLSR DRI or path protection DRI, check the **Dual Ring Interconnect** check box.

Step 15 If you selected VT-DS3 Mapped Conversion in Step 11, complete the following substeps; otherwise, continue with Step 16:

a. Click **Next**.

b. In the Conversion Circuit Route Constraints area, complete the following:

- Node—Choose a node with a DS3XM-12 card installed.

- Slot—Choose the slot where a DS3XM-12 card is installed.
- DS3 Mapped STS—If applicable, choose **Circuit Dest** to indicate that the STS is the circuit destination, or **Circuit Source** to indicate that the STS is the circuit source.

Step 16 If you checked Using Required Nodes/Spans in Step 11 or Dual Ring Interconnect for a path protection configuration in Step 14, complete the following substeps. If you checked Dual Ring Interconnect for a BLSR, skip this step and continue with Step 17. If you did not select any of these options, continue with Step 18.

a. In the Circuit Constraints for Automatic Routing area, click a node or span on the circuit map.

b. Click **Include** to include the node or span in the circuit. Click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans is the order in which the circuit is routed. Click spans twice to change the circuit direction.

c. Repeat Step b for each node or span you wish to include or exclude.

d. Review the circuit route. To change the circuit routing order, choose a node in the Required Nodes/Lines or Excluded Nodes Links lists and click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 17 Complete the "DLP-A563 Configure an Automatically Routed BLSR DRI" task on page 22-76.

Step 18 Click **Next**. If you are creating VT circuits, in the Create area of the VT Matrix Optimization page choose one of the following options. If not, continue with Step 18.

- Create VT tunnel on transit nodes—This option is available if the DS-1 circuit passes through a node that does not have a VT tunnel, or if an existing VT tunnel is full. VT tunnels allow VT circuits to pass through ONS 15454s without consuming cross-connect card resources. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the *Cisco ONS 15454 Reference Manual* for more information.
- Create VT aggregation point—This option is available if the DS-1 circuit source or destination is on an EC1, DS3, DS3E, DS3i-N-12, DS3/EC1-48, DS3XM-6, DS3XM-12, or OC-N port on a BLSR, 1+1, or unprotected node. VAPs collect DS-1s on an STS for handoff to non-ONS 15454 networks or equipment, such as an IOF, switch, or DACS. It allows VT1.5 circuits to be routed through the node using one STS connection on the cross-connect card matrix rather than multiple VT connections on the cross-connect card VT matrix. If you want to aggregate the DS-1 circuit you are creating with others onto an STS for transport outside the ONS 15454 network, choose one of the following:
  - STS grooming node is *source node,* VT grooming node is *destination node*—Creates the VAP on the DS-1 circuit source node. This option is available only if the DS-1 circuit originates on an EC1, DS3, DS3E, DS3i-N-12, DS3/EC1-48, DS3XM-6, DS3XM-12, or OC-N card.
  - STS grooming node is *destination node*, VT grooming node is *source node*—Creates the VAP on the DS-1 circuit destination node. This option is available only if the DS-1 circuit terminates on an EC1, DS3, DS3E, DS3i-N-12, DS3/EC1-48, DS3XM-6, DS3XM-12, or OC-N card.
- None—Choose this option if you do not want to create a VT tunnel or a VAP. This is the only available option if CTC cannot create a VT tunnel or VAP.

Step 19 Click **Next**. If you selected Review Route Before Creation in Step 11, complete the following substeps; otherwise, continue with Step 20.

a. Click **Next**.

b. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the "NTP-A185 Create a Manually Routed DS-3 or EC-1 Circuit" procedure on page 6-24.

Step 20 Click **Finish**. One of the following occurs if you entered more than 1 in the Number of Circuits field on the Circuit Creation dialog box:

- If you chose Auto-ranged, CTC automatically creates the number of circuits entered in the Number of Circuits field. If auto-ranging cannot complete all the circuits, for example, because sequential ports are unavailable at the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto-ranging. After completing the circuits, the Circuits window appears.
- If you did not choose Auto-ranged, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 5 through 19 for each additional circuit. After completing the circuits, the Circuits window appears.

Step 21 In the Circuits window, verify that the circuits you just created appear in the circuits list.

Step 22 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 6-38. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-A185 Create a Manually Routed DS-3 or EC-1 Circuit

Purpose	This procedure creates a DS-3 or EC-1 circuit and allows you to provision the circuit route.
Tools/Equipment	For VT2 circuits, the following cards must be installed at the circuit source and destination nodes: XC-VXC-10G and EC1.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 3.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 4.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **STS**. STS cross-connects will carry the DS-3 or EC-1 circuit across the ONS 15454 network.
- Number of Circuits—Enter the number of DS-3 or EC-1 circuits that you want to create. The default is 1.

- Auto-ranged—(Automatically routed circuits only) If you entered more than 1 in the Number of Circuits field, uncheck this box. (The box is unavailable if only one circuit is entered in the Number of Circuits field.)

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-3 on page 6-21):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave this field blank, CTC assigns a default name to the circuit.
- Size—For circuits on the DS3i-N-12 card, choose **STS-3c**. This sets a port group for Ports 1, 4, 7, and 10 using three ports at any given time. For VT2 circuits on the EC1 card, choose **VT2**. For all other circuits, choose **STS-1**.
- Bidirectional—Leave this field checked (default).
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, VT tunnels and Ethergroup sources and destinations are unavailable.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Puts the circuit cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

  Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.
- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, 1+1, or optimized 1+1 protection. If you check this check box, CTC provides only protected cards as source and destination choices.

Step 8 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12.

Step 9 Click **Next**.

Step 10 Complete the "DLP-A510 Provision a DS-3 Circuit Source and Destination" task on page 22-4.

Step 11 In the Circuit Routing Preferences area (Figure 6-4 on page 6-22), uncheck **Route Automatically**. When Route Automatically is not selected, the Using Required Nodes/Spans, Review Route Before Circuit Creation, and VT-DS3 Mapped Conversion check boxes are unavailable.

Step 12 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 17.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 17.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection configuration, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection DRI or BLSR DRI, click the **Dual Ring Interconnect** check box.

Step 15 Click **Next**. In the Route Review/Edit area, node icons appear for you to route the circuit manually. If you checked Dual Ring Interconnect for BLSR, continue with Step 16. If not, continue with Step 17.

Step 16 Complete the "DLP-A564 Configure a Manually Routed BLSR DRI" task on page 22-78.

Step 17 In the Route Review and Edit area, node icons appear so you can route the circuit manually. The green arrows pointing from the selected node to other network nodes indicate spans that are available for routing the circuit.

Step 18 Complete the "DLP-A96 Provision a DS-1 or DS-3 Circuit Route" task on page 17-92 for the DS-3 or EC-1 you are creating.

Step 19 Click **Finish**.

Step 20 If you entered more than 1 in the Number of Circuits field on the Circuit Creation dialog box, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 5 through 19 for each additional circuit.

Step 21 When all the circuits are created, the main Circuits window appears. Verify that the circuits you created appear in the window.

Step 22 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 6-38. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-A186 Create a Unidirectional DS-3 or EC-1 Circuit with Multiple Drops

Purpose	This procedure creates a unidirectional DS-3 or EC-1 circuit with multiple drops.
Tools/Equipment	For VT2 circuits, the following cards must be installed at the circuit source and destination nodes: XC-VXC-10G and EC1.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable when the Number of Circuits field is 1.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-5):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—For circuits on the DS3i-N-12 card, choose **STS-3c**. For VT2 circuits on the EC1 card, choose **VT2**. For all other circuits, choose **STS-1**.
- Bidirectional—Uncheck for this circuit.
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, VT tunnels and Ethergroup sources and destinations are unavailable.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Puts the circuit cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.

- IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
- OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

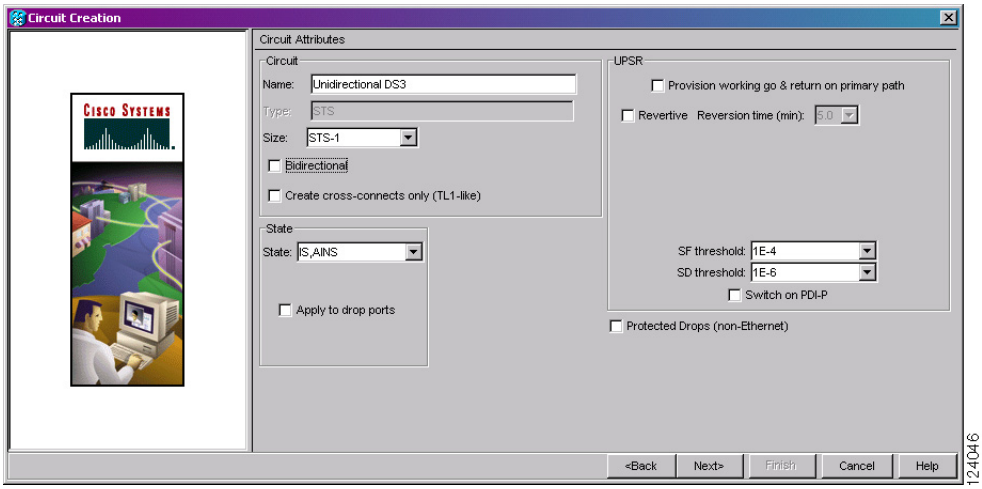
For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.

- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.

- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, 1+1, or optimized 1+1 protection. If you check this check box, CTC provides only protected cards as source and destination choices.

Figure 6-5 Setting Circuit Attributes for a Unidirectional DS-3 or EC-1 Circuit



Step 8 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12.

Step 9 Click **Next**.

Step 10 Complete the "DLP-A510 Provision a DS-3 Circuit Source and Destination" task on page 22-4.

Step 11 Uncheck **Route Automatically**. When Route Automatically is not selected, the Using Required Nodes/Spans, Review Route Before Circuit Creation, and VT-DS3 Mapped Conversion check boxes are unavailable.

Step 12 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 15.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection configuration, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a BLSR DRI or path protection DRI, check the **Dual Ring Interconnect** check box.

Step 15 Click **Next**. In the Route Review/Edit area, node icons appear for you to route the circuit manually. If you checked Dual Ring Interconnect for BLSR, continue with Step 16. If not, continue with Step 17.

Step 16 Complete the "DLP-A564 Configure a Manually Routed BLSR DRI" task on page 22-78.

Step 17 Complete the "DLP-A96 Provision a DS-1 or DS-3 Circuit Route" task on page 17-92 for the DS-3 or EC-1 you are creating.

Step 18 Click **Finish**. After completing the circuit, the Circuits window appears.

Step 19 In the Circuits window, click the circuit that you want to route to multiple drops. The Delete, Edit, and Search radio buttons become active.

Step 20 Click **Edit**. The Edit Circuit window appears with the General tab selected. All nodes in the DCC network appear on the network map. Circuit source and destination information appears under the source and destination nodes. To see a detailed view of the circuit, click **Show Detailed Map**. You can rearrange the node icons by selecting the node with the left mouse button while simultaneously pressing **Ctrl**, then dragging the icon to the new location.

Step 21 In the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops appears.

Step 22 Click **Create**.

Step 23 In the Define New Drop dialog box, define the new drop:

a. Node—Choose the target node for the circuit drop.

b. Slot—Choose the target card and slot.

c. Port, STS—Choose the port and/or STS from the Port and STS drop-down lists. The card selected in Step b determines whether port, STS, or both appear. See Table 6-2 on page 6-3 for a list of options.

d. The routing preferences for the new drop match those of the original circuit. However, if the following options are available, you can modify them:
   - If the original circuit was routed on a protected path protection path, you can change the nodal diversity options: Nodal Diversity Required, Nodal Diversity Desired, or Link Diversity Only. See Step 13 for option descriptions.
   - If the original circuit was not routed on a protected path, the Protection Channel Access option is available. See Step 12 for a description of the PCA option.

e. If you want to change the circuit state, choose the circuit state from the Target Circuit Admin State drop-down list. The state chosen applies to the entire circuit.

f. Check **Apply to drop ports** if you want to apply the state chosen in the Target Circuit Admin State to the circuit source and destination drops. For the requirements necessary to apply a service state to drop ports, refer to the *Cisco ONS 15454 Reference Manual*.

g. Click **Finish**. The new drop appears in the Drops list.

Step 24 If you need to create additional drops for the circuit, repeat Steps 22 and 23 to create the additional drops.

Step 25 Click **Close**. The Circuits window appears.

Step 26 Verify that the new drops appear in the Destination column for the circuit you edited. If they do not appear, repeat Steps 22 through 25, making sure that all options are provisioned correctly.

Step 27 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 6-38. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-A133 Create an Automatically Routed VT Tunnel

Purpose	This procedure creates an automatically routed VT tunnel from source to destination nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Note VT tunnels allow VT circuits to pass through intermediary ONS 15454s without consuming VT matrix resources on the cross-connect card. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual* for more information.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to create the VT tunnel. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, choose **VT Tunnel** from the Circuit Type list.

Step 6 Click **Next**.

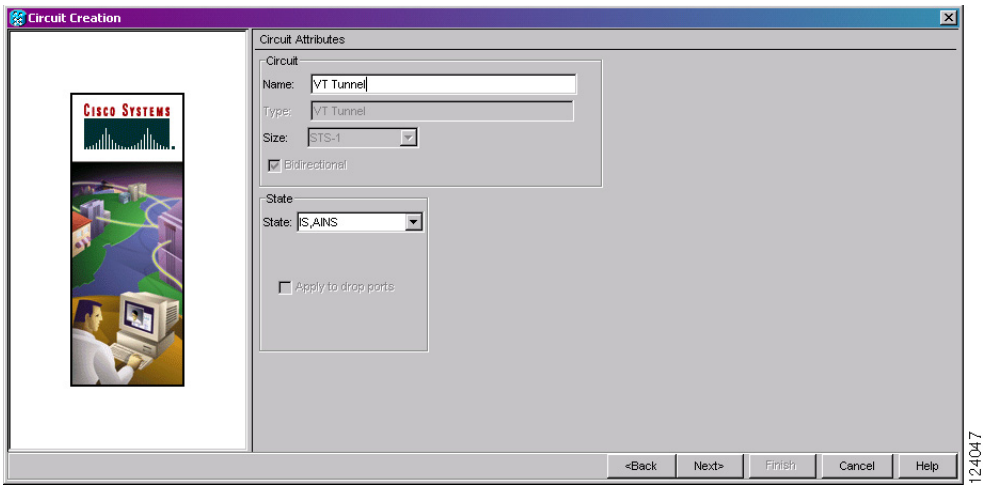
Step 7 Define the circuit attributes (Figure 6-6):

- Name—Assign a name to the VT tunnel. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the tunnel.
- Size—Unavailable for VT tunnels.
- Bidirectional—Unavailable for VT tunnels.
- State—Choose the administrative state to apply to all of the cross-connects in the VT tunnel:
  - IS—Puts the circuit cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

  Note A VT tunnel automatically transitions into the IS service state after a VT circuit is created.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Apply to drop ports—Unavailable for VT tunnels.

Figure 6-6 Setting Attributes for a VT Tunnel



Step 8 Click **Next**.

Step 9 In the Circuit Source area, choose the node where the VT tunnel will originate from the Node drop-down list.

Step 10 Click **Next**.

Step 11 In the Circuit Destination area, choose the node where the VT tunnel will terminate from the Node drop-down list.

Step 12 Click **Next**.

Step 13 In the Circuit Routing Preferences area, choose **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- Using Required Nodes/Spans—Check this check box to specify nodes and spans to include or exclude in the CTC-generated tunnel route.

  Including nodes and spans for a circuit ensures that those nodes and spans are in the working path of the circuit (but not the protect path). Excluding nodes and spans ensures that the nodes and spans are not in the working or protect path of the circuit.

- Review Route Before Creation—Check this check box to review and edit the VT tunnel route before the circuit is created. Proceed to Step 15.

Step 14 If you selected Using Required Nodes/Spans in Step 13:

a. Click **Next**.

b. In the Circuit Route Constraints area, click a span on the VT tunnel map.

c. Click **Include** to include the node or span in the VT tunnel. Click **Exclude** to exclude the node or span from the VT tunnel. The order in which you choose included nodes and spans sets the VT tunnel sequence. Click spans twice to change the circuit direction.

d. Repeat Steps b and c for each node or span you wish to include or exclude.

e. Review the VT tunnel route. To change the tunnel routing order, choose a node in the Required Nodes/Lines or Excluded Nodes Links lists, then click the **Up** or **Down** buttons to change the tunnel routing order. Click **Remove** to remove a node or span. Proceed to Step 16.

Step 15 If you selected Review Route Before Creation in Step 13:

a. Click **Next**.

b. Review the tunnel route. To add or delete a tunnel span, choose a node on the tunnel route. Blue arrows show the tunnel route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned tunnel does not reflect the routing and configuration you want, click **Back** to verify and change tunnel information.

Step 16 Click **Finish**. The Circuits window appears.

Step 17 Verify that the tunnel you just created appears in the circuits list. VT tunnels are identified by VTT in the Type column.

Stop. You have completed this procedure.

NTP-A134 Create a Manually Routed VT Tunnel

Purpose	This procedure creates a manually routed VT tunnel from source to destination nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note VT tunnels allow VT circuits to pass through intermediary ONS 15454s without consuming VT matrix resources on the cross-connect card. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual* for more information.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the VT tunnel. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, choose **VT Tunnel** from the Circuit Type list.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-6 on page 6-32):

- Name—Assign a name to the VT tunnel. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the tunnel.
- Size—Unavailable for VT tunnels.
- Bidirectional—Unavailable for VT tunnels.
- State—Choose the administrative state to apply to all of the cross-connects in the VT tunnel:

- IS—Puts the circuit cross-connects in the IS-NR service state.
- OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
- IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
- OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

Note A VT tunnel automatically transitions into the IS service state after a VT circuit is created.

For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.

- Apply to drop ports—Unavailable for VT tunnels.

Step 8 Click **Next**.

Step 9 In the Circuit Source area, choose the node where the VT tunnel will originate from the Node drop-down list.

Step 10 Click **Next**.

Step 11 In the Circuit Destination area, choose the node where the VT tunnel will terminate from the Node drop-down list.

Step 12 Click **Next**.

Step 13 In the Circuit Routing Preferences area, uncheck **Route Automatically**.

Step 14 Click **Next**. In the Route Review and Edit area, node icons appear so you can route the tunnel. The circuit source node is selected. Green arrows pointing from the source node to other network nodes indicate spans that are available for routing the tunnel.

Step 15 Complete the "DLP-A219 Provision a VT Tunnel Route" task on page 19-13 for the tunnel you are creating. The Circuits window appears.

Step 16 Verify that the tunnel you just created appears in the circuits list. VT tunnels are identified by VTT in the Type column.

Stop. You have completed this procedure.

NTP-A187 Create a VT Aggregation Point

Purpose	This procedure creates a VT aggregation point (VAP). VAPs allow multiple DS-1 (VT1.5) circuits to be aggregated on a single STS on an OC-N, EC1, DS3, DS3E, DS3/EC1-48, DS3XM-6, or DS3XM-12 card. VAPs allow multiple VT1.5 circuits to pass through cross-connect cards without utilizing resources on the cross-connect card VT matrix. You also have the option to route the circuit through a portless transmultiplexing interface.
Tools/Equipment	For portless transmultiplexing configurations, a DS3XM-12 card must be installed on a node in the network.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Note VT aggregation points can be created for circuits on BLSR, 1+1, or unprotected nodes. They cannot be created for circuits on path protection nodes.

Note The maximum number of VAPs that you can create depends on the node protection topology and number of VT1.5 circuits that terminate on the node. Assuming that no other VT1.5 circuits terminate at the node, the maximum number of VAPs that you can terminate at one node is 8 for 1+1 protection and 12 for BLSR protection.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the VT aggregation point. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, choose **VT Aggregation Point** from the Circuit Type list.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-7):

- Name—Assign a name to the VT aggregation point. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the VAP.
- Size—Unavailable for VAPs.
- Bidirectional—Unavailable for VAPs.

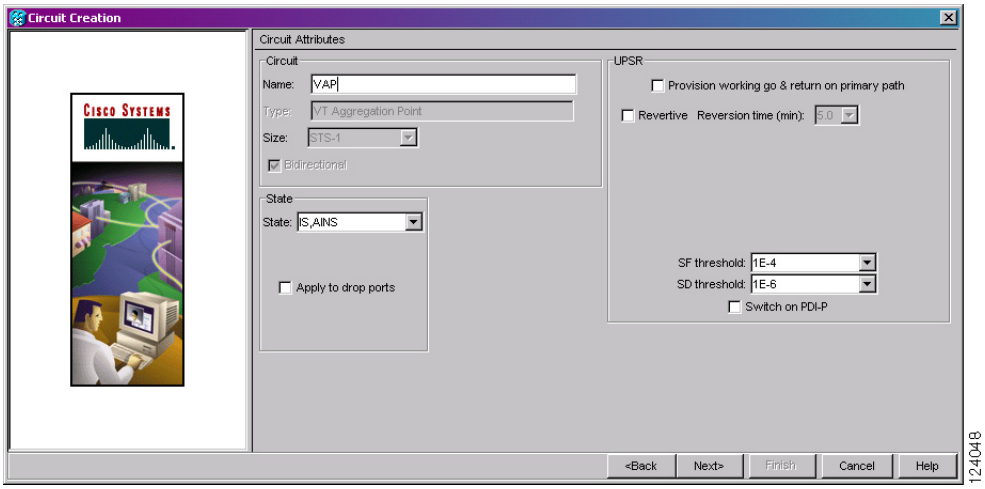
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Puts the circuit cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

Note A VAP automatically transitions into the IS service state after a VT circuit is created.

For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.

- Apply to drop ports—Uncheck this box.

Figure 6-7 Setting Attributes for a VT Aggregation Point



Step 8 Click **Next**.

Step 9 In the Circuit Source area, choose the source node, slot, port, and STS for the VAP. The VAP source is where the DS-1 (VT1.5) circuits will be aggregated into a single STS. The VAP destination is where the DS-1 circuits originate.

a. From the Node drop-down list, choose the node where the VAP will originate.

b. From the Slot drop-down list, choose the slot containing the OC-N, EC1, DS3, DS3E, DS3/EC1-48, DS3XM-6, or DS3XM-12 card where the VAP will originate.

c. Choose either the port or STS:

- If you choose an EC1, DS3, DS3E, DS3i-N-12, DS3/EC1-48, DS3XM-6, or DS3XM-12 card, from the Port drop-down list, choose the source port.

- If you choose an OC-N card from the STS drop-down list, choose the source STS.

Step 10 Click **Next**.

Step 11 In the Circuit Destination area, choose the node where the VT circuits aggregated by the VAP will terminate from the Node drop-down list.

Step 12 Click **Next**.

Step 13 In the Circuit Routing Preferences area, choose **Route Automatically**. Complete the following, as necessary:

- Using Required Nodes/Spans—Check this check box to specify nodes and spans to include or exclude in the CTC-generated tunnel route.

  Including nodes and spans for a circuit ensures that those nodes and spans are in the working path of the circuit (but not the protect path). Excluding nodes and spans ensures that the nodes and spans are not in the working or protect path of the circuit.
- Review Route Before Creation—Check this check box to review and edit the VT tunnel route before the circuit is created.
- VT-DS3 Mapped Conversion—Check this check box to route the VT tunnel over a portless transmultiplexing interface. This check box will be unavailable if you chose a DS3XM-6 or DS3XM-12 card as the VAP source in Step 9. This check box will be checked and greyed out if you chose a DS3, DS3E, DS3-EC1-48 card as the VAP source in Step 9.

Step 14 If you selected VT-DS3 Mapped Conversion in Step 13, complete the following substeps; otherwise, continue with Step 15:

a. Click **Next**.

b. In the Conversion Circuit Route Constraints area, complete the following:

- Node—Choose a node with a DS3XM-12 card installed.
- Slot—Choose the slot where a DS3XM-12 card is installed.
- DS3 Mapped STS—If applicable, choose **Circuit Dest** to indicate that the STS is the circuit destination, or **Circuit Source** to indicate that the STS is the circuit source.

Step 15 If you selected Using Required Nodes/Spans in Step 13:

a. Click **Next**.

b. In the Circuit Route Constraints area, click a span on the VAP map.

c. Click **Include** to include the node or span in the VAP. Click **Exclude** to exclude the node or span from the VAP. The sequence in which you choose the nodes and spans sets the VAP sequence. Click spans twice to change the circuit direction.

d. Repeat Steps b and c for each node or span you wish to include or exclude.

e. Review the VAP route. To change the tunnel routing order, choose a node in the Required Nodes/Lines or Excluded Nodes Links lists, then click the **Up** or **Down** buttons to change the tunnel routing order. Click **Remove** to remove a node or span.

Step 16 If you selected Review Route Before Creation in Step 13:

a. Click **Next**.

b. Review the tunnel route. To add or delete a tunnel span, choose a node on the tunnel route. Blue arrows show the tunnel route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned tunnel does not reflect the routing and configuration you want, click **Back** to verify and change tunnel information.

Step 17 Click **Finish**. The Circuits window appears.

Step 18 Verify that the VAP you just created appears in the circuits list. VAPs are identified in the Type column. The VAP tunnel automatically transitions into the IS-NR service state.

Stop. You have completed this procedure.

NTP-A135 Test Electrical Circuits

Purpose	This procedures tests DS-1 and DS-3 or EC-1 circuits.
Tools/Equipment	A test set and all appropriate cables
Prerequisite Procedures	This procedure assumes that you completed a facility loopback tests on the fibers and cables from the source and destination ONS 15454s to the digital signal cross-connect (DSX), and that you created a circuit using one of the following procedures: NTP-A139 Create a Half Circuit on a BLSR or 1+1 Node, page 6-53 NTP-A140 Create a Half Circuit on a Path Protection Node, page 6-55 NTP-A181 Create an Automatically Routed DS-1 Circuit, page 6-7 NTP-A182 Create a Manually Routed DS-1 Circuit, page 6-12 NTP-A183 Create a Unidirectional DS-1 Circuit with Multiple Drops, page 6-15 NTP-A184 Create an Automatically Routed DS-3 or EC-1 Circuit, page 6-19 NTP-A185 Create a Manually Routed DS-3 or EC-1 Circuit, page 6-24 NTP-A186 Create a Unidirectional DS-3 or EC-1 Circuit with Multiple Drops, page 6-27
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to test the electrical circuits. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuits** tab.

Step 4 Complete the "DLP-A230 Change a Circuit Service State" task on page 19-19 to set the circuit and circuit ports to the maintenance service state (OOS-MA,MT). Take note of the original state because you will return the circuit to that state later.

Step 5 Set the source and destination DS1 or DS3 card line length:

- **a.** In network view, double-click the source node.
- **b.** Double-click the circuit source card and click the **Provisioning > Line** tabs.
- **c.** From the circuit source port Line Length drop-down list, choose the line length for the distance (in feet) between the DSX (if used) or circuit termination point and the source ONS 15454.

d. Click **Apply**.

e. From the View menu, choose **Go to Network View**.

f. Repeat Steps a through e for the destination port line length.

Step 6 Attach loopback cables to the circuit destination card:

a. Verify the integrity of the loopback cable by looping the test set transmit (Tx) connector to the test set receive (Rx) connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to Step b.

b. Attach the loopback cable to the port you are testing. Connect the Tx connector to the Rx connector of the port.

Step 7 Attach loopback cables to the circuit source node:

a. Verify the integrity of loopback cable by looping the test set Tx connector to the test set Rx connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to Step b.

b. Attach the loopback cable to the port you are testing. Connect the test set to the circuit source port. Connect the Tx port of the test set to the circuit Rx port, and the test set Rx port to the circuit Tx port.

Step 8 Configure the test set for the ONS 15454 card that is the source of the circuit you are testing:

- DS-1—If you are testing an unmultiplexed DS-1, you must have a DSX-1 page or a direct DS-1 interface into the ONS 15454. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 page or a direct DS-3 interface into the ONS 15454. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.
- DS3XM—If you are testing a DS-1 circuit on a DS3XM-6 or DS3XM-12 card you must have a DSX-3 page or a direct DS-3 interface to the ONS 15454. Set the test set for a multiplexed DS-3. After you choose multiplexed DS-3, choose the DS-1 to test on the multiplexed DS-3. For information about configuring your test set, consult your test set user guide.
- EC-1—If you are testing a DS-1 on an EC1 card, you must have a DSX-3 page or a direct DS-3 interface to the ONS 15454. Set the test set for an STS-1. After you choose STS-1, choose the DS-1 to test the STS-1. For information about configuring your test set, consult your test set user guide.

Step 9 Verify that the test set shows a clean signal. If a clean signal does not appear, repeat Steps 2 through 8 to make sure the test set and cabling is configured correctly.

Step 10 Inject errors from the test set. Verify that the errors appear at the source and destination nodes.

Step 11 Clear the performance monitoring (PM) counts for the ports that you tested. See the "DLP-A349 Clear Selected PM Counts" task on page 20-35 for instructions.

Step 12 Complete the "DLP-A230 Change a Circuit Service State" task on page 19-19 to return the circuit and circuit ports to the service state they were in at the beginning of the test.

Step 13 Perform the protection switch test appropriate to the SONET topology:

- For path protection configurations, complete the "DLP-A94 Path Protection Configuration Protection Switching Test" task on page 17-90.
- For BLSRs, complete the "DLP-A91 BLSR Switch Test" task on page 17-83.

Step 14 Perform a bit error rate test (BERT) for 12 hours or follow your site requirements for length of time. For information about configuring your test set for a BERT, see your test set user guide.

Step 15 After the BERT is complete, print the results or save them to a disk for future reference. For information about printing or saving test results, see your test set user guide.

Stop. You have completed this procedure.

NTP-A343 Create an Automatically Routed Optical Circuit

Purpose	This procedure creates an automatically routed bidirectional or unidirectional optical circuit, including STS-1 and concatenated STS-3c, STS-6c, STS-9c, STS-12c, STS-18c, STS-24c, STS-36c, STS-48c, and STS-192c speeds.
Tools/Equipment	OC-N cards and all Ethernet cards, except E-Series cards. For a G-Series circuit, a G-Series card or ML-Series card must be installed at the other end of the circuit. For VT2 circuits, the XC-VXC-10G card must be installed at the circuit source and destination nodes.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 Complete the following as necessary (you can provision Ethernet or packet-over-SONET [POS] ports before or after the STS circuit is created):

- To provision Ethernet ports for CE-1000-4 circuits, complete the "DLP-A509 Provision CE-1000-4 Ethernet Ports" task on page 22-3.
- To provision Ethernet ports for CE-100T-8 or CE-MR-10 circuits, complete the "DLP-A513 Provision CE-100T-8 and CE-MR-10 Ethernet Ports" task on page 22-7.
- To provision POS ports for CE-Series circuits, complete the "DLP-A514 Provision CE-100T-8, CE-1000-4, and CE-MR-10 POS Ports" task on page 22-8.
- To enable the G-Series Ethernet ports for G-Series circuits, complete the "DLP-A222 Provision G-Series Ethernet Ports" task on page 19-15.
- To provision Ethernet ports for ML-Series circuits, complete the "DLP-A596 Provision the Ethernet Port of the ML-Series Card" task on page 22-104.
- To provision POS ports for ML-Series circuits, complete the "DLP-A597 Provision the POS Port of the ML-Series Card" task on page 22-105.

- To provision the card mode for ML-Series cards, complete the "DLP-A556 Provision the Card Mode for ML-Series Ethernet Cards" task on page 22-70.
- To change the default flow control settings for G-Series or CE-1000-4 circuits, complete the "DLP-A421 Provision G-Series and CE-1000-4 Flow Control Watermarks" task on page 21-6.

Step 4 From the View menu, choose **Go to Network View**.

Step 5 Click the **Circuits** tab, then click **Create**.

Step 6 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Enter the number of optical circuits that you want to create. The default is 1. If you are creating multiple circuits with the same source and destination, you can use auto-ranging to create the circuits automatically.
- Auto-ranged—This check box is automatically selected when you enter more than 1 in the Number of Circuits field. Leave this check box selected if you are creating multiple optical circuits with the same source and destination and you want CTC to create the circuits automatically. Uncheck the box if you do not want CTC to create the circuits automatically.

Step 7 Click **Next**.

Step 8 Define the circuit attributes (Figure 6-8 on page 6-42):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size: VT2, STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-18c, STS-24c, STS-36c, STS-48c, or STS-192c. Valid circuit sizes for a G-Series or CE-MR-10 circuit are STS-1, STS-3c, STS6c, STS-9c, STS-12c, STS-24c, and STS-48c.

Note Restrictions apply to provisioning multiple circuits on a G-Series card when one of the circuit sizes provisioned is STS-24c. Refer to the *Cisco ONS 15454 Reference Manual* for complete information.

- Bidirectional—Leave checked for this circuit (default).
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, VT tunnels and Ethergroup sources and destinations are unavailable.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Puts the circuit cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

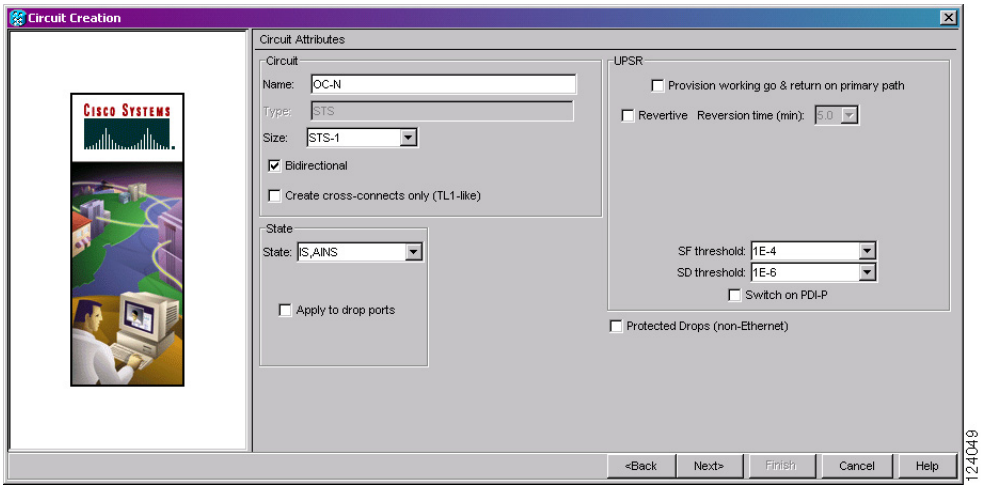
For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.

- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.

- Protected Drops—Check this check box if you want the circuit routed to protected drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, 1+1, or optimized 1+1 protection. If you check this check box, CTC provides only protected cards as source and destination choices.

Figure 6-8 Setting Circuit Attributes for an Optical Circuit



Step 9 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12.

Step 10 Click **Next**.

Step 11 Complete the "DLP-A97 Provision an OC-N Circuit Source and Destination" task on page 17-93 for the optical circuit you are creating.

Step 12 In the Circuit Routing Preferences area (Figure 6-9), choose **Route Automatically**. Three options are available; choose based on your preferences.

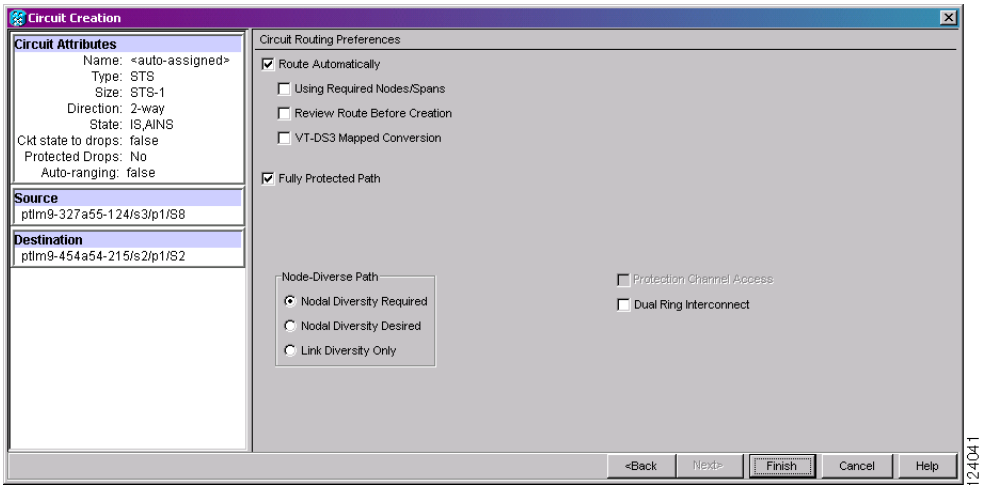
- Using Required Nodes/Spans—Check this check box to specify nodes and spans to include or exclude in the CTC-generated circuit route.

  Including nodes and spans for a circuit ensures that those nodes and spans are in the working path of the circuit (but not the protect path). Excluding nodes and spans ensures that the nodes and spans are not in the working or protect path of the circuit.

- Review Route Before Creation—Check this check box to review and edit the circuit route before the circuit is created.

- VT-DS3 Mapped Conversion—Check this check box to create a circuit using the portless transmultiplexing interface of the DS3XM-12 card.

Figure 6-9 Setting Circuit Routing Preferences for an Optical Circuit



Step 13 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 14. CTC creates a fully protected circuit route based on the path diversity option you choose. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 16.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 16.

Step 14 If you selected Fully Protected Path in Step 13 and the circuit will be routed on a path protection configuration, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 15 If you selected Fully Protected Path in Step 13 and the circuit will be routed on a BLSR DRI or path protection DRI, check the **Dual Ring Interconnect** check box.

Step 16 Click **Next**.

Step 17 If you selected VT-DS3 Mapped Conversion in Step 12, complete the following substeps; otherwise, continue with Step 18:

a. Click **Next**.

b. In the Conversion Circuit Route Constraints area, complete the following:

- Node—Choose a node with a DS3XM-12 card installed.

- Slot—Choose the slot where a DS3XM-12 card is installed.
- DS3 Mapped STS—If applicable, choose **Circuit Dest** to indicate that the STS is the circuit destination, or **Circuit Source** to indicate that the STS is the circuit source.

c. Click **Next**.

Step 18 If you checked Using Required Nodes/Spans in Step 12 or Dual Ring Interconnect for a path protection configuration in Step 15, complete the following substeps. If you checked Dual Ring Interconnect for a BLSR, skip this step and continue with Step 19. If you did not select any of these options, continue with Step 20.

a. In the Circuit Constraints for Automatic Routing area, click a node or span on the circuit map.

b. Click **Include** to include the node or span in the circuit. Click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans is the order in which the circuit is routed. Click spans twice to change the circuit direction.

c. Repeat Step b for each node or span you wish to include or exclude.

d. Review the circuit route. To change the circuit routing order, choose a node in the Required Nodes/Lines or Excluded Nodes Links lists and click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 19 Complete the "DLP-A563 Configure an Automatically Routed BLSR DRI" task on page 22-76.

Step 20 If you selected Review Route Before Creation in Step 12, complete the following substeps; otherwise, continue with Step 21.

a. Click **Next**.

b. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the "NTP-A344 Create a Manually Routed Optical Circuit" procedure on page 6-45 to assign the circuit route yourself.

Step 21 Click **Finish**. One of the following results occurs if you entered more than 1 in the Number of Circuits field on the Circuit Creation dialog box:

- If you chose Auto-ranged, CTC automatically creates the number of circuits entered in the Number of Circuits field. If auto-ranging cannot complete all the circuits, for example, because sequential ports are unavailable on the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto-ranging. After completing the circuits, the Circuits window appears.
- If you did not choose Auto-ranged, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 6 through 20 for each additional circuit. After completing the circuits, the Circuits window appears.

Step 22 In the Circuits window, verify that the circuits you created appear in the circuits list.

Step 23 Complete the following as necessary. Skip this step if you built a test circuit.

a. Complete the "NTP-A62 Test Optical Circuits" procedure on page 6-51.

b. Complete the "NTP-A149 Test G-Series Circuits" procedure on page 6-79.

Stop. You have completed this procedure.

NTP-A344 Create a Manually Routed Optical Circuit

Purpose	This procedure creates a manually routed, bidirectional or unidirectional, optical circuit, including STS-1 or concatenated STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, STS-48c, or STS-192c speeds.
Tools/Equipment	OC-N cards and all Ethernet cards, except E-Series cards. For a G-Series circuit, a G-Series card or ML-Series card must be installed at the other end of the circuit. For VT2 circuits, the XC-VXC-10G card must be installed at the circuit source and destination nodes.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 Complete the following as necessary (you can provision Ethernet or POS ports before or after the STS circuit is created):

- To provision Ethernet ports for CE-1000-4 circuits, complete the "DLP-A509 Provision CE-1000-4 Ethernet Ports" task on page 22-3
- To provision Ethernet ports for CE-100T-8 or CE-MR-10 circuits, complete the "DLP-A513 Provision CE-100T-8 and CE-MR-10 Ethernet Ports" task on page 22-7.
- To provision POS ports for CE-Series circuits, complete the "DLP-A514 Provision CE-100T-8, CE-1000-4, and CE-MR-10 POS Ports" task on page 22-8.
- To enable the G-Series Ethernet ports for G-Series circuits, complete the "DLP-A222 Provision G-Series Ethernet Ports" task on page 19-15.
- To provision Ethernet ports for ML-Series circuits, complete the "DLP-A596 Provision the Ethernet Port of the ML-Series Card" task on page 22-104.
- To provision POS ports for ML-Series circuits, complete the "DLP-A597 Provision the POS Port of the ML-Series Card" task on page 22-105.
- To provision the card mode for ML-Series cards, complete the "DLP-A556 Provision the Card Mode for ML-Series Ethernet Cards" task on page 22-70.
- To change the default flow control settings for G-Series or CE-1000-4 circuits, complete the "DLP-A421 Provision G-Series and CE-1000-4 Flow Control Watermarks" task on page 21-6.

Step 4 From the View menu, choose **Go to Network View**.

Step 5 Click the Circuits tab, then click **Create**.

Step 6 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Enter the number of optical circuits that you want to create. The default is 1.

- Auto-ranged—(Automatically routed circuits only) If you entered more than 1 in the Number of Circuits field, uncheck this box. (The box is unavailable if only one circuit is entered in the Number of Circuits field.)

Step 7 Click **Next**.

Step 8 Define circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size: VT2, STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-18c, STS-24c, STS-36c, STS-48c, or STS-192c. Valid circuit sizes for a G-Series or CE-MR-10 circuit are STS-1, STS-3c, STS6c, STS-9c, STS-12c, STS-24c, and STS-48c.

Note Restrictions apply to provisioning multiple circuits on a G-Series card when one of the circuit sizes provisioned is STS-24c. Refer to the *Cisco ONS 15454 Reference Manual* for complete information.

- Bidirectional—Leave checked for this circuit (default).
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, VT tunnels and Ethergroup sources and destinations are unavailable.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Puts the circuit cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.

- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, 1+1, or optimized 1+1 protection. If you check this check box, CTC provides only protected cards as source and destination choices.

Step 9 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12.

Step 10 Click **Next**.

Step 11 Complete the "DLP-A97 Provision an OC-N Circuit Source and Destination" task on page 17-93 for the optical circuit you are creating.

Step 12 In the Circuit Routing Preferences area (Figure 6-9 on page 6-43), uncheck **Route Automatically**.

Step 13 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 14.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 16.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 16.
- To create STS around the Ring circuits uncheck **Fully Protected Path, t**hen continue with Step 16.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 14 If you selected Fully Protected Path in Step 13 and the circuit will be routed on a path protection configuration, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 15 If you selected Fully Protected Path in Step 13 and the circuit will be routed on a BLSR DRI or path protection DRI, check the **Dual Ring Interconnect** check box.

Step 16 Click **Next**. In the Route Review/Edit area, node icons appear for you to route the circuit manually. If you checked Dual Ring Interconnect for BLSR, continue with Step 17. If not, continue with Step 18.

Step 17 Complete the "DLP-A564 Configure a Manually Routed BLSR DRI" task on page 22-78.

Step 18 Complete the "DLP-A369 Provision an OC-N Circuit Route" task on page 20-53.

Step 19 Click **Finish**. If the path does not meet the specified path diversity requirement, CTC displays an error message and allows you to change the circuit path. If you entered more than 1 in the Number of Circuits field on the Circuit Creation dialog box, the Circuit Creation dialog box appears after the circuit is created so you can create the remaining circuits. Repeat Steps 6 through 18 for each additional circuit.

Step 20 When all the circuits are created, the main Circuits window appears. Verify that the circuits you created appear in the window.

Step 21 Complete the following as necessary. Skip this step if you built a test circuit.

a. Complete the "NTP-A62 Test Optical Circuits" procedure on page 6-51.

b. Complete the "NTP-A149 Test G-Series Circuits" procedure on page 6-79.

Stop. You have completed this procedure.

NTP-A314 Create a Unidirectional Optical Circuit with Multiple Drops

Purpose	This procedure creates a unidirectional optical circuit with multiple traffic drops (circuit destinations).
Tools/Equipment	For VT2 circuits, the XC-VXC-10G card must be installed at the circuit source and destination nodes.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 on the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable when the Number of Circuits field is 1.

Step 6 Click **Next**.

Step 7 Define circuit attributes (Figure 6-10):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size: VT2, STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-18c, STS-24c, STS-36c, STS-48c, or STS-192c.
- Bidirectional—Uncheck this check box for this circuit.
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, VT tunnels and Ethergroup sources and destinations are unavailable.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Puts the circuit cross-connects in the IS-NR service state.

- OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
- IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
- OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

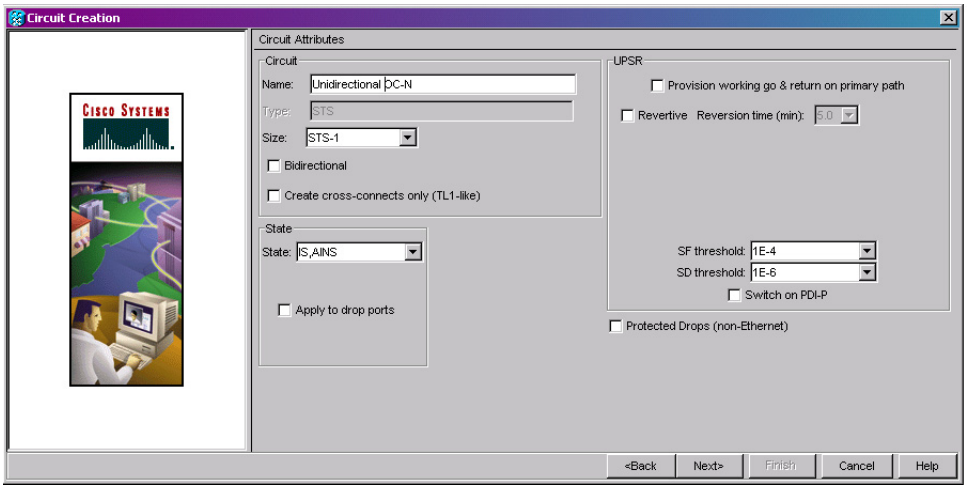
For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.

- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.

- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, 1+1, or optimized 1+1 protection. If you check this check box, CTC provides only protected cards as source and destination choices.

Figure 6-10 Setting Circuit Attributes for a Unidirectional Optical Circuit



Step 8 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12.

Step 9 Click **Next**.

Step 10 Complete the "DLP-A97 Provision an OC-N Circuit Source and Destination" task on page 17-93 for the circuit that you are creating.

Step 11 Uncheck **Route Automatically**. When Route Automatically is not selected, the Using Required Nodes/Spans and Review Route Before Circuit Creation check boxes are unavailable.

Step 12 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 15.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection configuration, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Note For manually routed circuits, CTC checks your manually provisioned path against the path diversity option you choose. If the path does not meet the path diversity requirement that is specified, CTC displays an error message.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a BLSR DRI or path protection DRI, check the **Dual Ring Interconnect** check box.

Step 15 Click **Next**. In the Route Review/Edit area, node icons appear for you to route the circuit manually. If you checked Dual Ring Interconnect for BLSR, continue with Step 16. If not, continue with Step 17.

Step 16 Complete the "DLP-A564 Configure a Manually Routed BLSR DRI" task on page 22-78.

Step 17 Complete the "DLP-A369 Provision an OC-N Circuit Route" task on page 20-53.

Step 18 Click **Finish**. After completing the circuit, the Circuits window appears.

Step 19 In the Circuits window, click the circuit that you want to route to multiple drops. The Delete, Edit, and Search buttons become active.

Step 20 Click **Edit**. The Edit Circuit window appears with the General tab selected. All nodes in the DCC network appear on the network map. Circuit source and destination information appears under the source and destination nodes. To see a detailed view of the circuit, click **Show Detailed Map**. You can rearrange the node icons by pressing **Ctrl** while you drag and drop the icon to the new location.

Step 21 In the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops appears.

Step 22 Click **Create**.

Step 23 In the Define New Drop dialog box, define the new drop:

a. Node—Choose the target node for the circuit drop.

b. Slot—Choose the target card and slot.

c. Port, STS—Choose the port and/or STS from the Port and STS drop-down lists. The choice in these menus depends on the card selected in Step b. See Table 6-2 on page 6-3 for a list of options.

d. The routing preferences for the new drop match those of the original circuit. However, if the following options are available, you can modify them:

- If the original circuit was routed on a protected path protection path, you can change the nodal diversity options: Nodal Diversity Required, Nodal Diversity Desired, or Link Diversity Only. See Step 13 for option descriptions.
- If the original circuit was not routed on a protected path, the Protection Channel Access option is available. See Step 12 for a description of the PCA option.

e. If you want to change the circuit state, choose the circuit state from the Target Circuit Admin State drop-down list. The state chosen applies to the entire circuit.

f. Check **Apply to drop ports** if you want to apply the state chosen in the Target Circuit Admin State to the circuit source and destination drops. For the requirements necessary to apply a service state to drop ports, refer to the *Cisco ONS 15454 Reference Manual*.

g. Click **Finish**. The new drop appears in the Drops list.

Step 24 If you need to create additional drops on the circuit, repeat Steps 21 through 23.

Step 25 Click **Close**. The Circuits window appears.

Step 26 Verify that the new drops appear in the Destination column for the circuit you edited. If they do not appear, repeat Steps 22 through 25, making sure all options are provisioned correctly.

Step 27 Complete the "NTP-A62 Test Optical Circuits" procedure on page 6-51.

Stop. You have completed this procedure.

NTP-A62 Test Optical Circuits

Purpose	This procedure tests an optical circuit. Required if you created an optical circuit.
Tools/Equipment	Test set capable of optical speeds, appropriate fibers, and attenuators
Prerequisite Procedures	This procedure assumes that you completed facility loopback tests to test the fibers and cables from the source and destination ONS 15454s to the fiber distribution page or the DSX, and one of following circuit procedures: NTP-A343 Create an Automatically Routed Optical Circuit, page 6-40 NTP-A344 Create a Manually Routed Optical Circuit, page 6-45 NTP-A314 Create a Unidirectional Optical Circuit with Multiple Drops, page 6-48
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you created the circuit.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuits** tab.

Step 4 Complete the "DLP-A230 Change a Circuit Service State" task on page 19-19 to set the circuit and circuit ports to the OOS-MA,MT service state.

Step 5 Set up the patch cable at the destination node:

a. Test the patch cable by connecting one end to the test set Tx port and the other end to the test Rx port. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly.

b. Install the loopback cable on the port you are testing. Connect the Tx connector to the Rx connector of the port being tested.

Step 6 Set up the patch cable at the source node:

a. Test the loopback cable by connecting one end to the test set Tx port and the other end to the test Rx port. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly.

b. At the source node, attach the loopback cable to the port you are testing. Connect the test set to the circuit source port. Connect the Tx port of the test set to the circuit Rx port, and the test set Rx port to the circuit Tx port.

Step 7 Configure the test set for the source ONS 15454 card:

- OC-3 cards—You will test either an OC-3c or a multiplexed OC-3. If you are testing an OC-3c, configure the test set for an OC-3c. If you are testing a multiplexed OC-3, configure the test set for a multiplexed OC-3 and choose the DS-3 and/or DS-1 you will test. For information about configuring your test set, consult your test set user guide.
- OC-12 cards—You will test either an OC-12c or a multiplexed OC-12. If you are testing an OC-12c, configure the test set for an OC-12c. If you are testing a multiplexed OC-12, configure the test set for a multiplexed OC-12 and choose the DS-3 and/or DS-1 you will test. For information about configuring your test set, consult your test set user guide.
- OC-48 cards—You will test either an OC-48c or a multiplexed OC-48. If you are testing an OC-48c, configure the test set for an OC-48c. If you are testing a multiplexed OC-48, configure the test set for a multiplexed OC-48 and choose the DS-3 and/or DS-1 you will test. For information about configuring your test set, consult your test set user guide.
- OC-192 cards—You will test an OC-192c or a multiplexed OC-192. If you are testing an OC-192c, configure the test set for an OC-192c. If you are testing a multiplexed OC-192, configure the test set for a multiplexed OC-192 and choose the DS-3 and/or DS-1 you will test. For information about configuring your test set, consult your test set user guide.

Step 8 Verify that the test set shows a clean signal. If a clean signal does not appear, repeat Steps 2 through 7 to make sure that you have configured the test set and cabling correctly.

Step 9 Inject errors from the test set. Verify that the errors appear at the source and destination nodes.

Step 10 Clear the PM counts for the ports that you tested. See the "DLP-A349 Clear Selected PM Counts" task on page 20-35 for instructions.

Step 11 Perform protection switch testing appropriate to the SONET topology:

- For path protection configurations, see the "DLP-A94 Path Protection Configuration Protection Switching Test" task on page 17-90.
- For BLSRs, see the "DLP-A91 BLSR Switch Test" task on page 17-83.

Step 12 Perform a BERT for 12 hours or follow your site requirements for length of time. For information about configuring your test set for the BERT, see your test set user guide.

Step 13 After the BERT is complete, print the results or save them to a disk for future reference. For information about printing or saving test results, see your test set user guide.

Step 14 Complete the "DLP-A230 Change a Circuit Service State" task on page 19-19 to change the circuit and circuit ports from OOS-MA,MT to their previous service states.

Stop. You have completed this procedure.

NTP-A139 Create a Half Circuit on a BLSR or 1+1 Node

Purpose	This procedure creates a DS-1, DS-3, or optical circuit from a drop card to an OC-N or G-Series trunk card on the same node in a BLSR or 1+1 topology.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node on the network where you will create the half circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—For DS-1 circuits, choose **VT**. VT cross-connects will carry the DS-1 circuit across the ONS 15454 network. For DS-3 or optical circuits, choose **STS**. STS cross-connects will carry the DS-3 circuit across the ONS 15454 network.
- Number of Circuits—Enter the number of circuits that you want to create. The default is 1.
- Auto-ranged—Uncheck this check box; it is automatically selected if you enter more than 1 in the Number of Circuits field.

Step 6 Click **Next**.

Step 7 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—For DS-3 or optical circuits, choose **STS-1**. For DS-1 circuits, VT1.5 is the default. You cannot change it.
- Bidirectional—Leave checked for this circuit (default).

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, VT tunnels and Ethergroup sources and destinations are unavailable.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Puts the circuit cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

  Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.
- Protected Drops—Uncheck this box.

Step 8 Click **Next**.

Step 9 Complete the "DLP-A311 Provision a Half Circuit Source and Destination on a BLSR or 1+1 Configuration" task on page 20-5.

Step 10 Click **Finish**. One of the following results occurs if you entered more than 1 in the Number of Circuits field on the Circuit Creation dialog box:

- If you chose Auto-ranged, CTC automatically creates the number of circuits entered in the Number of Circuits field. If auto-ranging cannot complete all the circuits, for example, because sequential ports are unavailable at the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto-ranging. After completing the circuits, the Circuits window appears.
- If you did not choose Auto-ranged, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 5 through 9 for each additional circuit. After completing the circuits, the Circuits window appears.

Step 11 In the Circuits window, verify that the new circuits appear in the circuits list.

Step 12 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 6-38 or the "NTP-A62 Test Optical Circuits" procedure on page 6-51, as applicable. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-A140 Create a Half Circuit on a Path Protection Node

Purpose	This procedure creates a DS-1, DS-3, or optical circuit from a drop to an OC-N or G-Series line card on the same path protection node.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—For DS-1 circuits, choose **VT**. VT cross-connects will carry the DS-1 circuit across the ONS 15454 network. For DS-3 or optical circuits, choose **STS**. STS cross-connects will carry the DS-3 circuit across the ONS 15454 network.
- Number of Circuits—Enter the number of circuits that you want to create. The default is 1.
- Auto-ranged—Uncheck this check box; it is automatically selected if you enter more than 1 in the Number of Circuits field.

Step 6 Click **Next**.

Step 7 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—For DS-1 circuits, VT1.5 is the default. You cannot change it. For DS-3 or optical circuits, choose **STS-1**.
- Bidirectional—Leave checked for this circuit (default).
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, VT tunnels and Ethergroup sources and destinations are unavailable.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Puts the circuit cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.

  - IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.

- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

  Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.

- Protected Drops—Leave this box unchecked.

Step 8 Set the path protection path selectors. See the "DLP-A218 Provision Path Protection Selectors" task on page 19-12.

Step 9 Click **Next**.

Step 10 Complete the "DLP-A312 Provision a Half Circuit Source and Destination on a Path Protection Configuration" task on page 20-6.

Step 11 Click **Finish**. One of the following results occurs if you entered more than 1 in the Number of Circuits field on the Circuit Creation dialog box:

- If you chose Auto-ranged, CTC automatically creates the number of circuits entered in the Number of Circuits field. If auto-ranging cannot complete all the circuits, for example, because sequential ports are unavailable at the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click Finish to continue auto-ranging. After completing the circuits, the Circuits window appears.
- If you did not choose Auto-ranged, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 5 through 10 for each additional circuit. After completing the circuits, the Circuits window appears.

Step 12 In the Circuits window, verify that the new circuits appear in the circuits list.

Step 13 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 6-38 or the "NTP-A62 Test Optical Circuits" procedure on page 6-51, as applicable. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-A191 Create an E-Series EtherSwitch Circuit (Multicard or Single-Card Mode)

Purpose	This procedure creates a multicard or single-card EtherSwitch circuit. It does not apply to E-Series cards in port-mapped mode. To create a port-mapped mode circuit, see NTP-A192 Create a Circuit for an E-Series Card in Port-Mapped Mode, page 6-60.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed at each end of the Ethernet circuit.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the EtherSwitch circuit. If you are already logged in, continue with Step 2.

Step 2 If the network is already using a high number of VLANs, complete the "DLP-A99 Determine Available VLANs" task on page 17-94 to verify that sufficient VLAN capacity is available. (You will create a VLAN during each circuit creation task.)

Step 3 If enough VLANs are not available, complete the "DLP-A335 Delete VLANs" task on page 20-23 to free space.

Step 4 Verify that the circuit source and destination Ethernet cards are provisioned for the mode of the circuit that you will create, either multicard or single-card. See the "DLP-A246 Provision E-Series Ethernet Card Mode" task on page 19-28.

Step 5 Provision and enable the Ethernet ports. See the "DLP-A220 Provision E-Series Ethernet Ports" task on page 19-13.

Step 6 From the View menu, choose **Go to Network View**.

Step 7 Click the **Circuits** tab, then click **Create**.

Step 8 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.

Step 9 Click **Next**.

Step 10 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.

- Size—Choose the circuit size. Valid circuit sizes for an Ethernet multicard circuit are STS-1, STS-3c, and STS6c. Valid circuit sizes for an Ethernet single-card circuit are STS-1, STS-3c, STS6c, and STS12c.
- Bidirectional—Leave the default unchanged (checked).
- Create cross-connects only (TL1-like)—Uncheck this box; it does not apply to Ethernet circuits.
- State—Choose **IS** (in service). Ethergroup circuits are stateless and always in service.
- Apply to drop ports—Uncheck this box; states cannot be applied to E-Series Ethernet card ports.
- Protected Drops—Leave the default unchanged (unchecked).

Step 11 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12.

Caution Layer 1 SONET protection does not extend to multicard EtherSwitch circuits on path protection configurations.

Caution A TCC2/TCC2P card reset disrupts single-card and multicard EtherSwitch circuits for 45 seconds to two minutes. During this time, a spanning tree topology is created by the newly activated TCC2/TCC2P card.

Step 12 Click **Next**.

Step 13 Provision the circuit source:

a. From the Node drop-down list, choose one of the EtherSwitch circuit endpoint nodes. (Either end node can be the EtherSwitch circuit source.)

b. From the Slot drop-down list, choose one of the following:

- If you are building a multicard EtherSwitch circuit, choose **Ethergroup**.
- If you are building a single-card EtherSwitch circuit, choose the Ethernet card where you enabled the single-card EtherSwitch.

Step 14 Click **Next**.

Step 15 Provision the circuit destination:

a. From the Node drop-down list, choose the second EtherSwitch circuit endpoint node.

b. From the Slot drop-down list, choose one of the following:

- If you are building a multicard EtherSwitch circuit, choose **Ethergroup**.
- If you are building a single-card EtherSwitch circuit, choose the Ethernet card where you enabled the single-card EtherSwitch.

Step 16 Click **Next**.

Step 17 In the Circuit VLAN Selection area, click **New VLAN**. If the desired VLAN already exists, continue with Step 20.

Tip You can also add VLANs in network view by choosing **Tools > Manage VLANs**. In the All VLANs dialog box, click the **Create** button to open the Define New VLAN dialog box.

Step 18 In the Define New VLAN dialog box, complete the following:

- VLAN Name—Assign an easily identifiable name to your VLAN.

- VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.
- Topology Host—Choose the node to serve as the topology host from the drop-down list.

Step 19 Click **OK**.

Step 20 In the Circuit VLAN Selection area, highlight the VLAN name and click the arrow button (>>) to move the available VLANs to the Circuit VLANs column.

Step 21 If you are building a single-card EtherSwitch circuit and want to disable spanning tree protection on this circuit, uncheck the **Enable Spanning Tree** check box and click **OK** in the Disabling Spanning Tree dialog box. The Enable Spanning Tree box remains checked or unchecked for the creation of the next single-card, point-to-point Ethernet circuit.

Caution Disabling spanning-tree protection increases the likelihood of logic loops on an Ethernet network.

Caution Turning off spanning tree on a circuit-by-circuit basis means that the ONS 15454 is no longer protecting the Ethernet circuit and that the circuit must be protected by another mechanism in the Ethernet network.

Caution Multiple circuits with spanning tree protection enabled incur blocking if the circuits traverse the same E-Series card and use the same VLAN.

Note Spanning-tree rules prevent users from creating new circuits or modifying existing circuits if the circuits do not meet certain VLAN assignment constraints. If the VLAN set of the new circuit overlaps existing circuits, the same spanning-tree instance is used for all circuits. If the VLAN set of the new circuit overlaps with VLAN sets of existing circuits with different spanning-tree instances, the VLAN assignment fails. Cisco recommends that you plan VLAN assignments so that circuits with larger VLAN sets and a higher chance of overlap are added first. This means that if a circuit with an overlapping VLAN set is added, it collapses into the same spanning tree. To view circuits mapped to a spanning tree and their VLAN assignments, see the "DLP-A430 View Spanning Tree Information" task on page 21-9.

Note You can disable or enable spanning tree protection on a circuit-by-circuit basis only for single-card, point-to-point Ethernet circuits. Other E-Series Ethernet configurations disable or enable spanning tree on a port-by-port basis.

Step 22 Click **Next**.

Step 23 In the Circuit Attributes area, confirm that the following information is correct:

- Circuit name
- Circuit type
- Circuit size
- ONS nodes

Step 24 If the information is not correct, click the **Back** button and repeat Steps 8 through 23 with the correct information. If the information is correct, check **Route Automatically**.

Step 25 Click **Finish**.

Step 26 Complete the "DLP-A221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 19-14.

Step 27 Complete the "NTP-A146 Test E-Series Circuits" procedure on page 6-73.

Stop. You have completed this procedure.

NTP-A192 Create a Circuit for an E-Series Card in Port-Mapped Mode

Purpose	This procedure creates an E-Series point-to-point SONET circuit with an E-Series card in port-mapped mode.
Tools/Equipment	An E-Series Ethernet card must be installed at each end of the circuit and configured in port-mapped mode.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 4.

Step 2 Provision the Ethernet cards that will carry the circuit for port-mapped mode. See the "DLP-A246 Provision E-Series Ethernet Card Mode" task on page 19-28.

Step 3 Complete the "DLP-A220 Provision E-Series Ethernet Ports" task on page 19-13.

Step 4 From the View menu, choose **Go to Network View**.

Step 5 Click the **Circuits** tab and click **Create**.

Step 6 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.

Step 7 Click **Next**.

Step 8 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.

- Size—Choose the circuit size. Valid circuit sizes for an E-Series circuit are STS-1, STS-3c, STS6c, and STS-12c.
- Bidirectional—Leave the default unchanged (checked).
- Create cross-connects only (TL1-like)—Uncheck this box.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Puts the circuit cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the state chosen in the State field (IS or OOS-MT only) to the Ethernet circuit source and destination ports. You cannot apply OOS-AINS to E-Series Ethernet card ports. CTC applies the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. If the box is unchecked, CTC does not change the state of the source and destination ports. For the requirements necessary to apply a service state to drop ports, refer to the *Cisco ONS 15454 Reference Manual*.

  Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.
- Auto-ranged—Unavailable.
- Protected Drops—Leave the default unchanged (unchecked).

Step 9 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12.

Step 10 Click **Next**.

Step 11 Provision the circuit source:

a. From the Node drop-down list, choose the circuit source node. Either end node can be the point-to-point circuit source.

b. From the Slot drop-down list, choose the slot containing the E-Series card that you will use for one end of the point-to-point circuit.

c. From the Port drop-down list, choose a port.

Step 12 Click **Next**.

Step 13 Provision the circuit destination:

a. From the Node drop-down list, choose the circuit destination node.

b. From the Slot drop-down list, choose the slot containing the E-Series card that you will use for other end of the point-to-point circuit.

c. From the Port drop-down list, choose a port.

Step 14 Click **Next**.

Step 15 In the Circuit Attributes area, confirm that the following information is correct:

- Circuit name
- Circuit type
- Circuit size
- ONS nodes

Step 16 If the information is not correct, click the **Back** button and repeat Steps 6 through 15 with the correct information. If the information is correct, check **Route Automatically**.

Step 17 Click **Finish**.

Step 18 Complete the "NTP-A146 Test E-Series Circuits" procedure on page 6-73.

Stop. You have completed this procedure.

NTP-A142 Create an E-Series Shared Packet Ring Ethernet Circuit

Purpose	This procedure creates a shared packet ring Ethernet circuit. It does not apply to E-Series cards in port-mapped mode.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed at both Ethernet circuit endpoint nodes.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If a high number of VLANs is already used by the network, complete the "DLP-A99 Determine Available VLANs" task on page 17-94 to verify that sufficient VLAN capacity is available. (You will create a VLAN during each circuit creation task.)

Step 3 Verify that the Ethernet cards that will carry the circuit are provisioned for the Multicard EtherSwitch Group. See the "DLP-A246 Provision E-Series Ethernet Card Mode" task on page 19-28.

Step 4 Provision and enable the Ethernet ports. See "DLP-A220 Provision E-Series Ethernet Ports" task on page 19-13.

Step 5 From the View menu, choose **Go to Network View**.

Step 6 Click the **Circuits** tab and click **Create**.

Step 7 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.

Step 8 Click **Next**.

Step 9 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size. Valid shared packet ring circuit sizes are STS-1, STS-3c, and STS6c.
- Bidirectional—Leave the default unchanged (checked).
- Create cross-connects only (TL1-like)—Uncheck this box; it does not apply to Ethernet circuits.
- State—The circuit is in service (default).
- Apply to drop ports—Uncheck this box; states cannot be applied to E-Series ports.
- Protected Drops—Leave the default unchanged (unchecked).

Step 10 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12.

Caution Layer 1 SONET protection does not extend to multicard EtherSwitch circuits on path protection configurations.

Step 11 Click **Next**.

Step 12 Provision the circuit source:

a. From the Node drop-down list, choose one of the shared packet ring circuit endpoint nodes. (Either end node can be the shared packet ring circuit source.)

b. From the Slot drop-down list, choose **Ethergroup**.

Step 13 Click **Next**.

Step 14 Provision the circuit destination:

a. From the Node drop-down list, choose the second shared packet ring circuit endpoint node.

b. From the Slot drop-down list, choose **Ethergroup**.

Step 15 Click **Next**.

Step 16 Review the VLANs listed in the Available VLANs list. If the VLAN you want to use appears, continue with Step 17. If you need to create a new VLAN, complete the following steps:

a. Click the **New VLAN** button.

b. In the Define New VLAN dialog box, complete the following:

- VLAN Name—Assign an easily identifiable name to your VLAN.
- VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.
- Topology Host—Choose the topology host ID from the drop-down list.

c. Click **OK**.

Tip You can also add VLANs in network view by choosing **Tools > Manage VLANs.** In the All VLANs dialog box, click the **Create** button to open the Define New VLAN dialog box.

Step 17 In the Available VLANs column, click the VLAN that you want to use and click the arrow button (**>>**) to move the VLAN to the Circuit VLANs column.

Note Moving the VLAN from Available VLANs to Circuit VLANs forces all the VLAN traffic to use the shared packet ring you are creating.

Step 18 Click **Next**.

Step 19 In the Circuit Routing Preferences area, uncheck the **Route Automatically** check box and click **Next**.

Step 20 In the Route Review and Edit area, click the source node, then click a span (green arrow) leading away from the source node.

The span turns white.

Step 21 Click **Add Span**.

The span turns blue. CTC adds the span to the Included Spans list.

Step 22 Click the node at the end of the blue span.

Step 23 Click the green span joining the node selected in Step 22.

The span turns white.

Step 24 Click **Add Span**.

The span turns blue.

Step 25 Repeat Steps 21 through 24 for every node in the ring.

Step 26 In the Route Review and Edit area, verify that the new circuit is correctly configured. If the circuit information is not correct, click the **Back** button and repeat Steps 7 through 25 with the correct information.

Note If the circuit is incorrect, you can also click **Finish**, delete the completed circuit, and begin the procedure again.

Step 27 Click **Finish**.

Step 28 Complete the "DLP-A220 Provision E-Series Ethernet Ports" task on page 19-13 for each node that carries the circuit.

Step 29 Complete the "DLP-A221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 19-14 for each node that carries the circuit.

Step 30 Complete the "NTP-A146 Test E-Series Circuits" procedure on page 6-73.

Stop. You have completed this procedure.

NTP-A143 Create an E-Series Hub-and-Spoke Ethernet Configuration

Purpose	This procedure creates a hub-and-spoke Ethernet configuration, which is made up of multiple circuits that share a common endpoint. It does not apply to E-Series cards in port-mapped mode.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed at all Ethernet circuit endpoint nodes.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" in appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the hub node (the common endpoint). If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A99 Determine Available VLANs" task on page 17-94 to verify that sufficient VLAN capacity is available. (You will create a VLAN during each circuit creation task.)

Step 3 Display the node view.

Step 4 Verify that the Ethernet card that will carry the hub-and-spoke circuit is provisioned for Single-card EtherSwitch Group. See the "DLP-A246 Provision E-Series Ethernet Card Mode" task on page 19-28.

Step 5 Provision and enable the Ethernet ports. See "DLP-A220 Provision E-Series Ethernet Ports" task on page 19-13.

Step 6 Log into a spoke endpoint node and repeat Steps 3 through 5 for the destination Ethernet card. You only need to verify that the hub node is provisioned for single-card EtherSwitch once.

Step 7 Click the **Circuits** tab and click **Create**.

Step 8 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.

Step 9 Click **Next**.

Step 10 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size.
- Bidirectional—Leave the default unchanged (checked).

- Create cross-connects only (TL1-like)—Uncheck this box; it does not apply to Ethernet circuits.
- State—The circuit is in service (default).
- Apply to drop ports—Uncheck this box; states cannot be applied to E-Series ports.
- Protected Drops—Leave the default unchanged (unchecked).

Step 11 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12.

Step 12 Click **Next**.

Step 13 Provision the circuit source:

a. From the Node drop-down list, choose the hub node.

b. From the Slot drop-down list, choose the Ethernet card where you enabled the single-card EtherSwitch.

Step 14 Click **Next**.

Step 15 Provision the circuit destination:

a. From the Node drop-down list, choose an EtherSwitch circuit endpoint node.

b. From the Slot drop-down list, choose the Ethernet card where you enabled the single-card EtherSwitch.

Step 16 Click **Next**.

Step 17 Review the VLANs listed in the Available VLANs list. If the VLAN you want to use appears, continue with Step 19. If you need to create a new VLAN, complete the following steps:

a. Click the **New VLAN** button.

b. In the Define New VLAN dialog box, complete the following:

- VLAN Name—Assign an easily identifiable name to your VLAN.
- VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.
- Topology Host—Choose the topology host ID from the drop-down list.

c. Click **OK**.

Tip You can also add VLANs in network view by choosing **Tools > Manage VLANs**. In the All VLANs dialog box, click the **Create** button to open the Define New VLAN dialog box.

Step 18 In the Available VLANs column, click the VLAN that you want to use and click the arrow button (>>) to move the VLAN to the Circuit VLANs column.

Note Moving the VLAN from Available VLANs to Circuit VLANs forces all the VLAN traffic to use the shared packet ring you are creating.

Step 19 Click **Next**.

Step 20 In the Circuit Attributes area, confirm that the following information is correct:

- Circuit name
- Circuit type

- Circuit size
- VLAN names
- ONS nodes

Step 21 If the information is not correct, click the **Back** button and repeat Steps 8 through 20 with the correct information. If the information is correct, check **Route Automatically**.

Step 22 Click **Finish**.

Step 23 Complete the "DLP-A220 Provision E-Series Ethernet Ports" task on page 19-13 for each node that carries the circuit.

Step 24 Complete the "DLP-A221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 19-14.

Step 25 Complete the "NTP-A146 Test E-Series Circuits" procedure on page 6-73 for each node that carries the circuit.

Step 26 To create additional circuits (spokes), repeat Steps 2 through 25.

Stop. You have completed this procedure.

NTP-A144 Create an E-Series Single-Card EtherSwitch Manual Cross-Connect

Purpose	This procedure manually creates a single-card EtherSwitch cross-connect between E-Series Ethernet cards and OC-N cards connected to non-ONS equipment.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed at the circuit source node.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Note In this procedure, cross-connect refers to a circuit connection created within the same node between the Ethernet card and an OC-N card connected to third-party equipment. You create cross-connects at the source and destination nodes so an Ethernet circuit can be routed from source to destination across third-party equipment.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 If a high number of VLANs is already used by the network, complete the "DLP-A99 Determine Available VLANs" task on page 17-94 to verify that sufficient VLAN capacity is available. (You will create a VLAN during each circuit creation task.)

Step 4 In the node view, double-click the Ethernet card that will carry the cross-connect.

Step 5 Verify that the Ethernet cards that will carry the circuit are provisioned for single-card EtherSwitch. See the "DLP-A246 Provision E-Series Ethernet Card Mode" task on page 19-28.

Step 6 From the View menu, choose **Go to Network View**.

Step 7 Click the **Circuits** tab and click **Create**.

Step 8 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).

Step 9 Click **Next**.

Step 10 Define the circuit attributes:

- Name—Assign a name to the cross-connect. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the cross-connect.
- Size—Choose the cross-connect size. For single-card EtherSwitch, the available sizes are STS-1, STS-3c, STS-6c, and STS-12c.
- Bidirectional—Leave the default unchanged (checked).
- Create cross-connects only (TL1-like)—Uncheck this box.
- State—The circuit is in service (default).
- Apply to drop ports—Uncheck this box.
- Protected Drops—Leave the default unchanged (unchecked).

Step 11 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12.

Step 12 Click **Next**.

Step 13 Provision the circuit source:

a. From the Node drop-down list, choose the cross-connect source node.

b. From the Slot drop-down list, choose the Ethernet card where you enabled the single-card EtherSwitch in Step 5.

Step 14 Click **Next**.

Step 15 Provision the circuit destination:

a. From the Node drop-down list, choose the cross-connect circuit source node selected in Step 13. (For Ethernet cross-connects, the source and destination nodes are the same.)

b. From the Slot drop-down list, choose the OC-N card that is connected to the non-ONS equipment.

c. Depending on the OC-N card, choose the port and/or STS from the Port and STS drop-down lists.

Step 16 Click **Next**.

Step 17 Review the VLANs listed in the Available VLANs list. If the VLAN you want to use appears, continue with Step 18. If you need to create a new VLAN, complete the following steps:

a. Click the **New VLAN** button.

b. In the Define New VLAN dialog box, complete the following:

- VLAN Name—Assign an easily identifiable name to your VLAN.
- VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.
- Topology Host—Choose the topology host ID from the drop-down list.

c. Click **OK**.

Tip You can also add VLANs in network view by choosing **Tools > Manage VLANs**. In the All VLANs dialog box, click the **Create** button to open the Define New VLAN dialog box.

Step 18 Click the VLAN that you want to use in the Available VLANs column, then click the arrow button (**>>**) to move the VLAN to the Circuit VLANs column.

Step 19 Click **Next**.

Step 20 In the Circuit Attributes area, confirm that the following information about the single-card EtherSwitch manual cross-connect is correct (in this task, "circuit" refers to the Ethernet cross-connect):

- Circuit name
- Circuit type
- Circuit size
- VLAN names
- ONS nodes

Step 21 If the information is not correct, click the **Back** button and repeat Steps 8 through 20 with the correct information. If the information is correct, check **Route Automatically**.

Step 22 Click **Finish**.

Step 23 Complete the "DLP-A220 Provision E-Series Ethernet Ports" task on page 19-13 for each node that carries the circuit.

Step 24 Complete the "DLP-A221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 19-14 for each node that carries the circuit.

Stop. You have completed this procedure.

NTP-A145 Create an E-Series Multicard EtherSwitch Manual Cross-Connect

Purpose	This procedure manually creates multicard EtherSwitch cross-connects between E-Series Ethernet cards and an OC-N cards connected to non-ONS equipment.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed at the circuit source node.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note In this procedure, cross-connect refers to a circuit connection created within the same node between the Ethernet card and an OC-N card connected to third-party equipment. You create cross-connects at the source and destination nodes so an Ethernet circuit can be routed from source to destination across third-party equipment.

Note This procedure requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A99 Determine Available VLANs" task on page 17-94 to verify that sufficient VLAN capacity is available. (You will create a VLAN during each circuit creation task.)

Step 3 Verify that the Ethernet card that will carry the circuit is provisioned for Multicard EtherSwitch Group. See the "DLP-A246 Provision E-Series Ethernet Card Mode" task on page 19-28.

Step 4 Provision and enable the Ethernet ports. See the "DLP-A220 Provision E-Series Ethernet Ports" task on page 19-13.

Step 5 From the View menu, choose **Go to Network View**.

Step 6 Click the **Circuits** tab and click **Create**.

Step 7 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.

Step 8 Click **Next**.

Step 9 Define the circuit attributes:

- Name—Assign a name to the source cross-connect. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the source cross-connect.
- Size—Choose the size of the circuit that will be carried by the cross-connect. For multicard EtherSwitch circuits, the available sizes are STS-1, STS-3c, and STS-6c.
- Bidirectional—Leave checked (default).
- Create cross-connects only (TL1-like)—Uncheck this box.
- State—The circuit is in service (default).
- Apply to drop ports—Uncheck this box.
- Protected Drops—Leave the default unchanged (unchecked).

Step 10 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12.

Step 11 Click **Next**.

Step 12 Provision the cross-connect source:

a. From the Node drop-down list, choose the cross-connect source node.

b. From the Slot drop-down list, choose **Ethergroup**.

Step 13 Click **Next**.

Step 14 From the Node drop-down list in the Destination area, choose the circuit source node selected in Step 12. For Ethernet cross-connects, the source and destination nodes are the same.

The Slot field is provisioned automatically for Ethergroup.

Step 15 Click **Next**.

Step 16 Review the VLANs listed in the Available VLANs list. If the VLAN you want to use appears, continue with Step 18. If you need to create a new VLAN, complete the following steps:

a. Click the **New VLAN** button.

b. In the Define New VLAN dialog box, complete the following:

- VLAN Name—Assign an easily identifiable name to your VLAN.
- VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.
- Topology Host—Choose the topology host ID from the drop-down list.

c. Click **OK**.

Tip You can also add VLANs in network view by choosing **Tools > Manage VLANs**. In the All VLANs dialog box, click the **Create** button to open the Define New VLAN dialog box.

Step 17 In the Available VLANs column, click the VLAN that you want to use and click the arrow button (**>>**) to move the VLAN to the Circuit VLANs column.

Step 18 Click **Next**.

Step 19 In the Circuit Attributes area, confirm that the following information is correct:

- Circuit name

- Circuit type
- Circuit size
- VLANs
- ONS nodes

Step 20 If the information is not correct, click the **Back** button and repeat Steps 7 through 19 with the correct information. If the information is correct, check **Route Automatically**.

Step 21 Click **Finish**.

Step 22 Complete the "DLP-A220 Provision E-Series Ethernet Ports" task on page 19-13.

Step 23 Complete the "DLP-A221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 19-14.

Step 24 From the View menu, choose **Go to Home View**.

Step 25 Click the **Circuits** tab.

Step 26 Highlight the circuit and click **Edit**.

The Edit Circuit dialog box appears.

Step 27 In the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops appears.

Step 28 Click **Create**.

Step 29 In the Define New Drop dialog box, define the new drop:

a. Node—Choose the target node for the circuit drop.

b. Slot—Choose the OC-N card that links the ONS 15454 to the non-ONS 15454 equipment.

c. Port, STS—Choose the port and/or STS from the Port and STS drop-down lists.

d. The routing preferences for the new drop match those of the original circuit. However, if the following options are available, you can modify them:

- If the original circuit was routed on a protected path protection path, you can change the nodal diversity options: Nodal Diversity Required, Nodal Diversity Desired, or Link Diversity Only.
- If the original circuit was not routed on a protected path, the Protection Channel Access option is available.

e. If you want to change the circuit state, choose the circuit state from the Target Circuit Admin State drop-down list. The state chosen applies to the entire circuit.

f. Check **Apply to drop ports** if you want to apply the state chosen in the Target Circuit Admin State to the circuit source and destination drops. For the requirements necessary to apply a service state to drop ports, refer to the *Cisco ONS 15454 Reference Manual*.

g. Click **Finish**. The new drop appears in the Drops list.

Step 30 Confirm the circuit information that appears in the Edit Circuit dialog box and click **Close**.

Step 31 Repeat Steps 2 through 30 at the second Ethernet manual cross-connect endpoint.

The first and second Ethernet manual cross-connect endpoints will be bridged by the OC-N STS cross-connect circuit.

Note The appropriate STS circuit must exist in the non-ONS equipment to connect the two Ethernet manual cross-connect endpoints.

Caution If a CARLOSS alarm repeatedly appears and clears on an Ethernet manual cross-connect, the two Ethernet circuits might have a circuit-size mismatch. For example, a circuit size of STS-3c was configured on the first ONS 15454 and circuit size of STS-12c was configured on the second ONS 15454. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if the alarm persists.

Step 32 Complete the "NTP-A146 Test E-Series Circuits" procedure on page 6-73.

Stop. You have completed this procedure.

NTP-A146 Test E-Series Circuits

Purpose	This procedure tests circuits created on E-Series Ethernet cards provisioned for multicard EtherSwitch, single-card EtherSwitch, or port-mapped mode.
Tools/Equipment	Ethernet test set and appropriate fibers
Prerequisite Procedures	This procedure assumes that you completed facility loopback tests to test the fibers and cables from the source and destination ONS 15454s to the fiber distribution page or the DSX, and one of the following procedures: NTP-A191 Create an E-Series EtherSwitch Circuit (Multicard or Single-Card Mode), page 6-57 NTP-A192 Create a Circuit for an E-Series Card in Port-Mapped Mode, page 6-60 NTP-A142 Create an E-Series Shared Packet Ring Ethernet Circuit, page 6-62 NTP-A143 Create an E-Series Hub-and-Spoke Ethernet Configuration, page 6-65 NTP-A145 Create an E-Series Multicard EtherSwitch Manual Cross-Connect, page 6-70
Required/As Needed	As needed
Onsite/Remote	Onsite
Security	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the ONS 15454 source Ethernet node.

Step 2 On the shelf graphic, double-click the circuit source card.

Step 3 Click the **Provisioning > Port** tabs.

Step 4 Verify the following settings:

- Mode—Auto, 10 Half, 10 Full, 100 Half, or 100 Full.
- Enabled—Checked.
- Priority—Set to the priority level indicated by the circuit or site plan. Priority does not apply to E-Series cards in port-mapped mode.

- Stp State—Checked if Spanning Tree Protocol (STP) is enabled for the circuit. STP does not apply to E-Series cards in port-mapped mode.

Step 5 Click the **VLAN** tab. If the E-Series cards is not in port-mapped mode, verify that the source port is on the same VLAN as the destination port.

Step 6 Repeat Steps 1 through 5 for the destination node.

Step 7 At the destination node, connect the Ethernet test set to the destination port and configure the test set to send and receive the appropriate Ethernet traffic.

Note At this point, you are not able to send and receive Ethernet traffic.

Step 8 At the source node, connect an Ethernet test set to the source port and configure the test set to send and receive the appropriate Ethernet traffic.

Step 9 Transmit Ethernet frames between both test sets. If you cannot transmit and receive Ethernet traffic between the nodes, repeat Steps 1 through 8 to make sure that you configured the Ethernet ports and test set correctly.

Step 10 Perform protection switch testing appropriate to the SONET topology:

- For path protection configurations, see the "DLP-A94 Path Protection Configuration Protection Switching Test" task on page 17-90.
- For BLSRs see the "DLP-A91 BLSR Switch Test" task on page 17-83.

Configure your test set according to local site practice. For information about configuring your test set, see your test set user guide.

Step 11 After the Ethernet test is complete, print the results or save them to a disk for future reference. For information about printing or saving test results, see your test set user guide.

Stop. You have completed this procedure.

NTP-A148 Create a Manual Cross-Connect for a G-Series or E-Series Card in Port-Mapped Mode

Purpose	This procedure creates a manual cross-connect between a G-Series Ethernet card or an E-Series Ethernet card in port-mapped mode and an OC-N card connected to non-ONS equipment.
Tools/Equipment	A G-Series or E-Series card must be installed at the circuit source node.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Note In this procedure, cross-connect refers to a circuit connection created within the same node between the Ethernet card and an OC-N card connected to third-party equipment. You create cross-connects at the source and destination nodes so an Ethernet circuit can be routed from source to destination across third-party equipment.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the cross-connect. If you are already logged in, continue with Step 2.

Step 2 If you are provisioning an E-Series card, verify that the Ethernet card that will carry the circuit is provisioned for port-mapped mode. See the "DLP-A246 Provision E-Series Ethernet Card Mode" task on page 19-28.

Step 3 If you are provisioning a G-Series card, complete the "DLP-A222 Provision G-Series Ethernet Ports" task on page 19-15.

Step 4 If you want to change the default flow control settings, complete the "DLP-A421 Provision G-Series and CE-1000-4 Flow Control Watermarks" task on page 21-6.

Step 5 Click the **Circuits** tab and click **Create**.

Step 6 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.

Step 7 Click **Next**.

Step 8 Define the circuit attributes:

- Name—Assign a name to the source cross-connect. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the source cross-connect.
- Size—Choose the size of the circuit that will be carried by the cross-connect. Valid sizes for a G-Series circuit are STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, and STS-48c. For an E-Series card in port-mapped mode, valid sizes are STS-1, STS-3c, STS-6c, and STS-12c.
- Bidirectional—Leave the default unchanged (checked).
- Create cross-connects only (TL1-like)—Uncheck this box.
- State—The circuit is in service (default).
- Apply to drop ports—Uncheck this box.
- Protected Drops—Leave the default unchanged (unchecked).

Step 9 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12.

Step 10 Click **Next**.

Step 11 Provision the circuit source:

a. From the Node drop-down list, choose the circuit source node.

b. From the Slot drop-down list, choose the Ethernet card that will be the cross-connect source.

c. From the Port drop-down list, choose the cross-connect source port.

Step 12 Click **Next**.

Step 13 Provision the circuit destination:

a. From the Node drop-down list, choose the cross-connect source node selected in Step 11. (For Ethernet cross-connects, the source and destination nodes are the same.)

b. From the Slot drop-down list, choose the OC-N card that connects to the non-ONS equipment.

c. Depending on the OC-N card, choose the port and STS from the Port and STS drop-down lists.

Step 14 Click **Next**.

Step 15 In the Circuit Attributes area, confirm that the following information is correct:

- Circuit name
- Circuit type
- Circuit size
- ONS nodes

Step 16 If the information is not correct, click the **Back** button and repeat Steps 5 through 15 with the correct information. If the information is correct, check **Route Automatically**.

Step 17 Click **Finish**.

Step 18 Complete the "NTP-A149 Test G-Series Circuits" procedure on page 6-79.

Stop. You have completed this procedure.

NTP-A241 Provision G-Series Ports for Transponder Mode

Purpose	This procedure provisions G-Series ports into transponder mode.
Tools/Equipment	None
Prerequisite Procedures	DLP-A222 Provision G-Series Ethernet Ports, page 19-15
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will provision G-Series ports. If you are already logged in, continue with Step 2.

Step 2 In the node view, double-click the G-Series card graphic to open the card.

Step 3 Click the **Provisioning > Port** tabs.

Step 4 To put a pair of G-Series card ports in two-port bidirectional transponder mode (Figure 6-11):

Note In Step 4, "Port A" represents the first port in a pair and "Port B" the second port in the pair. You can pair any two ports on a G-Series card in two-port bidirectional mode.

a. Click the Port A row (for example, Port 1).

b. In the TXP Port column, choose the port number that reflects Port A (for example, Port 1).

c. In the TXP Mode column, choose **TX/RX** from the drop-down list.

d. Click a Port B row (for example, Port 2).

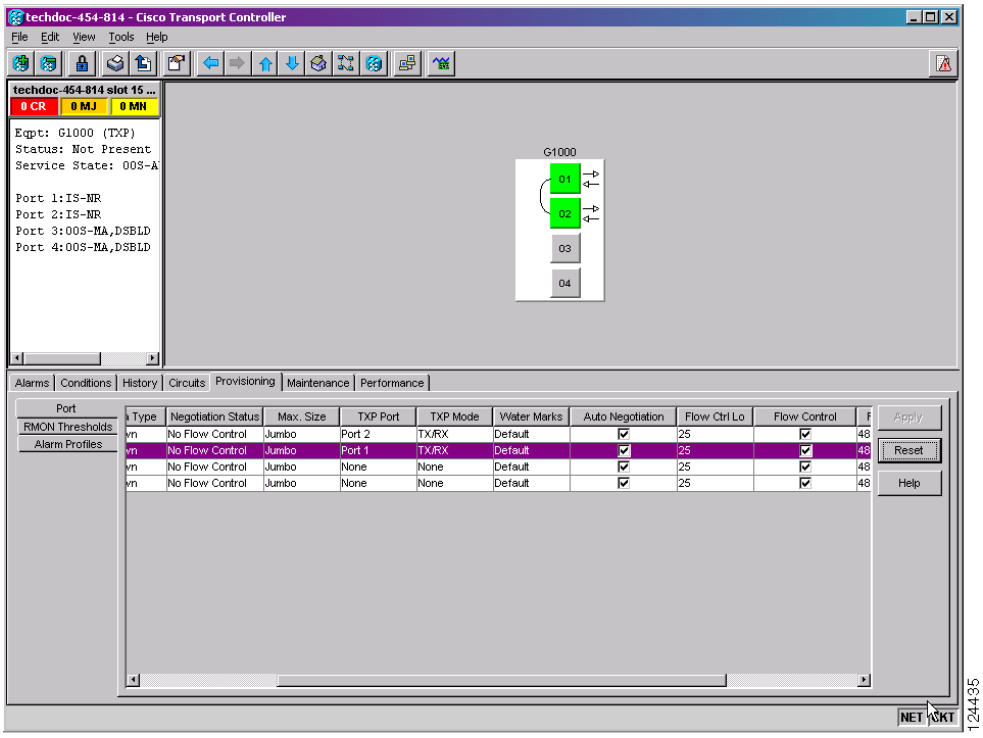
e. In the TXP Port column, choose Port A (for example, Port 1) from the drop-down list.

f. In the TXP Mode column, choose **TX/RX** from the drop-down list.

g. Click **Apply**.

The ports in card view have arrows and a connecting line between the backs of the ports.

Figure 6-11 Two-Port Bidirectional Transponder Mode



Step 5 To put a G-Series card port in one-port bidirectional transponder mode (Figure 6-12):

a. Click the desired port row (for example, Port 1).

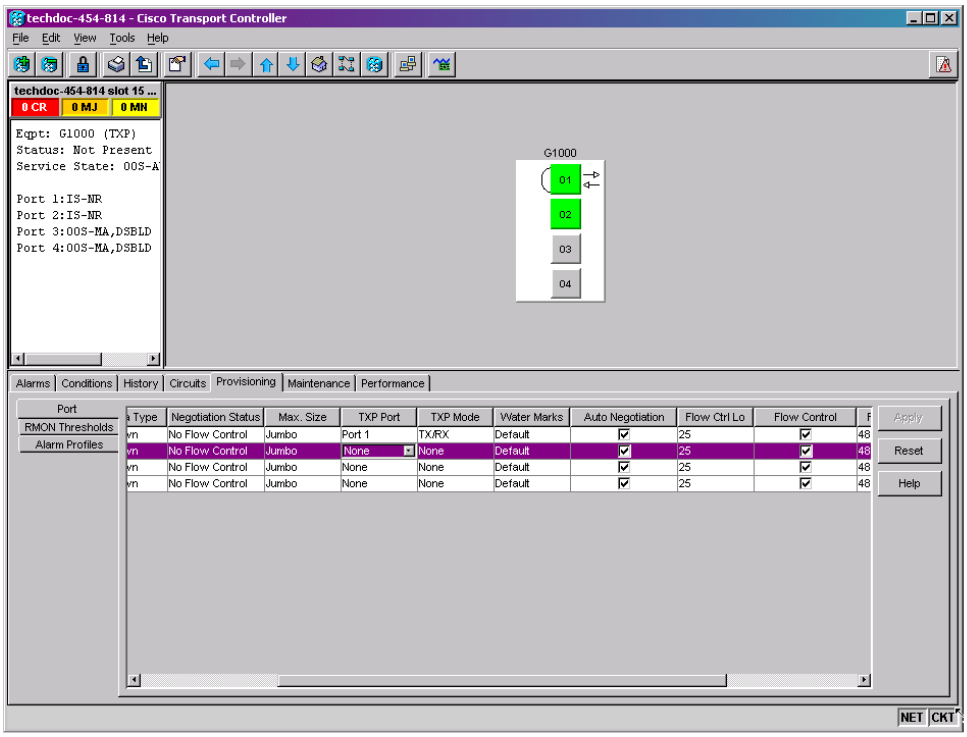
b. In the TXP Port column, choose the desired port from the drop-down list (for example, Port 1).

c. In the TXP Mode column, choose **TX/RX** from the drop-down list.

d. Click **Apply**.

In card view, the desired port has arrows and a curved line on the back of the port.

Figure 6-12 One-Port Bidirectional Transponder Mode



Step 6 To provision two-port unidirectional transponder mode (Figure 6-13):

Note In Step 6, "Port A" represents the first port in a pair and "Port B" the second port in the pair. You can pair any two ports on a G-Series card in two-port unidirectional mode.

a. Click the Port A row (for example, Port 1).

b. Uncheck Auto Negotiation. Ports cannot be provisioned in unidirectional transponder mode when autonegotiation is enabled.

c. In the TXP Port column, choose Port B (for example, Port 2) from the drop-down list.

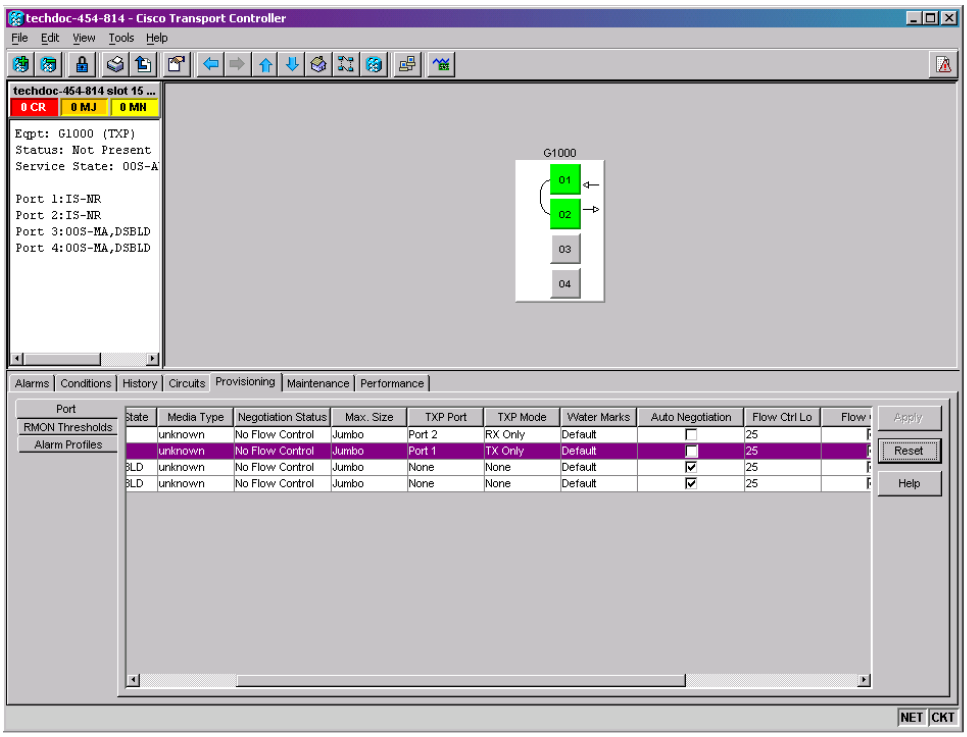
d. In the TXP Mode column, choose **RX Only** from the drop-down list. CTC completes the Port B TXP Port with Port A and TXP Mode with TX Only.

e. Click the Port B row and uncheck Auto Negotiation.

f. Click **Apply**.

The ports on the CTC card level view display arrows and a line between the back of the ports.

Figure 6-13 Two-Port Unidirectional Transponder Mode



Stop. You have completed this procedure.

NTP-A149 Test G-Series Circuits

Purpose	This procedure tests circuits created on G-Series cards.
Tools/Equipment	Ethernet test set and appropriate fibers
Prerequisite Procedures	This procedure assumes that you completed facility loopback tests to test the fibers and cables from the source and destination ONS 15454s to the fiber distribution page or the DSX, and one of the following procedures: NTP-A343 Create an Automatically Routed Optical Circuit, page 6-40 NTP-A344 Create a Manually Routed Optical Circuit, page 6-45 NTP-A148 Create a Manual Cross-Connect for a G-Series or E-Series Card in Port-Mapped Mode, page 6-74
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you created the circuit.

Step 2 Complete the "DLP-A230 Change a Circuit Service State" task on page 19-19 to change the circuit and circuit ports to the OOS-MA,MT service state.

Step 3 On the shelf graphic, double-click the circuit source card.

Step 4 Click the **Provisioning > Port** tabs.

Step 5 Verify the following settings:

- State—OOS,MT
- Flow Control Neg—Checked or unchecked as indicated by the circuit or site plan
- Max Size—Jumbo or 1548 as indicated by the circuit or site plan
- Media Type—SX, LX, ZX, CWDM, or DWDM

Step 6 Repeat Steps 1 through 5 for the destination node.

Step 7 At the destination node, connect the Ethernet test set to the destination port and configure the test set to send and receive the appropriate Ethernet traffic.

Note At this point, you are not able to send and receive Ethernet traffic.

Step 8 At the source node, connect an Ethernet test set to the source port and configure the test set to send and receive the appropriate Ethernet traffic.

Step 9 Transmit Ethernet frames between both test sets. If you cannot transmit and receive Ethernet traffic between the nodes, repeat Steps 1 through 8 to make sure you configured the Ethernet ports and test set correctly.

Step 10 Perform protection switch testing appropriate to the SONET topology:

- For path protection configurations, complete the "DLP-A94 Path Protection Configuration Protection Switching Test" task on page 17-90.
- For BLSRs, complete the "DLP-A91 BLSR Switch Test" task on page 17-83.

Configure your test set according to local site practice. For information about configuring your test set, see your test set user guide.

Step 11 Complete the "DLP-A230 Change a Circuit Service State" task on page 19-19 to change the circuit and circuit ports to the IS-NR service state.

Step 12 After the circuit test is complete, print the results or save them to a disk for future reference. For information about printing or saving test results, see your test set user guide.

Stop. You have completed this procedure.

NTP-A264 Create an Automatically Routed VCAT Circuit

Purpose	This procedure creates an automatically routed VCAT circuit. For more information about VCAT circuits, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
Tools/Equipment	CE-100T-8, CE-1000-4, CE-MR-10, FC_MR-4, or ML-Series cards must be installed at the nodes used in the VCAT circuit.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This procedure requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the VCAT circuit. If you are already logged in, continue with Step 2.

Step 2 Complete the following as necessary (you can provision Ethernet or POS ports before or after the VCAT circuit is created):

- To provision Ethernet ports for CE-1000-4 circuits, complete the "DLP-A509 Provision CE-1000-4 Ethernet Ports" task on page 22-3.
- To provision Ethernet ports for CE-100T-8 or CE-MR-10 circuits, complete the "DLP-A513 Provision CE-100T-8 and CE-MR-10 Ethernet Ports" task on page 22-7.
- To provision POS ports for CE-Series circuits, complete the "DLP-A514 Provision CE-100T-8, CE-1000-4, and CE-MR-10 POS Ports" task on page 22-8.
- To provision Ethernet ports for ML-Series circuits, complete the "DLP-A596 Provision the Ethernet Port of the ML-Series Card" task on page 22-104.
- To provision POS ports for ML-Series circuits, complete the "DLP-A597 Provision the POS Port of the ML-Series Card" task on page 22-105.
- To provision a VCAT circuit that traverses through a third-party network, complete the "NTP-A326 Create a Server Trail" procedure on page 6-93.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, choose **STS-V** or **VT-V** from the Circuit Type drop-down list. To create VT-V circuits, a CE-100T-8 or CE-MR-10 card must be installed or preprovisioned.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-14 on page 6-83):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Displays the circuit type you chose in Step 5. You cannot change it.

- Bidirectional—Checked is the default. You cannot change it.
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits.
- State—Choose **IS**.
- Apply to drop ports—Check this check box to apply the IS administrative state to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box shows the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not change the service state of the source and destination ports.

Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.

- Symmetric—Checked is the default. You cannot change it.
- Open VCAT—Check this check box if you are creating open-ended VCAT circuits. For more information on open-ended VCAT, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Member size—Choose the member size. For information about the member size supported for each card, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Num. of members—Choose the number of members. For information about the number of members supported for each card, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.

Note When creating open-ended VCAT circuits the number of members must be the same on each side of the virtual concatenated group (VCG). The configuration with different number of members on each side of circuit is not supported. This is applicable to circuits created on CE-Series and ML-Series cards.

- Mode—Choose the protection mode for the VCAT circuit. For information about the mode supported for each card, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
  - None—Provides no protection. A failure on one member causes the entire VCAT circuit to fail. For CE-Series cards, you can add or delete members after creating a VCAT circuit with no protection. During the time it takes to add or delete members (from seconds to minutes), the entire VCAT circuit will be unable to carry traffic. For all other cards, you cannot add or delete members if the protection mode is None.
  - SW-LCAS—(Software link capacity adjustment scheme [LCAS]) Allows the VCAT circuit to adapt to member failures and keep traffic flowing after failures at a reduced bandwidth. Sw-LCAS uses legacy SONET failure indicators like path alarm indication signal (AIS-P) and path remote defect indication (RDI-P) to detect member failure.

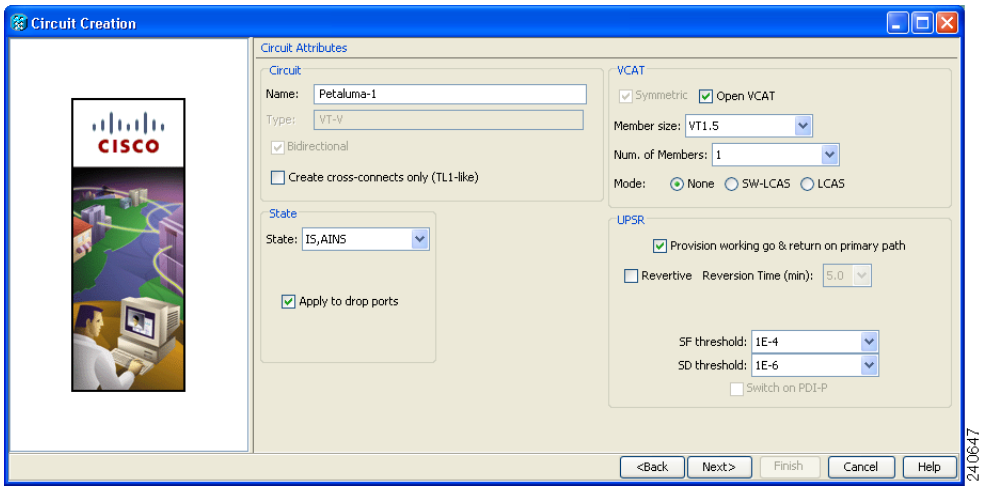
Note While deleting SW-LCAS circuit members change the administrative state of the members to OOS,DSBLD. This is applicable to circuits created on CE-Series and ML-Series cards.

– LCAS—Sets the VCAT circuit to use LCAS. With LCAS, you can add or delete members without interrupting the operation of uninvolved members, and if a member fails, LCAS temporarily removes the failed member from the VCAT circuit. The remaining members carry the traffic until the failure clears.

Note Cisco recommends using LCAS for CE-100T-8 cards that do not need to interoperate with ML-Series cards.

Note While deleting HW-LCAS circuit members change the administrative state of the members to OOS,OOG. This is applicable to circuits created on CE-Series and ML-Series cards.

Figure 6-14 Setting VCAT Circuit Attributes



Step 8 Click **Next**.

Step 9 Complete the "DLP-A324 Provision a VCAT Circuit Source and Destination" task on page 20-14 for the VCAT circuit you are creating. If you are creating an open-ended VCAT circuit, complete the "DLP-A579 Provision an Open VCAT Circuit Source and Destination" task on page 22-92.

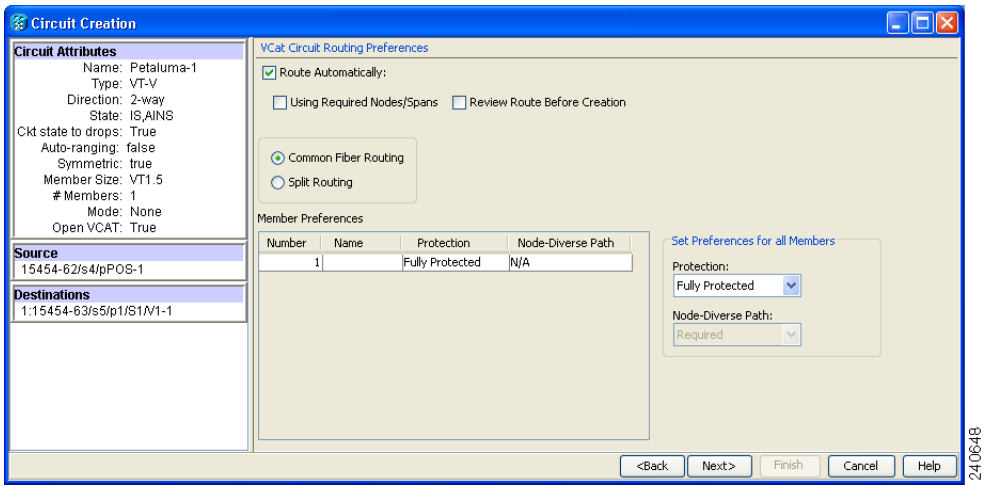
Step 10 In the VCAT Circuit Routing Preferences area (Figure 6-15), check **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- Using Required Nodes/Spans—Check this check box to specify nodes and spans to include or exclude in the CTC-generated circuit route.

  Including nodes and spans for a circuit ensures that those nodes and spans are in the working path of the circuit (but not the protect path). Excluding nodes and spans ensures that the nodes and spans are not in the working or protect path of the circuit.

- Review Route Before Creation—Check this check box to review and edit the circuit route before the circuit is created.

Figure 6-15 Automatically Routing a VCAT Circuit



Step 11 If the VCAT circuit has a source or destination on a CE-Series card, choose one of the following routing types.

- Common Routing—Routes the members on the same fiber.
- Split Routing—Allows the individual members to be routed on different fibers or each member to have different routing constraints. Split routing is required when creating circuits over a path protection configuration.

If the VCAT circuit does not have a source or destination on a CE-Series card, common routing is automatically selected and you cannot change it.

Step 12 If you want to set preferences for individual members, complete the following in the Member Preferences area. Repeat for each member. To set identical preferences for all members, skip this step and continue with Step 13:

- Number—Choose a number (between 1 and 256) from the drop-down list to identify the member.
- Name—Type a unique name to identify the member. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the circuit.
- Protection—Choose the member protection type:
  - Fully Protected—Routes the circuit on a protected path.
  - Unprotected—Creates an unprotected circuit.
  - PCA—Routes the circuit on a BLSR protection channel.
  - DRI—(Split routing only) Routes the member on a dual-ring interconnect circuit.
- Node-Diverse Path—(Split routing only) Available for each member when Fully Protected is chosen.

Step 13 To set preferences for all members, complete the following in the Set Preferences for All Members area:

- Protection—Choose the member protection type:
  - Fully Protected—Routes the circuit on a protected path.
  - Unprotected—Creates an unprotected circuit.
  - PCA—Routes the member on a BLSR protection channel.

  - DRI—(Split routing only) Routes the member on a dual-ring interconnect circuit.
- Node-Diverse Path—(Split routing only) Available when Fully Protected is chosen.

Step 14 Click **Next**. If you chose Fully Protected or PCA, click **OK** to continue. If not, continue with the next step.

Step 15 If you selected Using Required Nodes/Spans in Step 10, complete the following substeps. If not, continue with Step 16:

a. In the Circuit Constraints area (Figure 6-16), choose the member that you want to route from the Route member number drop-down list.

b. Click a node or span on the circuit map.

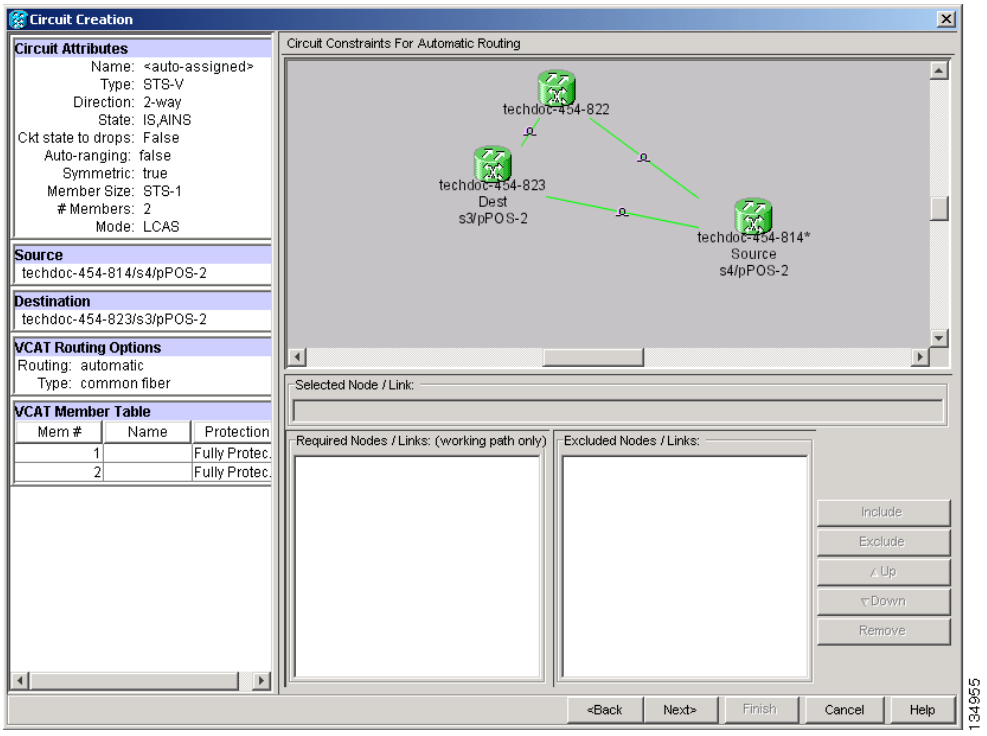
c. Click **Include** to include the node or span in the circuit, or click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans is the order in which the circuit is routed. Click spans twice to change the circuit direction.

d. Repeat Steps b and c for each node or span you wish to include or exclude.

e. Review the circuit route. To change the circuit routing order, choose a node in the Required Nodes/Lines or Excluded Nodes Links lists, then click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

f. Repeat Steps a through e for each member.

Figure 6-16 VCAT Circuit Route Constraints



Step 16 If you selected Review Route Before Creation in Step 10, complete the following substeps; otherwise, continue with Step 17:

a. In the Route Review/Edit area, choose the member that you want to route from the Route member number drop-down list.

b. Click a node or span on the circuit map.

c. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

d. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the "NTP-A265 Create a Manually Routed VCAT Circuit" procedure on page 6-86 to assign the circuit route yourself.

e. Repeat Steps a through d for each member.

Step 17 Click **Finish**. The Circuits window appears.

Note Depending on the complexity of the network and number of members, the VCAT circuit creation process can take several minutes.

Step 18 In the Circuits window, verify that the circuit you created appear in the circuits list.

Stop. You have completed this procedure.

NTP-A265 Create a Manually Routed VCAT Circuit

Purpose	This procedure creates a manually routed VCAT circuit. For more information about VCAT circuits, refer to the "Circuits and Tunnels" chapter of the *Cisco ONS 15454 Reference Manual*.
Tools/Equipment	CE-100T-8, CE-1000-4, CE-MR-10, FC_MR-4, or ML-Series cards must be installed at the nodes used in the VCAT circuit.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 Complete the following as necessary (you can provision Ethernet or POS ports before or after the VCAT circuit is created):

- To provision Ethernet ports for CE-1000-4 circuits, complete the "DLP-A509 Provision CE-1000-4 Ethernet Ports" task on page 22-3.
- To provision Ethernet ports for CE-100T-8 or CE-MR-10 circuits, complete the "DLP-A513 Provision CE-100T-8 and CE-MR-10 Ethernet Ports" task on page 22-7.
- To provision POS ports for CE-Series circuits, complete the "DLP-A514 Provision CE-100T-8, CE-1000-4, and CE-MR-10 POS Ports" task on page 22-8.

- To provision Ethernet ports for ML-Series circuits, complete the "DLP-A596 Provision the Ethernet Port of the ML-Series Card" task on page 22-104.
- To provision POS ports for ML-Series circuits, complete the "DLP-A597 Provision the POS Port of the ML-Series Card" task on page 22-105.
- To provision a VCAT circuit that traverses through a third-party network, complete the "NTP-A326 Create a Server Trail" procedure on page 6-93.

Step 4 From the View menu, choose **Go to Network View**.

Step 5 In the Circuit Creation dialog box, choose **STS-V** or **VT-V** from the Circuit Type drop-down list. To create VT-V circuits, a CE-100T-8 or CE-MR-10 card must be installed or preprovisioned.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-14 on page 6-83):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Displays the circuit type you chose in Step 5. You cannot change it.
- Bidirectional—Checked is the default. You cannot change it.
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits.
- State—Choose **IS**.
- Apply to drop ports—Check this check box to apply the IS administrative state to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box shows the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not change the service state of the source and destination ports.
- Symmetric—Checked is the default. You cannot change it.
- Open VCAT—Check this check box if you are creating open-ended VCAT circuits. For more information on open-ended VCAT refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Member size—Choose the member size. For information about the member size supported for each card, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Num. of members—Choose the number of members. For information about the number of members supported for each card, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*. You can add additional members using the **Edit** circuit function.

Note When creating open-ended VCAT circuits the number of members must be the same on each side of the virtual concatenated group (VCG). The configuration with different number of members on each side of circuit is not supported. This is applicable to circuits created on CE-Series and ML-Series cards.

- Mode—Choose the protection mode for the VCAT circuit. For information about the mode supported for each card, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.

- None—Provides no protection. A failure on one member causes the entire VCAT circuit to fail. For CE-Series cards, you can add or delete members after creating a VCAT circuit with no protection. During the time it takes to add or delete members (from seconds to minutes), the entire VCAT circuit will be unable to carry traffic. For all other cards, you cannot add or delete members if the protection mode is None.
- SW-LCAS—Allows the VCAT circuit to adapt to member failures and keep traffic flowing after failures at a reduced bandwidth. Sw-LCAS uses legacy SONET failure indicators like AIS-P and RDI-P to detect member failure.

Note While deleting SW-LCAS circuit members change the administrative state of the members to OOS,DSBLD. This is applicable to circuits created on CE-Series and ML-Series cards.

- LCAS—Sets the VCAT circuit to use LCAS. With LCAS, you can add or delete members without interrupting the operation of uninvolved members, and if a member fails, LCAS temporarily removes the failed member from the VCAT circuit. The remaining members carry the traffic until the failure clears.

Note Cisco recommends using LCAS for CE-T100-8 cards that do not need to interoperate with the ML-Series cards.

Note While deleting HW-LCAS circuit members change the administrative state of the members to OOS,OOG. This is applicable to circuits created on CE-Series and ML-Series cards.

Step 8 Click **Next**.

Step 9 Complete the "DLP-A324 Provision a VCAT Circuit Source and Destination" task on page 20-14 for the VCAT circuit you are creating. If you are creating an open-ended VCAT circuit, complete the "DLP-A579 Provision an Open VCAT Circuit Source and Destination" task on page 22-92.

Step 10 In the Circuit Routing Preferences area (Figure 6-15 on page 6-84), uncheck **Route Automatically**.

Step 11 If the VCAT circuit has a source or destination on a CE-Series card, choose one of the following routing types.

- Common Routing—Routes the members on the same fiber.
- Split Routing—Allows the individual members to be routed on different fibers or each member to have different routing constraints. Split routing is required when creating circuits over a path protection configuration.

If the VCAT circuit does not have a source or destination on a CE-Series card, common routing is automatically selected and you cannot change it.

Step 12 If you want to set preferences for individual members, complete the following in the Member Preferences area. Repeat for each member. To set identical preferences for all members, skip this step and continue with Step 13.

- Number—Choose a number (between 1 and 256) from the drop-down list to identify the member.
- Name—Type a unique name to identify the member. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the circuit.
- Protection—Choose the member protection type:

  - Fully Protected—Routes the circuit on a protected path.
  - Unprotected—Creates an unprotected circuit.
  - PCA—Routes the member on a BLSR protection channel.
  - DRI—(Split routing only) Routes the member on a dual-ring interconnect circuit.
- Node-Diverse Path—(Split routing only) Available for each member when Fully Protected is chosen.

Step 13 To set preferences for all members, complete the following in the Set Preferences for All Members area:

- Protection—Choose the member protection type:
  - Fully Protected—Routes the circuit on a protected path.
  - Unprotected—Creates an unprotected circuit.
  - PCA—Routes the member on a BLSR protection channel.
  - DRI—(Split routing only) Routes the member on a dual-ring interconnect circuit.
- Node-Diverse Path—(Split routing only) Available when Fully Protected is chosen.

Step 14 Click **Next**. If you chose Fully Protected or PCA, click **OK** to continue. If not, continue with the next step.

Step 15 In the Route Review and Edit area, node icons appear so you can route the circuit manually.

Step 16 Complete the "DLP-A325 Provision a VCAT Circuit Route" task on page 20-15.

Step 17 Click **Finish**. If the path does not meet the specified path diversity requirement, CTC displays an error message and allows you to change the circuit path.

Note Depending on the complexity of the network and number of members, the VCAT circuit creation process can take several minutes.

Step 18 When all the circuits are created, the main Circuits window appears. Verify that the circuit you created appear in the window.

Stop. You have completed this procedure.

NTP-A194 Create Overhead Circuits

Purpose	This procedure creates overhead circuits on an ONS 15454 network. Overhead circuits include DCC tunnels, IP-encapsulated tunnels, the Alarm Interface Controller–International (AIC-I) card orderwire, and the AIC-I card user data channel (UDC).
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The SDCCs and LDCCs should not be provisioned between SONET (ANSI) and SDH (ETSI) nodes using CTC or TL1 because they cannot operate between SONET and SDH nodes. These communication channels should be provisioned on similar nodes, such as SONET-to-SONET or SDH-to-SDH. To establish communication channels between SONET and SDH nodes, create a DCC tunnel. See the "DLP-A313 Create a DCC Tunnel" task on page 20-7 to create a DCC tunnel.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the overhead circuit. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 As needed, complete the "DLP-A313 Create a DCC Tunnel" task on page 20-7.

Step 4 As needed, complete the "DLP-A341 Create an IP-Encapsulated Tunnel" task on page 20-32.

Step 5 As needed, complete the "DLP-A83 Provision Orderwire" task on page 17-79.

Step 6 As needed, complete the "DLP-A212 Create a User Data Channel Circuit" task on page 19-8.

Stop. You have completed this procedure.

NTP-A167 Create an STS Test Circuit around the Ring

Purpose	This procedure creates an STS test circuit that routes traffic around a ring with the source and destination located on different ports of the same node.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the Circuits tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Enter the number of circuits that you want to create. The default is 1.
- Auto-ranged—(Automatically routed circuits only) If you entered more than 1 in the Number of Circuits field, uncheck this box. (The box is unavailable if only one circuit is entered in the Number of Circuits field.)

Step 6 Click **Next**.

Step 7 Define circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size. Choices are STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-18c, STS-24c, STS-36c, STS-48c, and STS-192c.
- Bidirectional—Leave checked for this circuit (default).
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, VT tunnels and Ethergroup sources and destinations are unavailable.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Puts the circuit cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

  Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.

- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, 1+1, or optimized 1+1 protection. If you check this check box, CTC provides only protected cards as source and destination choices.

Step 8 Click **Next**.

Step 9 Choose the circuit source:

a. From the Node drop-down list, choose the node where the circuit will originate.

b. From the Slot drop-down list, choose the slot containing the card where the circuit originates. (If card capacity is fully utilized, it does not appear in the list.)

c. Depending on the circuit origination card, choose the source port and/or STS from the Port and STS drop-down lists. The Port drop-down list is only available if the card has multiple ports. STSs do not appear if they are already in use by other circuits.

Note The STSs that appear depend on the card, circuit size, and protection scheme.

Step 10 Click **Next**.

Step 11 Choose the circuit destination:

Note The destination port must be located on the same node as the circuit source port.

a. From the Node drop-down list, choose the node selected in Step 9a.

b. From the Slot drop-down list, choose the slot containing the card where the circuit will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the list.)

c. Depending on the card selected in Step b, choose the destination port and/or STS from the Port and STS drop-down lists. The Port drop-down list is available only if the card has multiple ports. The STSs that appear depend on the card, circuit size, and protection scheme.

Step 12 Click **Next**.

Step 13 In the Circuit Routing Preferences area, uncheck **Route Automatically**.

Step 14 When routing a test circuit with source and destination ports on the same node, the Fully Protected Path check box is automatically disabled. Choose one of the following options:

- To leave the test circuit unprotected, continue with Step 15.
- To route the test circuit on a BLSR protection channel, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 15.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 15 Click **Next**.

Step 16 In the Route Review/Edit area, node icons appear for you to route the circuit manually:

a. In the Route Review/Edit area, click the source node icon if it is not already selected.

b. Starting with a span on the source node, click the arrow of the span you want the circuit to travel. To reverse the direction of the arrow, click the arrow twice.

c. The arrow turns white. In the Selected Span area, the From and To fields provide span information. The source STS appears. If you want to change the source STS, adjust the Source STS field; otherwise, continue with Step d.

d. Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

e. Repeat Steps b through d until the circuit is provisioned from the source to the destination node through all intermediary nodes.

Step 17 Click **Finish**. If the path does not meet the specified path diversity requirement, CTC displays an error message and allows you to change the circuit path. If you entered more than 1 in the Number of Circuits field on the Circuit Creation dialog box, the Circuit Creation dialog box appears after the circuit is created so you can create the remaining circuits. Repeat Steps 7 through 16 for each additional circuit.

Step 18 When all the circuits are created, the main Circuits window appears. Verify that the circuits you created appear in the window.

Stop. You have completed this procedure.

NTP-A326 Create a Server Trail

Purpose	This procedure creates a server trail, which provides a connection between ONS nodes through a third-party network. You can create server trails between any two optical ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You cannot create server trails on ports with DCC links.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Provisioning > Server Trails** tabs.

Step 4 Click **Create**.

Step 5 In the Server Trail Creation dialog box, complete the following fields:

- Type—Choose **VT** or **STS**.
- Size—Depending on the type selected, choose the server trail size. For VTs, choose VT1.5 or VT2; for STSs, choose STS1, STS-3c, STS-6c, STS-12c, STS-48c, or STS-192c.
- Protection Type—Choose one of the following protection types: Preemptible, Unprotected, or Fully Protected. The server trail protection sets the protection type for any circuit that traverses it.
  - Preemptible— PCA circuits will use server trails with the Preemptible attribute.
  - Unprotected—In Unprotected Server Trail, CTC assumes that the circuits going out from that specific port will not be protected by provider network and will look for a secondary path from source to destination if you are creating a protected circuit.
  - Fully Protected—In Fully Protected Server Trail, CTC assumes that the circuits going out from that specific port will be protected by provider network and will not look for a secondary path from source to destination.
- Number of Trails—Enter the number of server trails. Number of trails determine the number of circuits that can be created on server trail. You can create a maximum of 3744 server trails on a node. You can create multiple server trails from the same port. This is determined by how many circuits of a particular server trail size can be supported on the port (for example, you can create 12 STS-1 server trails from one OC-12 port or two STS3c and six STS-1 server trails from same port).

- SRLG—Enter a value for the Shared Resource Link Group (SRLG). SRLG is used by Cisco Transport Manager (CTM) to specify link diversity. The SRLG field has no restrictions. If you create multiple server trails from one port, you can assign the same SRLG value to all the links to indicate that they originate from the same port.

Step 6 Click **Next**.

Step 7 In the Source area, complete the following:

- From the Node drop-down list, choose the node where the server trail will originate.
- From the Slot drop-down list, choose the slot containing the card where the server trail originates. (If a card's capacity is fully utilized, the card does not appear in the list.)
- Depending on the origination card, choose the source port and/or STS or VT from the Port and STS or VT lists. The Port list is only available if the card has multiple ports. STSs and VTs do not appear if they are already in use by other circuits.

Step 8 Click **Next**.

Step 9 In the Destination area, complete the following:

- From the Node drop-down list, choose the destination node.
- From the Slot drop-down list, choose the slot containing the card where the server trail will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the list.)
- Depending on the card selected, choose the destination port and/or STS or VT from the Port and STS or VT drop-down lists. The Port drop-down list is available only if the card has multiple ports. The STSs that appear depend on the card, circuit size, and protection scheme.

Step 10 Click **Finish**.

Note When Server Trails are created on an IPv4 or IPv6 node and the IP address of the node changes, complete the "DLP-A599 Repair Server Trails" task on page 22-106 to repair the Server Trails.

Stop. You have completed this procedure.

NTP-A327 Create an Automatically Routed Open-Ended Path Protection Circuit

Purpose	This procedure creates an open-ended STS or VT path protection circuit.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Note This procedure is necessary when you need to route VT traffic between a path protection configuration across an ONS 15600 hub node to a line-protected domain. For more information about the ONS 15600 as a hub node for mixed ONS 15454 protection domains, refer to the "Turn Up Network" chapter in the *Cisco ONS 15600 Procedure Guide* and the "Circuits and Tunnels" chapter in the *Cisco ONS 15600 Reference Manual*.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **VT** or **STS**. If you are creating an open-ended path protection circuit to route VT traffic across an ONS 15600 hub node with mixed protection domains, choose VT.
- Number of Circuits—Enter the number of circuits that you want to create. The default is 1. If you are creating multiple circuits with the same slot and sequential port numbers, you can use Auto-ranged to create the circuits automatically.
- Auto-ranged—This check box is automatically selected if you enter more than 1 in the Number of Circuits field. Auto-ranging creates identical (same source and destination) sequential circuits automatically. Uncheck the box if you do not want CTC to create sequential circuits automatically.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-1):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters, (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—If the circuit type is VT, choose **VT1.5**. If the circuit type is STS, choose **STS-1**.
- Bidirectional—Leave checked for this circuit (default).
- Create cross-connects only (TL1-like)—Check this check box to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you are creating an open-ended path protection circuit to bridge VT traffic, you must check this check box.
- Diagnostic—Leave unchecked.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Puts the circuit cross-connects in the In-Service and Normal (IS-NR) service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. Traffic is not passed on the circuit.

  - IS,AINS—Puts the circuit cross-connects in the Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS) service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.

- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

  Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.

- Protected Drops—Check this box if you want the circuit routed on protected drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, 1+1, or optimized 1+1 protection. If you check this box, CTC displays only protected cards and ports as source and destination choices.

Step 8 If the circuit will be routed on a path protection configuration, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12. Otherwise, continue with the next step.

Step 9 Click **Next**.

Step 10 Complete one of the following, depending on the source and destination cards. Choose single source and secondary destinations to create the open-ended path protection circuit:

- "DLP-A95 Provision a DS-1 Circuit Source and Destination" task on page 17-91
- "DLP-A510 Provision a DS-3 Circuit Source and Destination" task on page 22-4
- "DLP-A97 Provision an OC-N Circuit Source and Destination" task on page 17-93

Step 11 In the Circuit Routing Preferences area (Figure 6-2), choose **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- Using Required Nodes/Spans—Check this check box if you want to specify nodes and spans to include or exclude in the CTC-generated circuit route.

  Including nodes and spans for a circuit ensures that those nodes and spans are in the working path of the circuit (but not the protect path). Excluding nodes and spans ensures that the nodes and spans are not in the working or protect path of the circuit.

- Review Route Before Creation—Check this check box if you want to review and edit the circuit route before the circuit is created.

Step 12 Leave **Fully Protected Path** checked.

Step 13 Choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within path protection portions of the complete circuit path are nodally diverse.

- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected Using Required Nodes/Spans in Step 11, complete the following substeps. If not, continue with Step 15.

a. Click **Next**.

b. In the Circuit Route Constraints area, click a node or span on the circuit map.

c. Click **Include** to include the node or span in the circuit. Click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans is the order in which the circuit is routed. Click spans twice to change the circuit direction.

d. Repeat Steps b and c for each node or span you wish to include or exclude.

e. Review the circuit route. To change the circuit routing order, choose a node in the Required Nodes/Lines or Excluded Nodes Links lists and click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 15 Click **Next**. If the circuit you are creating is a VT circuit for routing traffic over an ONS 15600 hub node, in the Create area of the VT Matrix Optimization page choose **Create VT tunnel on transit nodes** and click **Next**. If not, continue with Step 16.

This option is available if the circuit passes through a node that does not have a VT tunnel, or if an existing VT tunnel is full. VT tunnels allow VT circuits to pass through ONS 15454s without consuming cross-connect card resources. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the *Cisco Cisco ONS 15454 Reference Manual* for more information.

Step 16 If you selected Review Route Before Creation in Step 11, complete the following substeps. If not, continue with Step 17.

a. Click **Next**.

b. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information.

Step 17 Click **Finish**. One of the following results occurs if you entered more than one circuit in the Number of Circuits field on the Circuit Creation dialog box.

- If you chose Auto-ranged, CTC automatically creates the number of circuits entered in the Number of Circuits field. If auto-ranging cannot complete all the circuits, for example, because sequential ports are unavailable at the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto-ranging. After completing the circuits, the Circuits window appears.
- If you did not choose Auto-ranged, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 5 through 17 for each additional circuit. After completing the circuits, the Circuits window appears.

Step 18 In the Circuits window, verify that the new circuits appear in the circuits list.

Step 19 Complete one of the following to test the circuit. Skip this step if you built a test circuit.

- "NTP-A135 Test Electrical Circuits" procedure on page 6-38

- "NTP-A62 Test Optical Circuits" procedure on page 6-51

Stop. You have completed this procedure.

NTP-A361 Create an Overlay Ring Circuit

Purpose	This procedure creates an overlay ring circuit that routes traffic around multiple rings, passing through one or more nodes more than once.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the Circuits tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Enter the number of circuits that you want to create. The default is 1.
- Auto-ranged—Uncheck this checkbox.

Note If specify the number of circuits as more than 1 and if the auto-ranged check box is selected, the Route Automatically check box in the Circuit Routing Preferences area is automatically checked; this prevents you from creating an overlay ring circuit.

Step 6 Click **Next**.

Step 7 Define circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size. Choices are STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-18c, STS-24c, STS-36c, STS-48c, and STS-192c.
- Bidirectional—Leave checked for this circuit (default).
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, VT tunnels and Ethergroup sources and destinations are unavailable.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:

- IS—Puts the circuit cross-connects in the IS-NR service state.
- OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
- IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
- OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.

- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

Note If ports managed into the IS administrative state are not receiving signals, Loss of Signal (LOS) alarms are generated and the port service state transitions to OOS-AU,FLT.

- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, 1+1, or optimized 1+1 protection. If you check this check box, CTC provides only protected cards as source and destination choices.

Step 8 Click **Next**.

Step 9 Choose the circuit source:

a. From the Node drop-down list, choose the node where the circuit will originate.

b. From the Slot drop-down list, choose the slot containing the card where the circuit originates. (If card capacity is fully utilized, it does not appear in the list.)

c. Depending on the circuit origination card, choose the source port and/or STS from the Port and STS drop-down lists. The Port drop-down list is only available if the card has multiple ports. STSs do not appear if they are already in use by other circuits.

Note The STSs that appear depend on the card, circuit size, and protection scheme.

Step 10 Click **Next**.

Step 11 Choose the circuit destination:

a. From the Node drop-down list, choose the node selected in Step 9a.

b. From the Slot drop-down list, choose the slot containing the card where the circuit will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the list.)

c. Depending on the card selected in Step b, choose the destination port and/or STS from the Port and STS drop-down lists. The Port drop-down list is available only if the card has multiple ports.

Note The STSs that appear depend on the card, circuit size, and protection scheme.

Step 12 Click **Next**.

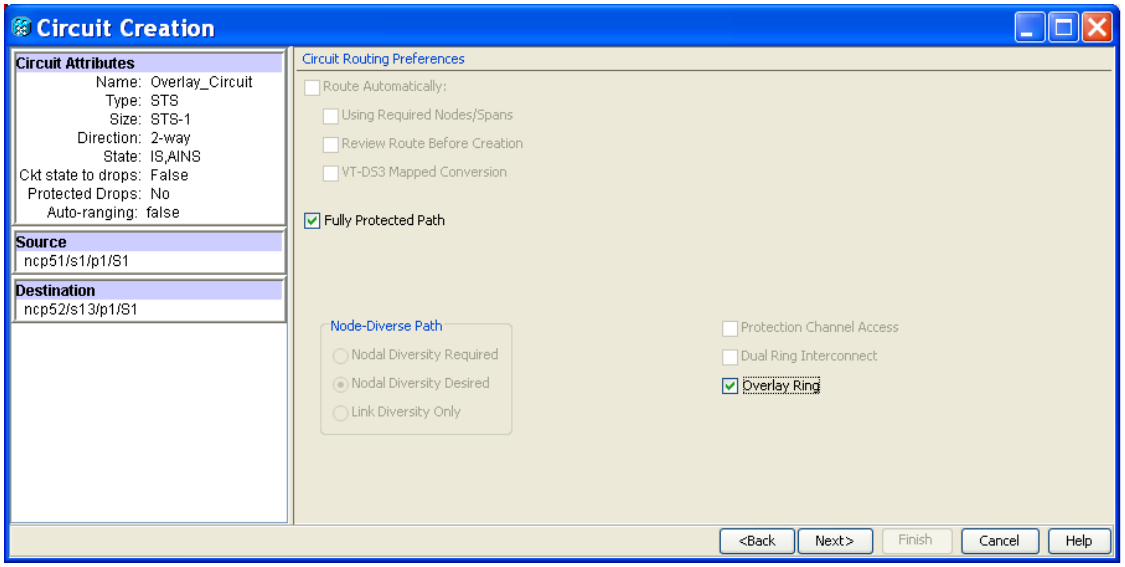
Step 13 In the Circuit Routing Preferences area, uncheck **Route Automatically** to enable the **Overlay Ring** check box.

Step 14 To set the circuit path protection, complete one of the following:

- To create an unprotected circuit, uncheck the **Fully Protected Path** check box.
- To create a protected circuit, check the **Fully Protected Path** check box.

Step 15 Check the **Overlay Ring** check box (Figure 6-17).

Figure 6-17 Overlay Ring Check Box



Step 16 Click **Next**.

Step 17 In the Route Review/Edit area, node icons appear for you to route the circuit manually:

a. In the Route Review/Edit area, click the source node icon if it is not already selected.

b. Starting with a span on the source node, click the arrow of the span you want the circuit to travel. To reverse the direction of the arrow, click the arrow twice.

c. In the Selected Span area, the From and To fields provide span information. The source STS appears. If you want to change the source STS, adjust the Source STS field; otherwise, continue with Step d.

d. Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

e. Repeat Steps b through d until the circuit is provisioned from the source to the destination node through all intermediary nodes.

Note During manual routing, while creating an overlay ring circuit, you can create loops. Creating loops allows you to return to the same node more than once while selecting the spans.

Step 18 Click **Finish**.

Step 19 When all the circuits are created, the main Circuits window appears. Verify that the circuits you created appear in the window.

Stop. You have completed this procedure.

NTP-A362 Create an Ethernet Drop and Continue Circuit

Purpose	This procedure creates a unidirectional Ethernet drop and continue circuit with multiple drops (circuit destinations) on CE-MR-10 cards. **Note** Ethernet drop and continue is supported only on CCAT circuits.
Tools/Equipment	The CE-MR-10 card must be installed at the circuit source and destination nodes.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 To assign a name to the circuit source and destination ports, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 4.

Step 3 To provision the CE-MR-10 card, complete the "NTP-A246 Install Ethernet Cards and Connectors" task on page 2-13.

Step 4 From the View menu, choose **Go to Network View**.

Step 5 Click the **Circuits** tab, then click **Create**.

Step 6 In the Circuit Creation dialog box, choose the following:

- Circuit Type—Choose **STS**.
- Number of Circuits—Enter the number of circuits that you want to create. The default is 1. Leave the default unchanged (1).
- Auto-ranged—Unavailable when the Number of Circuits field is 1.

Step 7 Click **Next**.

Step 8 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose **STS-1**.
- Bidirectional—Uncheck to create a unidirectional circuit.
- Create cross-connects only (TL1-like)—Check this check box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, VT tunnels and Ethergroup sources and destinations are unavailable.

- State—Choose the administrative state to apply to all cross-connects in the circuit:
  - IS—Puts the circuit cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth. If the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

Note If ports in IS administrative state are not receiving signals, LOS (loss of signal) alarms are generated and the service state of ports change to OOS-AU,FLT.

- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, 1+1, or optimized 1+1 protection. If you check this check box, CTC provides only protected cards as source and destination choices.

Step 9 Click **Next**.

Step 10 Uncheck **Route Automatically**. When Route Automatically is not selected, the Using Required Nodes/Spans, Review Route Before Circuit Creation, and VT-DS3 Mapped Conversion check boxes are unavailable.

Step 11 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 12. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 14.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 14.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 12 If you selected Fully Protected Path in Step 11 and the circuit will be routed on a path protection configuration, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 13 If you selected Fully Protected Path in Step 11 and the circuit will be routed on a BLSR DRI or path protection DRI, check the **Dual Ring Interconnect** check box.

Step 14 Click **Next**. In the Route Review/Edit area, node icons appear for you to route the circuit manually. If you checked Dual Ring Interconnect for BLSR, continue with Step 15. If not, continue with Step 16.

Step 15 Complete the "DLP-A564 Configure a Manually Routed BLSR DRI" task on page 22-78.

Step 16 Click **Finish**. After completing the circuit, the Circuits window appears.

Step 17 In the Circuits window, click the circuit that you want to route to multiple drops. The Delete, Edit, and Search radio buttons become active.

Step 18 Click **Edit**. The Edit Circuit window appears with the General tab selected. All nodes in the DCC network appear on the network map. Circuit source and destination information appears under the source and destination nodes. To see a detailed view of the circuit, click **Show Detailed Map**. You can rearrange the node icons by selecting the node with the left mouse button while simultaneously pressing **Ctrl**, then dragging the icon to the new location.

Step 19 In the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops appears.

Step 20 Click **Create**.

Step 21 In the Define New Drop dialog box, define the new drop:

a. Node—Choose the target node for the circuit drop.

b. Slot—Choose the target card and slot.

c. Port, STS—Choose the port and/or STS from the Port and STS drop-down lists. The card selected in Step b determines whether port, STS, or both appear. See Table 6-2 on page 6-3 for a list of options.

d. The routing preferences for the new drop match those of the original circuit. However, if the following options are available, you can modify them:

- If the original circuit was routed on a path protected path, you can change the nodal diversity options: Nodal Diversity Required, Nodal Diversity Desired, or Link Diversity Only. See Step 12 for option descriptions.
- If the original circuit was not routed on a protected path, the Protection Channel Access option is available. See Step 11 for a description of the Protection Channel Access option.

e. If you want to change the circuit state, choose the circuit state from the Target Circuit Admin State drop-down list. The state chosen applies to the entire circuit.

f. Check **Apply to drop ports** if you want to apply the state chosen in the Target Circuit Admin State to the circuit source and destination drops. For the requirements necessary to apply a service state to drop ports, refer to the *Cisco ONS 15454 Reference Manual*.

g. Click **Finish**. The new drop appears in the Drops list.

Step 22 If you need to create additional drops for the circuit, repeat Steps 21a through g to create the additional drops.

Step 23 Click **Close**. The Circuits window appears.

Step 24 Verify that the new drops appear in the Destination column for the circuit you edited. If they do not appear, repeat Steps 21a through g, making sure that all options are provisioned correctly.

Stop. You have completed this procedure.

NTP-A363 Create a Dual Source, Single Destination Circuit

Purpose	This procedure creates a dual source and single destination circuit on an ML-MR-10 card with the card port protection (CPP) enabled.
Tools/Equipment	Two ML-MR-10 cards must be installed at one end of the circuit and a CE-MR-6, CE-MR-10, or ML-MR-10 card at the other end.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 20-8. If not, continue with Step 3.

Step 3 To provision the card mode for ML-Series cards, complete the "DLP-A556 Provision the Card Mode for ML-Series Ethernet Cards" task on page 22-70.

Step 4 From the View menu, choose **Go to Network View**.

Step 5 Click the **Circuits** tab, then click **Create**.

Step 6 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **STS, VT, VT-V,** or **STS-V**.

Note The circuit size varies based on the type of circuit selected.

- Number of Circuits—Enter the number of circuits that you want to create. The default is 1.
- Auto-ranged—This check box is automatically selected when you enter more than 1 in the Number of Circuits field. Leave this check box selected if you are creating multiple optical circuits with the same source and destination and you want CTC to create the circuits automatically. Uncheck the box if you do not want CTC to create the circuits automatically.

Step 7 Click **Next**.

Step 8 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—If the circuit type is VT, choose **VT1.5**. If the circuit type is STS, choose **STS-1**.
- Bidirectional—As desired. When checked, CTC creates a two-way circuit.

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, VT tunnels and Ethergroup sources and destinations are unavailable.
- Diagnostic—Leave unchecked.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - **IS**—Puts the circuit cross-connects in the IS-NR service state.
  - **OOS,DSBLD**—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - **IS,AINS**—Puts the circuit cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - **OOS,MT**—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily.
  - OOS,OOG—(VCAT circuits only) Puts the member in the Out-of-Service and Management, Out-of-Group (OOS-MA,OOG) service state. This administrative state is used to place a member circuit out of the group and to stop sending traffic. OOS-MA,OOG only applies to the cross-connects on an end node where VCAT resides. The cross-connects on intermediate nodes are in the OOS-MA,MT service state. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A230 Change a Circuit Service State" task on page 19-19.

  For additional information about circuit service states, refer to the "Administrative and Service States" appendix in the *Cisco ONS 15454 Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state to the source and destination ports.

Note If ports managed into the IS administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to OOS-AU,FLT.

Step 9 Click **Next**.

Step 10 To configure the dual source, single destination circuit, complete the "DLP-A594 Provision a Dual Source, Single Destination Circuit" task on page 22-102.

Step 11 In the Circuit Routing Preferences area, uncheck **Route Automatically**.

Note When Route Automatically is not selected, the Using Required Nodes/Spans and Review Route Before Circuit Creation check boxes are unavailable.

Step 12 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 15.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection configuration, choose one of the following:

- **Nodal Diversity Required**—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
- **Nodal Diversity Desired**—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- **Link Diversity Only**—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a BLSR DRI or path protection DRI, click the **Dual Ring Interconnect** check box.

Step 15 Click **Next**. In the Route Review/Edit area, node icons appear for you to route the circuit manually.

Step 16 Click **Finish**.

Step 17 When all the circuits are created, the main Circuits window appears. Verify that the circuits you created appear in the window.

Stop. You have completed this procedure.

NTP-A371 Manually Create a CCAT or VCAT Circuit on the CE-MR-10 Card

Purpose	This procedure manually creates a CCAT or VCAT circuit on the CE-MR-10 Card.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 In the node view, double-click the CE-MR-10 card.

Step 3 Complete the "DLP-A595 Provision Card Mode for CE-MR-10 Card" procedure on page 22-103 to change the card mode to Manual.

Step 4 Click the **Circuits** > **Circuits** tabs and click **Create**.

Step 5 In the Circuit Creation dialog box, choose **STS-V** or **VT-V** from the Circuit Type drop-down list.

Step 6 Click **Next**.

Step 7 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 43 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Displays the circuit type that you chose in Step 5. You cannot change it.
- Bidirectional—Checked is the default. You cannot change it.
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits.
- State—Choose **IS**.
- Apply to drop ports—Check this check box to apply the IS administrative state to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box shows the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not change the service state of the source and destination ports.
- Symmetric—Checked is the default. You cannot change it.
- Open VCAT—Check this check box if you are creating open-ended CCAT/VCAT circuits. For more information on open-ended CCAT/VCAT refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Member size—Choose the member size. For information about the member size supported for each card, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
- Num. of members—Choose the number of members. For information about the number of members supported for each card, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*. You can add additional members using the **Edit** circuit function.
- Mode—Choose the protection mode for the CCAT/VCAT circuit. For information about the mode supported for each card, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
  - None—Provides no protection. A failure on one member causes the entire CCAT/ VCAT circuit to fail. For CE-MR-10 cards, you can add or delete members after creating a VCAT circuit with no protection. During the time it takes to add or delete members (from seconds to minutes), the entire VCAT circuit will be unable to carry traffic. For all other cards, you cannot add or delete members if the protection mode is None.
  - SW-LCAS—Allows the VCAT circuit to adapt to member failures and keep traffic flowing after failures at a reduced bandwidth. Sw-LCAS uses legacy SONET failure indicators like AIS-P and RDI-P to detect member failure.
  - LCAS—Sets the VCAT circuit to use LCAS. With LCAS, you can add or delete members without interrupting the operation of uninvolved members, and if a member fails, LCAS temporarily removes the failed member from the VCAT circuit. The remaining members carry the traffic until the failure clears.

Note For CE-MR-10 card, before you create a VCAT circuit with LCAS protection mode, it is recommended that you put all members of the VCAT circuit being created in OOS-OOG service state and later move them to IS state.

Step 8 Click **Next**.

Step 9 Complete the "DLP-A324 Provision a VCAT Circuit Source and Destination" task on page 20-14 for the VCAT circuit you are creating. If you are creating an open-ended VCAT circuit, complete the "DLP-A579 Provision an Open VCAT Circuit Source and Destination" task on page 22-92.

Step 10 In the VCAT Circuit Routing Preferences area, uncheck **Route Automatically**.

Step 11 If the VCAT circuit has a source or destination on a CE-MR-10 card, choose one of the following routing types.

- Common Fiber Routing—Routes the members on the same fiber.
- Split Routing—Allows the individual members to be routed on different fibers or each member to have different routing constraints. Split routing is required when creating circuits over a path protection configuration.

If the VCAT circuit does not have a source or destination on a CE-MR-10 card, common routing is automatically selected and you cannot change it.

Step 12 If you want to set preferences for individual members, complete the following in the Member Preferences area. Repeat for each member. To set identical preferences for all members, skip this step and continue with Step 13.

- Number—Choose a number (between 1 and 256) from the drop-down list to identify the member.
- Name—Type a unique name to identify the member. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the circuit.
- Protection—Choose the member protection type:
  - Fully Protected—Routes the circuit on a protected path.
  - Unprotected—Creates an unprotected circuit.
  - PCA—Routes the member on a BLSR protection channel.
  - DRI—(Split routing only) Routes the member on a dual-ring interconnect circuit.
- Node-Diverse Path—(Split routing only) Available for each member when Fully Protected is chosen.

Step 13 To set preferences for all members, complete the following in the Set Preferences for All Members area:

- Protection—Choose the member protection type:
  - Fully Protected—Routes the circuit on a protected path.
  - Unprotected—Creates an unprotected circuit.
  - PCA—Routes the member on a BLSR protection channel.
  - DRI—(Split routing only) Routes the member on a dual-ring interconnect circuit.
- Node-Diverse Path—(Split routing only) Available when Fully Protected is chosen.

Step 14 Click **Next**. If you chose Fully Protected or PCA, click **OK** to continue. If not, continue with the next step.

Step 15 In the Route Review and Edit area, node icons appear so you can route the circuit manually.

Step 16 Complete the "DLP-A325 Provision a VCAT Circuit Route" task on page 20-15.

Step 17 Click **Finish**. If the path does not meet the specified path diversity requirement, CTC displays an error message and allows you to change the circuit path.

Note Depending on the complexity of the network and number of members, the VCAT circuit creation process can take several minutes.

Step 18 When all the circuits are created, the main Circuits window appears. Verify that the circuit you created appear in the window.

Stop. You have completed this procedure.

CHAPTER 7

Manage Circuits

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter explains how to manage Cisco ONS 15454 electrical, optical (OC-N), Ethernet, and virtual concatenated (VCAT) circuits.

Before You Begin

To create circuits, see Chapter 6, "Create Circuits and VT Tunnels."

To clear any alarm or trouble conditions, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A329 Locate and View Circuits, page 7-2—Complete as needed.
2. NTP-A200 View Cross-Connect Card Resource Usage, page 7-3—Complete as needed.
3. NTP-A151 Modify and Delete Circuits, page 7-4—Complete as needed to edit a circuit name; change the active and standby colors of spans; change signal fail (SF) and signal degrade (SD) thresholds, reversion time, and path payload defect indication (PDI-P) settings for path protection circuits; or add or delete a VCAT member.
4. NTP-A278 Modify and Delete Overhead Circuits and Server Trails, page 7-5—Complete as needed to change a tunnel type, repair an IP circuit, or delete overhead circuits.
5. NTP-A78 Create a Monitor Circuit, page 7-5—Complete as needed to monitor traffic on primary bidirectional circuits.
6. NTP-A328 Create a J0 Section Trace, page 7-7—Complete as needed to monitor interruptions or changes to circuit traffic.
7. NTP-A79 Create a J1 Path Trace, page 7-8—Complete as needed to monitor interruptions or changes to circuit traffic.
8. NTP-A293 Create a J2 Path Trace, page 7-9—Complete as needed to monitor interruptions or changes to circuit traffic.
9. NTP-A334 Bridge and Roll Traffic, page 7-11—Complete as needed to bridge and roll traffic.

10. NTP-A298 Reconfigure Circuits, page 7-12—Complete as needed to reconfigure circuits.
11. NTP-A301 Merge Circuits, page 7-13—Complete as needed to merge circuits.
12. NTP-A325 Manage VLANs, page 7-13—Complete as needed to view, create, or delete VLANs.
13. NTP-A348 Display IEEE 802.17 RPR Circuits, page 7-14—Complete as needed to view a map or list of IEEE 802.17 RPR circuits between ML-Series cards.

NTP-A329 Locate and View Circuits

Purpose	This procedure allows you to locate and view circuits and spanning tree information. You can also export circuit data from the Circuits and Edit Circuits windows.
Tools/Equipment	None
Prerequisite Procedures	Circuit creation procedure(s) in Chapter 6, "Create Circuits and VT Tunnels"
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node on the network where you want to view the circuits. If you are already logged in, continue with Step 2.

Note Do not check Disable Circuit Management in the Login dialog box. No circuits appear if this option is checked.

Step 2 As needed, complete the "DLP-A416 View Circuit Information" task on page 21-2.

Step 3 As needed, complete the "DLP-A131 Search for Circuits" task on page 18-14.

Step 4 As needed, complete the "DLP-A262 Filter the Display of Circuits" task on page 19-43.

Step 5 As needed, complete the "DLP-A229 View Circuits on a Span" task on page 19-18.

Step 6 As needed, complete the "DLP-A454 View the BLSR STS Squelch Table" task on page 21-35.

Step 7 As needed, complete the "DLP-A455 View the BLSR VT Squelch Table" task on page 21-36.

Step 8 As needed, complete the "DLP-A430 View Spanning Tree Information" task on page 21-9.

Step 9 As needed, complete the "DLP-A532 Export CTC Data" section on page 22-34.

Stop. You have completed this procedure.

NTP-A200 View Cross-Connect Card Resource Usage

Purpose	This procedure allows you to view the percentage of cross-connect card resources used by circuits that traverse or terminate at an ONS 15454.
Tools/Equipment	XCVT, XC10G, or XC-VXC-10G cards must be installed.
Prerequisite Procedures	DLP-A37 Install the XCVT, XC10G, or XC-VXC-10G Cards, page 17-40
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to view the cross-connect card resource usage. If you are already logged in, continue with Step 2.

Step 2 Click the **Maintenance > Cross-Connect > Resource Usage** tabs.

Step 3 In the Summary area of the Resources Usage tab, view the following information:

- STS-1 Matrix—Provides the percent of cross-connect card STS-1 path resources that are in use. 288 STS-1 paths are available for XCVT cards; 1152 STS-1 paths are available for XC10G and XC-VXC-10G cards.
- VT Matrix Ports—Provides the percent of cross-connect card VT matrix ports that are in use. Each port is one STS in size, and each can transport 28 VT1.5s or 21 VT2s. 24 VT matrix ports are available for the XCVT and XC10G cards. 96 VT matrix ports are available for the XC-VXC-10G cards.
- VT Matrix—Provides the percent of VT matrix resources that are in use. 672 are available for the XCVT and XC10G cards. (672 is the number of VT matrix ports [24] multiplied by the number of VT1.5s in an STS [28].) The VT matrix on the XC-VXC-10G has capacity for 2688 VT1.5 terminations (1344 VT1.5 bidirectional circuits) or 2016 VT2 terminations (1008 VT2 bidirectional circuits).

Step 4 In the VT Matrix Port Detail section, you can view details of the VT Matrix Port usage:

- Drop—Identifies the source slot, port, and STS.
- Tunnel Name—Displays the tunnel name if the port is used by a VT tunnel. VT tunnels use VT matrix ports on the tunnel source and destination nodes. (VT tunnels do not use matrix resources on pass-through nodes.)
- % Used—Shows the percent of the matrix port that are in use. For example, each matrix port can carry 28 VT1.5s; if one STS carries seven VT1.5 circuits, the matrix port will be 25 percent used.
- Usage—Shows the port usage. For example, if one STS carries seven VT1.5 circuits, the matrix port will show that 7 of 28 VT1.5 circuits are in use.

Step 5 As needed, you can perform the following actions:

- Click the **Refresh** button to see an updated XC Resources view. For example, if other users create circuits while you view the XC Resources tab, click **Refresh** to see the effects those circuits have on the VT matrix usage.
- Click the **Delete** button to delete STSs that use VT matrix resources but no longer carry VT circuits. This occasionally occurs when many VT circuits are added and deleted over a period of time. Stranded STSs appear as STSs with 0 percent usage in the VT Matrix Port Detail area. If stranded STSs appear, click the STS, then click **Delete** to free VT matrix capacity.

Note The Delete button requires a Superuser security level.

Note VT tunnels might appear as STSs with 0 percent capacity used. These cannot be deleted.

Stop. You have completed this procedure.

NTP-A151 Modify and Delete Circuits

Purpose	This procedure modifies and deletes ONS 15454 circuits and tunnels.
Tools/Equipment	None
Prerequisite Procedures	Circuits must exist on the network. See Chapter 6, "Create Circuits and VT Tunnels" for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node containing the circuit that you want to modify. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-A230 Change a Circuit Service State" task on page 19-19.

Step 3 As needed, complete the "DLP-A231 Edit a Circuit Name" task on page 19-20.

Step 4 As needed, complete the "DLP-A232 Change Active and Standby Span Color" task on page 19-21.

Step 5 As needed, complete the "DLP-A233 Edit Path Protection Circuit Path Selectors" task on page 19-22.

Step 6 As needed, complete the "DLP-A263 Edit Path Protection Dual-Ring Interconnect Circuit Hold-Off Timer" task on page 19-45.

Step 7 As needed, complete the "DLP-A333 Delete Circuits" task on page 20-21.

Step 8 As needed, complete the "DLP-A437 Change a VCAT Member Service State" task on page 21-16.

Step 9 As needed, complete the "DLP-A384 Add a Member to a VCAT Circuit" task on page 20-79.

Step 10 As needed, complete the "DLP-A385 Delete a Member from a VCAT Circuit" task on page 20-83.

Stop. You have completed this procedure.

NTP-A278 Modify and Delete Overhead Circuits and Server Trails

Purpose	This procedure changes the tunnel type, repairs IP circuits, and deletes overhead circuits and server trails.
Tools/Equipment	None
Prerequisite Procedures	Circuits must exist on the network. See Chapter 6, "Create Circuits and VT Tunnels."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Deleting circuits can be service affecting and should be performed during a maintenance window.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 for a node on the network where you want to delete the circuit. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-A332 Change Tunnel Type" task on page 20-20.

Step 3 As needed, complete the "DLP-A336 Repair an IP Tunnel" task on page 20-24.

Step 4 As needed, complete the "DLP-A334 Delete Overhead Circuits" task on page 20-22.

Step 5 As needed, complete the "DLP-A453 Delete a Server Trail" task on page 21-34.

Stop. You have completed this procedure.

NTP-A78 Create a Monitor Circuit

Purpose	This procedure creates a monitor circuit that monitors traffic on primary, bidirectional circuits.
Tools/Equipment	None
Prerequisite Procedures	Bidirectional (two-way) circuits must exist on the network. See Chapter 6, "Create Circuits and VT Tunnels" for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Monitor circuits cannot be used with EtherSwitch circuits.

Note For unidirectional circuits, create a drop to the port where the test equipment is attached.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node on the network where you will create the monitor circuit. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuits** tab.

Step 4 Choose the bidirectional (two-way) circuit that you want to monitor and click **Edit**.

Step 5 Verify that the circuit name is no longer than 44 characters. Monitor circuits append a "_MON" to the circuit name. If the name is longer than 44 characters, edit the name in the Name field, then click **Apply**.

Step 6 In the Edit Circuit window, click the **Monitors** tab.

The Monitors tab displays ports that you can use to monitor the circuit.

Note The Monitors tab is only available when the circuit has a DISCOVERED status.

Step 7 On the Monitors tab, choose the monitor source port. The monitor circuit will display traffic coming into the node at the port you choose.

Note In Figure 7-1, you would choose either the DS1-14 card (to test circuit traffic entering Node 2 on the DS1-14) or the OC-N card at Node 1 (to test circuit traffic entering Node 1 on the OC-N card).

Step 8 Click **Create Monitor Circuit**.

Step 9 In the Circuit Destination section of the Circuit Creation wizard, choose the destination node, slot, and port, and as applicable, STS, VT, and/or DS1 for the monitored circuit.

Note In the Figure 7-1 example, the monitor circuit destination is Port 2 on the EC1-12 card.

Step 10 Click **Next**.

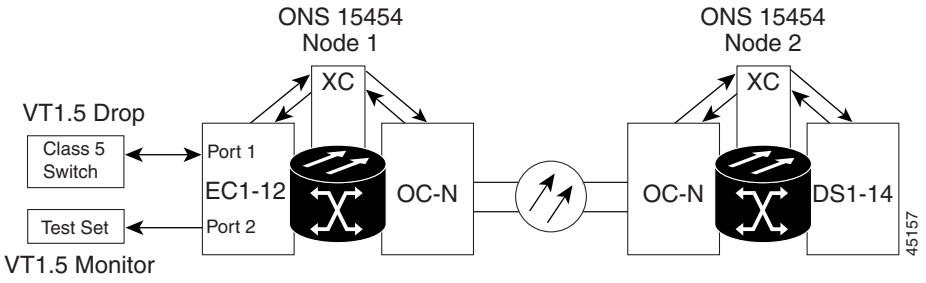
Step 11 In the Circuit Routing Preferences area, review the monitor circuit information. If you want the monitor circuit routed on a bidirectional line switched ring (BLSR) protection channel, click **Protection Channel Access**.

Step 12 Click **Finish**.

Step 13 In the Edit Circuit window, click **Close**. The new monitor circuit appears on the Circuits tab.

Figure 7-1 shows a sample monitor circuit setup. VT1.5 traffic is received by Port 1 of the EC1-12 card at Node 1. To monitor the VT1.5 traffic, test equipment is plugged into Port 2 of the EC1-12 card and a monitor circuit to Port 2 is provisioned in CTC. (Circuit monitors are one-way.) This example assumes that circuits have been created.

Figure 7-1 VT1.5 Monitor Circuit Received at an EC1-12 Port



Stop. You have completed this procedure.

NTP-A328 Create a J0 Section Trace

Purpose	This procedure creates a repeated, fixed-length string of characters used to monitor interruptions or changes to traffic between nodes.
Tools/Equipment	At least one of the following cards must be installed: MRC-2.5G-4, MRC-12 or OC192-XFP.
Prerequisite Procedures	None
Required/As Needed	As needed (optional if path trace is set)
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node on the network where you will create the section trace. If you are already logged in, continue with Step 2.

Step 2 In node view, double-click the MRC-2.5G-4, MRC-12 or OC192-XFP card.

Step 3 Click the **Provisioning > Line > Section Trace** tabs.

Step 4 From the Port drop-down list, choose the port for the section trace.

Step 5 From the Trace Mode drop-down list, enable the section trace expected string by choosing **Auto** or **Manual**:

- Auto—The first string received from the source port is automatically provisioned as the current expected string. An alarm is raised when a string that differs from the baseline is received.
- Manual—The string entered in the Current Expected String field is the baseline. An alarm is raised when a string that differs from the Current Expected String is received.

Step 6 In the Section Trace String Size area, click **1 byte**, **16 byte,** or **64 byte**. In the New Transmit String field, enter the string that you want to transmit. Enter a string that makes the destination port easy to identify, such as the node IP address, node name, or another string. If the New Transmit String field is left blank, the J0 transmits a string of null characters.

Step 7 If you set the Section Trace Mode field to Manual, enter the string that the destination port should receive from the source port in the New Expected String field. If you set Section Trace Mode to Auto, skip this step.

Step 8 Click the **Disable AIS and RDI if TIM-P is detected** check box if you want to suppress the alarm indication signal (AIS) and remote defect indication (RDI) when the STS Section Trace Identifier Mismatch Path (TIM-P) alarm appears. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for descriptions of alarms and conditions.

Step 9 Click **Apply**.

Step 10 After you set up the section trace, the received string appears in the Received field. The following options are available:

- Click **Hex Mode** to display section trace in hexadecimal format. The button name changes to ASCII Mode. Click it to return the section trace to ASCII format.
- Click the **Reset** button to reread values from the port.
- Click **Default** to return to the section trace default settings (Section Trace Mode is set to Off and the New Transmit and New Expected Strings are null).

Caution Clicking Default will generate alarms if the port on the other end is provisioned with a different string.

The expect and receive strings are updated every few seconds if the Section Trace Mode field is set to Auto or Manual.

Stop. You have completed this procedure.

NTP-A79 Create a J1 Path Trace

Purpose	This procedure creates a repeated, fixed-length string of characters used to monitor interruptions or changes to circuit traffic.
Tools/Equipment	ONS 15454 cards capable of transmitting and/or receiving path trace must be installed. See Table 19-3 on page 19-46 for a list of cards.
Prerequisite Procedures	Path trace can only be provisioned on OC-N (STS) circuits. See Chapter 6, "Create Circuits and VT Tunnels" for OC-N circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You cannot create a J1 path trace on a TL1-like circuit.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node on the network where you will create the path trace. If you are already logged in, continue with Step 2.

Step 2 Complete the following tasks as needed:

- As needed, complete the "DLP-A264 Provision a J1 Path Trace on Circuit Source and Destination Ports" task on page 19-45.
- As needed, complete the "DLP-A137 Provision Path Trace on OC-N Ports" task on page 18-15.

Stop. You have completed this procedure.

NTP-A293 Create a J2 Path Trace

Purpose	This procedure creates a repeated, fixed-length string of characters used to monitor interruptions or changes to circuit traffic.
Tools/Equipment	DS3XM-12 card or DS1/E1-56 card
Prerequisite Procedures	See Chapter 6, "Create Circuits and VT Tunnels" for DS-3 circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You cannot create a J2 path trace on a TL1-like circuit.

Note This procedure assumes that you are setting up path trace on a bidirectional circuit and setting up transmit strings at the circuit source and destination.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node on the network where you will create the path trace. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuits** tab.

Step 4 For the VT circuit you want to monitor, verify that the source and destination ports are on a card that can transmit and receive the path trace string.

Note If neither port is on a transmit/receive card, you will not be able to complete this procedure. If one port is on a transmit/receive card and the other is on a receive-only card, you can set up the transmit string at the transmit/receive port and the receive string at the receive-only port, but you will not be able to transmit in both directions.

Step 5 Choose the VT circuit you want to trace, then click **Edit**.

Step 6 In the Edit Circuit window, click the **Show Detailed Map** check box at the bottom of the window. A detailed map of the source and destination ports appears.

Step 7 Provision the circuit source transmit string:

a. On the detailed circuit map, right-click the circuit source port (the square on the left or right of the source node icon) and choose **Edit J2 Path Trace (port)** from the shortcut menu.

b. In the New Transmit String field, enter the circuit source transmit string. Enter a string that makes the source port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J2 transmits a string of null characters.

c. Click **Apply**, then click **Close**.

Step 8 Provision the circuit destination transmit string:

a. On the detailed circuit map, right-click the circuit destination port and choose **Edit Path Trace** from the shortcut menu.

b. In the New Transmit String field, enter the string that you want the circuit destination to transmit. Enter a string that makes the destination port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J2 transmits a string of null characters.

c. Click **Apply**.

Step 9 Provision the circuit destination expected string:

a. In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down list:

- Auto—The first string received from the source port is automatically provisioned as the current expected string. An alarm is raised when a string that differs from the baseline is received.
- Manual—The string entered in the Current Expected String field is the baseline. An alarm is raised when a string that differs from the Current Expected String is received.

b. If you set the Path Trace Mode field to Manual, enter the string that the circuit destination should receive from the circuit source in the New Expected String field. If you set Path Trace Mode to Auto, skip this step.

c. (Check box visibility depends on card selection) Click the **Disable AIS on C2 Mis-Match** check box if you want to suppress the AIS when a C2 mismatch occurs.

d. Click **Apply**, then click **Close**.

Note It is not necessary to set the format (16 or 64 bytes) for the circuit destination expected string; the path trace process automatically determines the format.

Step 10 Provision the circuit source expected string:

a. In the Edit Circuit window (with Show Detailed Map chosen), right-click the circuit source port and choose **Edit Path Trace** from the shortcut menu.

b. In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down list:

- Auto—Uses the first string received from the port at the other path trace end as the baseline string. An alarm is raised when a string that differs from the baseline is received.
- Manual—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.

c. If you set the Path Trace Mode field to Manual, enter the string that the circuit source should receive from the circuit destination in the New Expected String field. If you set Path Trace Mode to Auto, skip this step.

d. (Check box visibility depends on card selection) Click the **Disable AIS on C2 Mis-Match** check box if you want to suppress the AIS when a C2 mismatch occurs.

e. Click **Apply**.

Note It is not necessary to set the format (16 or 64 bytes) for the circuit source expected string; the path trace process automatically determines the format.

Step 11 After you set up the path trace, the received string appears in the Received field on the path trace setup window. The following options are available:

- Click **Hex Mode** to display path trace in hexadecimal format. The button name changes to ASCII Mode. Click it to return the path trace to ASCII format.
- Click the **Reset** button to reread values from the port.
- Click **Default** to return to the path trace default settings (Path Trace Mode is set to Off and the New Transmit and New Expected Strings are null).

Caution Clicking Default will generate alarms if the port on the other end is provisioned with a different string.

The expect and receive strings are updated every few seconds if the Path Trace Mode field is set to Auto or Manual.

Step 12 Click **Close**.

The detailed circuit map indicates path trace with an M (manual path trace) or an A (automatic path trace) at the circuit source and destination ports.

Stop. You have completed this procedure.

NTP-A334 Bridge and Roll Traffic

Purpose	This procedure reroutes live traffic without interrupting service. You can use the Bridge and Roll wizard for maintenance functions such as card replacement or load balancing. A circuit consists of a source facility, destination facility(s), and intermediate facilities (path).
Tools/Equipment	None
Prerequisite Procedures	• Circuits must exist on the network. See Chapter 6, "Create Circuits and VT Tunnels" for circuit creation procedures. • To route circuits on protected ports, you must create a protection group using the "DLP-A73 Create a 1+1 Protection Group" task on page 17-76 or the "NTP-A126 Create a BLSR" procedure on page 5-12. • When a roll involves two circuits, a data communications channel (DCC) connection must exist. See the "DLP-A377 Provision Section DCC Terminations" task on page 20-69. • Use the "NTP-A329 Locate and View Circuits" procedure on page 7-2 to verify that the planned Roll To paths are in service. Verify that the planned Roll To and Roll From paths are not in the Roll Pending status, used in test access, or used in a loopback. Refer to the *Cisco ONS 15454 Troubleshooting Guide* to clear any alarms.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

Note Using the bridge and roll feature, you can upgrade an unprotected circuit to a fully protected circuit or downgrade a fully protected circuit to an unprotected circuit.

Caution Performing bridge and roll on an STS192C might cause a traffic hit up to and including 50 ms.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the ONS 15454 circuit source node. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-A463 Roll the Source or Destination of One Optical Circuit" task on page 21-45.

Step 3 As needed, complete the "DLP-A464 Roll One Cross-Connect from an Optical Circuit to a Second Optical Circuit" task on page 21-48.

Step 4 As needed, complete the "DLP-A465 Roll Two Cross-Connects on One Optical Circuit Using Automatic Routing" task on page 21-50 or the "DLP-A466 Roll Two Cross-Connects on One Optical Circuit Using Manual Routing" task on page 21-53.

Step 5 As needed, complete the "DLP-A467 Roll Two Cross-Connects from One Optical Circuit to a Second Optical Circuit" task on page 21-56.

Step 6 As needed, complete the "DLP-A489 Cancel a Roll" task on page 21-61.

Step 7 As needed, complete the "DLP-A468 Delete a Roll" task on page 21-58. Use caution when selecting this option. Delete a roll only if it cannot be completed or canceled. Circuits might have a PARTIAL status when this option is selected.

Stop. You have completed this procedure.

NTP-A298 Reconfigure Circuits

Purpose	This procedure rebuilds circuits, which might be necessary when a large number of circuits are in the PARTIAL status.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Click the **Circuits** tab.

Step 3 Highlight the circuits that you want to reconfigure.

Step 4 From the Tools menu, choose **Circuits > Reconfigure Circuits**.

Step 5 In the confirmation dialog box, click **Yes** to continue.

Step 6 In the notification box, view the reconfiguration result. Click **Ok**.

Stop. You have completed this procedure.

NTP-A301 Merge Circuits

Purpose	This procedure merges two circuits that create a single, contiguous path but are separate circuits because of different circuit IDs or conflicting parameters. A merge combines a single master circuit with one or more circuits.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Click the **Circuits** tab.

Step 3 Click the circuit that you want to use as the master circuit for a merge.

Step 4 Click **Edit.**

Step 5 In the Edit Circuits window, click the **Merge** tab.

Step 6 Choose the circuits that you want to merge with the master circuit.

Step 7 Click **Merge**.

Step 8 In the confirmation dialog box, click **Yes** to continue.

Step 9 In the notification box, view the merge result. Click **Ok**.

Stop. You have completed this procedure.

NTP-A325 Manage VLANs

Purpose	This procedure allows you to view, create, or delete VLANs.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Remove all unused VLANs. The recommended number of VLANs is a maximum of 100; if more than 100 VLANs exist, the E-Series cards may have problems accepting new VLANs.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 From the Tools menu, choose **Manage VLANs**. The All VLANS dialog box appears listing all of the VLAN topologies in the network.

Step 3 Complete the following as necessary:

- To add a VLAN, complete the "DLP-A452 Create a VLAN" task on page 21-33.
- To delete a VLAN, complete the "DLP-A335 Delete VLANs" task on page 20-23.

Stop. You have completed this procedure.

NTP-A348 Display IEEE 802.17 RPR Circuits

Purpose	This procedure displays a map of and provides information about IEEE 802.17 Resilient Packet Ring (RPR) circuits between ML-Series cards. For more information about IEEE 802.17 RPR, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide.*
Tools/Equipment	None
Prerequisite Procedures	DLP-A556 Provision the Card Mode for ML-Series Ethernet Cards, page 22-70
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note CTC does not support the display of Cisco proprietary RPR circuit topology.

Note CTC does not support provisioning or maintenance of IEEE RPR rings. You must use Cisco IOS.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will view the circuit. If you are already logged in, continue with Step 2.

Step 2 From network, shelf, or ML-Series card view, click the **Circuits** tab and select the circuit where you want to display information.

Note If you are viewing the circuits list from network or shelf view, you must look at the Source and Destination fields to determine which circuits are RPR circuits.

Step 3 Click **Tools > Circuits > Show RPR Circuit Ring**.

The map displays the following information about each IEEE 802.17 RPR circuit:

- Circuit name
- Type
- Size
- OCHNC Wlen
- Direction
- Protection
- Status
- Source
- Destination
- # of VLANs
- # of Spans
- State
- Loopback

Step 4 Repeat this procedure as necessary for additional 802.17 RPR circuits you want to display.

Stop. You have completed this procedure.

CHAPTER 8

Manage Alarms

This chapter contains the procedures for viewing and managing the alarms and conditions on a Cisco ONS 15454.

Cisco Transport Controller (CTC) detects and reports alarms generated by the Cisco ONS 15454 and the Optical Networking System (ONS) network. You can use CTC to monitor and manage alarms at a card, node, or network level. You can also view alarm counts on the LCD front panel.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A195 Document Card, Node, and Network Provisioning, page 8-2—Complete this procedure as needed to print or export node data.
2. NTP-A196 View Alarms, History, Events, and Conditions, page 8-2—Complete this procedure as needed to see alarms and conditions occurring on the node and a complete history of alarm and condition messages.
3. NTP-A68 Delete Cleared Alarms from Display, page 8-3—Complete this procedure as needed to delete cleared alarm information.
4. NTP-A69 View Alarm-Affected Circuits, page 8-4—Complete this procedure as needed to find circuits that are affected by a particular alarm or condition.
5. NTP-A70 View Alarm Counts on the LCD for a Node, Slot, or Port, page 8-5—Complete this procedure as needed to see a statistical count of alarms that have occurred for a slot or port.
6. NTP-A71 Create, Download, and Assign Alarm Severity Profiles, page 8-6—Complete this procedure as needed to change the default severity for certain alarms, to assign the new severities to a port, card, or node, and to delete alarm profiles.
7. NTP-A168 Enable, Modify, or Disable Alarm Severity Filtering, page 8-7—Complete this procedure as needed to enable, disable, or modify alarm severity filtering in the Conditions, Alarms, or History screens at the node or network level.
8. NTP-A72 Suppress Alarms or Discontinue Alarm Suppression, page 8-7—Complete this procedure as needed to suppress reported alarms at the port, card, or node level and to disable the suppress command to resume normal alarm reporting.
9. NTP-A258 Provision External Alarms and Controls on the Alarm Interface Controller–International, page 8-8—Complete this procedure as needed to provision external alarms and controls on the Alarm Interface Controller-International (AIC-I) card.

NTP-A195 Document Card, Node, and Network Provisioning

Purpose	Use this procedure to print card, node, or network CTC information in graphical or tabular form on a Windows-provisioned printer. This procedure is useful for network record keeping and troubleshooting.
Tools/Equipment	A printer connected to the CTC computer by a direct or network connection
Prerequisite Procedures	Chapter 4, "Turn Up a Node"
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to record or save data. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-A531 Print CTC Data" task on page 22-32.

Step 3 As needed, complete the "DLP-A532 Export CTC Data" task on page 22-34.

Stop. You have completed this procedure.

NTP-A196 View Alarms, History, Events, and Conditions

Purpose	Use this procedure to view current or historical alarms and conditions for a card, node, or network. This information is useful for monitoring and troubleshooting hardware and software events.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node that contains the alarms you want to view. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A390 View Alarms" task on page 20-97 as needed.

Step 3 Complete the "DLP-A517 View Alarm or Event History" task on page 22-10 as needed.

Step 4 Complete the "DLP-A111 Changing the Maximum Number of Session Entries for Alarm History" task on page 18-1 as needed.

Step 5 Complete the "DLP-A112 Display Alarms and Conditions Using Time Zone" task on page 18-2 as needed.

Step 6 Complete the "DLP-A113 Synchronize Alarms" task on page 18-3 as needed.

Step 7 Complete the "DLP-A114 View Conditions" task on page 18-3 as needed.

Stop. You have completed this procedure.

NTP-A68 Delete Cleared Alarms from Display

Purpose	Use this procedure to delete Cleared (C) status alarms from the alarms window or transient messages from the CTC History window.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 To delete cleared node-level alarms:

a. In the node view, click the **Alarms** tab.

b. Click **Delete Cleared Alarms**, referring to the following rules:

- If the Autodelete Cleared Alarms check box is checked, an alarm disappears from the window when it is cleared.
- If the Autodelete Cleared Alarms check box is not checked, an alarm remains in the window when it is cleared. The alarm appears white in the window and has a Clear (C) severity. The alarm can be removed by clicking the **Delete Cleared Alarms** button.

This action removes any cleared ONS 15454 alarms from the Alarms tab. The rows of cleared alarms turn white and have a C in their status (ST) column.

Step 3 To delete cleared card-level alarms:

a. In the node view, double-click the card graphic for the card you want to open.

b. Click the **Alarms** tab and then click **Delete Cleared Alarms**, referring to the note in Step 2.

Step 4 To delete cleared network-level alarms:

a. In the node view click **View > Go to Network View**.

b. Click the **Alarms** tab and then click **Delete Cleared Alarms**, referring to the rules in Step 2.

Step 5 To remove the transient messages from the History window, click **Delete Cleared Alarms**. Transient messages are single messages, not raise-and-clear pairs (that is, they do not have companion messages stating they are cleared).

Stop. You have completed this procedure.

NTP-A69 View Alarm-Affected Circuits

Purpose	Use this procedure to view all circuits, if any, that are affected by an alarm or condition.
Tools/Equipment	None
Prerequisite Procedures	NTP-A196 View Alarms, History, Events, and Conditions, page 8-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

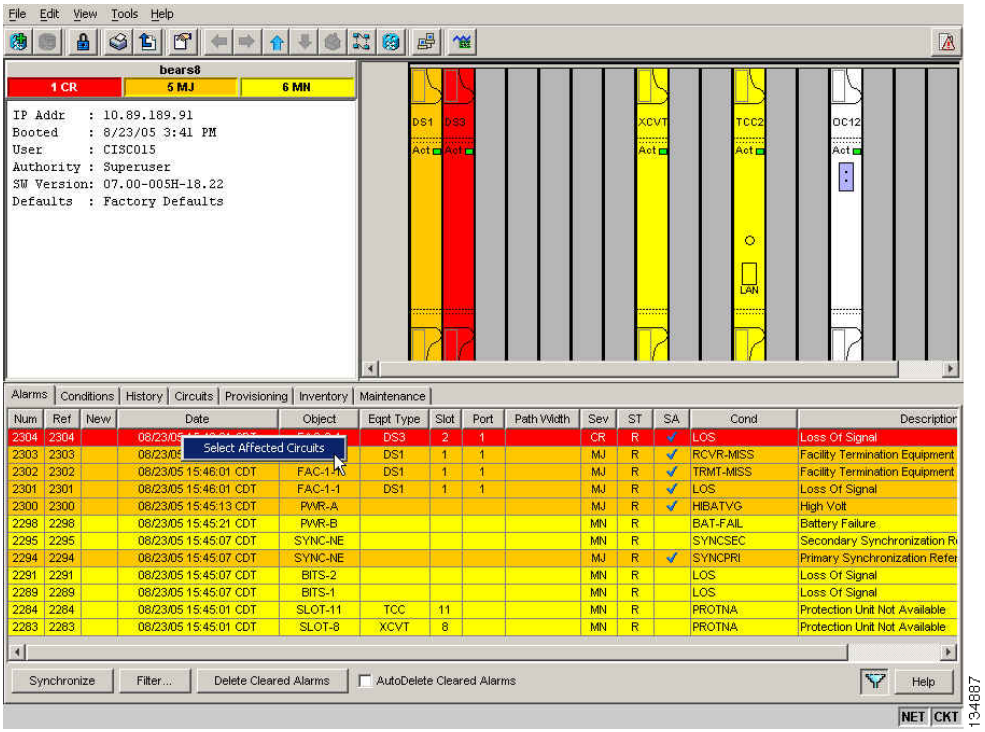
Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 In the network, node, or card view, click the **Alarms** tab or **Conditions** tab and then right-click anywhere in the row of an active alarm or condition.

Note The node view is the default, but you can also navigate to the Alarms tab in the network view or card view to perform Step 2.

The Select Affected Circuit option appears on the shortcut menu (Figure 8-1).

Figure 8-1 Select Affected Circuits Option



Step 3 Left-click or right-click **Select Affected Circuits**.

The **Circuits** window appears with the affected circuits highlighted.

Step 4 If you want to search for particular circuits, see the "DLP-A131 Search for Circuits" task on page 18-14.

Stop. You have completed this procedure.

NTP-A70 View Alarm Counts on the LCD for a Node, Slot, or Port

Purpose	Use this procedure to view an alarm summary for a node, slot, or port without using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 If you want to view the entire alarm summary for the node, press either the **Slot** button or **Port** button on the LCD panel until "Node" appears on the LCD. You will also see the direction, "Status=Alm Ct." This means that if you press the Status button at this time, as directed in Step 2, you will see an alarm count for the node.

Step 2 Press the **Status** button to see a summary of alarms and severities for the node. You will see a message similar to "Alm CT: 2: MJ:2 MN:2," meaning that there are two Critical alarms, two Major alarms, and two Minor alarms.

Step 3 If you want to see alarm counts for a particular slot, such as the alarms for an OC-3 card in Slot 2, press the **Slot** button until you see "Slot-3" on the LCD. You will see the direction, "Status=Alm Ct."

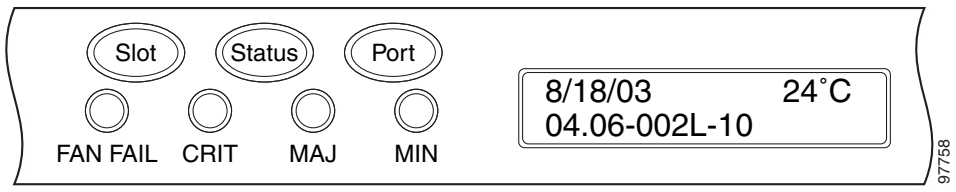
Step 4 Press the **Status** button to see a summary of alarms and severities against the slot. For example, you might see "Slot-3 Alm CT:0 MJ:1 MN:2." This means that there are no Critical alarms, one Major alarm, and two Minor alarms against the slot.

Step 5 If you want to view the alarms against a port on the card, such as Port 3 of the OC-3 card you viewed previously, press the **Port** button until you see "Port-3 Status=Alm Ct."

Step 6 Press **Status** to view alarm count against the port. You will see a message similar to "Port-3 Alm CT:0 MJ:1 MN:0." This means that there is one Major alarm against this port.

Figure 8-2 shows the shelf LCD panel.

Figure 8-2 Shelf LCD Panel



To return to the previous view from the Port screen, continue to press **Port** until the display cycles through all the ports on the slot. For instance, on the OC-3 card, press Port until it cycles past Slot 4 and you see "Slot."

To return to the node menu from the Slot screen, press **Slot** until you cycle through all the slots and see "Node."

If you do not press any buttons, the LCD will return to its default display with the node name. However, if you did not cycle through the options to return to the node status, you will see the slot or port where you last checked status.

Note A blank LCD results when the fuse on the alarm interface panel (AIP) board has blown. If this occurs, contact your next level of support. For information, see the "Obtaining Documentation and Submitting a Service Request" section on page lxiv.

Stop. You have completed this procedure.

NTP-A71 Create, Download, and Assign Alarm Severity Profiles

Purpose	Use this procedure to create a customized alarm profile at the network, node, or card level. This procedure also provides links to tasks that describe how to assign custom severities individually to each port, card, or node, and to delete alarm profiles.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to create an alarm profile. If you are already logged in, continue with Step 2 to create, clone or modify an alarm profile, or go to Step 3 to download an alarm profile.

Step 2 Complete the "DLP-A518 Create a New or Cloned Alarm Severity Profile" task on page 22-11. This task clones a current alarm profile, renames the profile, and customizes the new profile.

Step 3 Complete the "DLP-A524 Download an Alarm Severity Profile" task on page 22-22. This task downloads an alarm severity profile from a CD or a node.

Note After storing a created or downloaded alarm profile, you must go to the node (either by logging into it or clicking on it from the network view) and activate the profile by applying it to the shelf, one or more cards, or one or more ports.

Step 4 As necessary, complete the "DLP-A519 Apply Alarm Profiles to Ports" task on page 22-15 or the "DLP-A117 Apply Alarm Profiles to Cards and Nodes" task on page 18-5.

Step 5 As necessary, complete the "DLP-A520 Delete Alarm Severity Profiles" task on page 22-17.

Stop. You have completed this procedure.

NTP-A168 Enable, Modify, or Disable Alarm Severity Filtering

Purpose	Use this procedure to start, change, or stop alarm filtering for one or more severities in the Alarms, Conditions, and History windows in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to enable alarm severity filtering. If you are already logged in, continue with Step 2.

Step 2 As necessary, complete the "DLP-A225 Enable Alarm Filtering" task on page 19-17. This task enables alarm filtering at the card, node, and network views for all nodes in the network. Alarm filtering can be enabled for alarms, conditions, or events.

Step 3 As necessary, complete the "DLP-A521 Modify Alarm, Condition, and History Filtering Parameters" task on page 22-18 to modify the alarm filtering for network nodes to show or hide particular alarms or conditions.

Step 4 As necessary, complete the "DLP-A227 Disable Alarm Filtering" task on page 19-18 to disable alarm profile filtering for all network nodes.

Stop. You have completed this procedure.

NTP-A72 Suppress Alarms or Discontinue Alarm Suppression

Purpose	Use this procedure to prevent alarms from being reported for a port, card, or node in circumstances when an alarm or condition is known to exist but you do not want to include it in the display. This procedure also provides a link to a task that explains how to resume normal alarm reporting by discontinuing the suppression.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A522 Suppress Alarm Reporting" task on page 22-20 to enable the node to send autonomous messages that clear specific raised alarms and cause suppressed alarms to appear in the Conditions window.

Note Suppressing one or more alarms prevents them from appearing in Alarm or History windows or in any other clients. The suppress command causes CTC to display them in the Conditions window with their severity, their severity color code, and service-affecting status.

Step 3 Complete the "DLP-A523 Discontinue Alarm Suppression" task on page 22-21 to discontinue alarm suppression and resume normal alarm reporting.

Stop. You have completed this procedure.

NTP-A258 Provision External Alarms and Controls on the Alarm Interface Controller–International

Purpose	Use this procedure to create external (environmental) alarms and external controls for the AIC-I card.
Tools/Equipment	An AIC-I card must be installed in Slot 9.
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The AIC-I card alarm provides direct alarm contacts (external alarm inputs and external control outputs) routed through the backplane to wire-wrap pins accessible from the back of the shelf. If you install an Alarm Expansion Panel (AEP), the AIC-I alarm contacts cannot be used. Only the AEP alarm contacts can be used. For further information about the AEP, see the "NTP-A119 Install the Alarm Expansion Panel" procedure on page 1-14 and the "NTP-A120 Install an External Wire-Wrap Panel to the AEP" procedure on page 1-18.

Note For information about the AIC-I alarms, controls, and virtual wires, refer to the *Cisco ONS 15454 Reference Manual*.

Step 1 Verify the backplane wiring using the following substeps. If you are using the AEP, see the "NTP-A119 Install the Alarm Expansion Panel" procedure on page 1-14. Otherwise, see the "NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections" procedure on page 1-17 for information about the ONS 15454 backplane pins.

a. For external alarms, verify that the external device relays are wired to the ENVIR ALARMS IN backplane pins.

b. For external controls, verify that the external device relays are wired to the ENVIR ALARMS OUT backplane pins.

Step 2 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 3 In the node view, double-click the AIC-I card on the shelf graphic. The card view appears.

Step 4 Click the **Provisioning > Card** tabs.

Step 5 In the Alarm Contacts area, click the Add Extension radio button if you are using the AEP. Clicking this option will choose the External Alarm input/output type and the AEP extension type; it will give you access to 16 external alarm contacts.

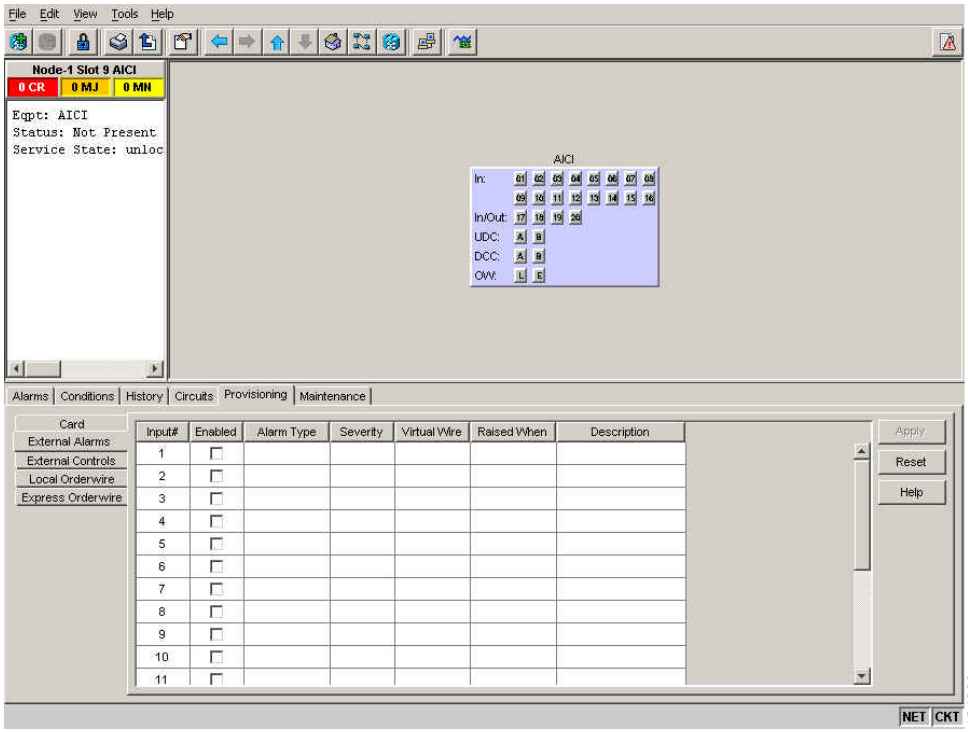
Step 6 If you did not click Add Extension, in the Input/Output area, choose either External Alarm or External Control. (External Alarm will limit your input/output options as explained in Step 5.) Choosing External Control will enable both external alarms and external controls. This will convert four of the external alarm contacts to external controls, leaving 12 available external control contacts. The extension type for both options is AEP.

Step 7 Click **Apply**.

Step 8 To add User Defined Alarm Types, complete the "DLP-A580 Create User Defined Alarm Types" task on page 22-93. If you are not adding User Defined Alarm Types continue with Step 9.

Step 9 If you are provisioning external alarms, click the **External Alarms** tab (Figure 8-3). If you are not provisioning external alarms, skip Steps 10 through 12 and go to Step 13.

Figure 8-3 Provisioning External Alarms on The AIC-I Card



Step 10 For external alarms, complete the following fields:

- Enabled—Check the check box to activate the fields for the alarm input number.
- Alarm Type—Choose an alarm type from the drop-down list.
- Severity—Choose a severity from the drop-down list.

  The severity determines the alarm's severity in the Alarms and History tabs and determines whether the LEDs are activated. Critical (CR), Major (MJ), and Minor (MN) alarms activate the LEDs. Not Alarmed (NA) and Not Reported (NR) do not activate LEDs, but do report the information in CTC.

- Virtual Wire—Choose the virtual wire number from the drop-down list to assign the external device to a virtual wire. Otherwise, do not change the None default. For information about the AIC-I virtual wire, see the "Alarm Monitoring and Management" in the *Cisco ONS 15454 Reference Manual*.
- Raised When—From the drop-down list, choose the contact condition (open or closed) that triggers the alarm.
- Description—A default description is provided; enter a different description if needed.

Step 11 To provision additional devices, complete Step 10 for each additional device.

Step 12 Click **Apply**.

Step 13 For external controls, click the **External Controls** tab and complete the following fields for each control wired to the ONS 15454 backplane:

- Enabled—Check this check box to activate the fields for the alarm input number.
- Control Type—Choose the control type from the drop-down list: air conditioner, engine, fan, generator, heat, light, sprinkler, or miscellaneous.
- Trigger Type—Choose a trigger type: a local Minor, Major, or Critical alarm; a remote Minor, Major, or Critical alarm; or a virtual wire activation.
- Description—Enter a description.

Step 14 To provision additional external controls, complete Step 13 for each device.

Step 15 Click **Apply**.

Note When you provision an external alarm, the alarm object is ENV-IN-*nn*. The variable *nn* refers to the external alarm's number, regardless of the name you assign.

Note Environmental alarms that you create (and name) should be recorded locally for the NE. Both the Alarm name and resolution are node-specific.

Stop. You have completed this procedure.

CHAPTER 9

Monitor Performance

This chapter explains how to enable and view performance monitoring statistics for the Cisco ONS 15454. Performance monitoring (PM) parameters are used by service providers to gather, store, and set thresholds and report performance data for early detection of problems. For more PM information, details, and definition, refer to the *Cisco ONS 15454 Reference Manual*.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A253 Change the PM Display, page 9-2—Complete as needed to change the displayed PM counts.
2. NTP-A122 Monitor Electrical Performance, page 9-3—Complete as needed to monitor electrical performance.
3. NTP-A198 Monitor Ethernet Performance, page 9-5—Complete as needed to monitor Ethernet performance.
4. NTP-A279 Create or Delete Ethernet RMON Thresholds, page 9-5—Complete as needed to create or delete Ethernet remote monitoring (RMON) thresholds.
5. NTP-A250 Monitor OC-N Performance, page 9-6—Complete as needed to monitor optical (OC-N) performance.
6. NTP-A347 Monitor Multirate Performance, page 9-7—Complete as needed to monitor multirate (MRC-N) performance.
7. NTP-A285 Monitor FC_MR-4 Performance, page 9-7—Complete as needed to monitor FC_MR-4 performance.
8. NTP-A289 Create or Delete FC_MR-4 RMON Thresholds, page 9-8—Complete as needed to create or delete FC_MR-4 RMON thresholds.
9. NTP-A357 Enable or Disable AutoPM, page 9-8—Complete as needed to enable or disable automatic autonomous performance monitoring (AutoPM) reports.

Note For additional information regarding PM parameters, refer to the Digital transmission surveillance section in Telcordia's GR-1230-CORE, GR-820-CORE, GR-499-CORE, and GR-253-CORE documents, and in the ANSI document entitled *Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*.

NTP-A253 Change the PM Display

Purpose	This procedure enables you to change the display of PM counts by selecting drop-down list or radio button options in the Performance window.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits and VT Tunnels" and Chapter 11, "Change Node Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node that you want to monitor. If you are already logged in, continue with Step 2.

Step 2 In node view, double-click the electrical, Ethernet, optical (OC-N), or multirate transport cards where you want to view PM counts. The card view appears.

Step 3 As needed, use the following tasks to change the display of PM counts:

- DLP-A124 Refresh PM Counts at 15-Minute Intervals, page 18-10
- DLP-A125 Refresh PM Counts at One-Day Intervals, page 18-11
- DLP-A347 Refresh E-Series and G-Series Ethernet PM Counts, page 20-33
- DLP-A126 View Near-End PM Counts, page 18-12
- DLP-A127 View Far-End PM Counts, page 18-12
- DLP-A348 Monitor PM Counts for a Selected Signal, page 20-34
- DLP-A129 Reset Current PM Counts, page 18-13
- DLP-A349 Clear Selected PM Counts, page 20-35
- DLP-A458 Clear All PM Thresholds, page 21-40
- DLP-A260 Set Auto-Refresh Interval for Displayed PM Counts, page 19-42
- DLP-A259 Refresh Ethernet PM Counts at a Different Time Interval, page 19-41
- DLP-A261 Refresh PM Counts for a Different Port, page 19-42

Stop. You have completed this procedure.

NTP-A122 Monitor Electrical Performance

Purpose	This procedure enables you to view node near-end or far-end performance during selected time intervals on an electrical card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits and VT Tunnels" and Chapter 11, "Change Node Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node that you want to monitor. If you are already logged in, continue with Step 3.

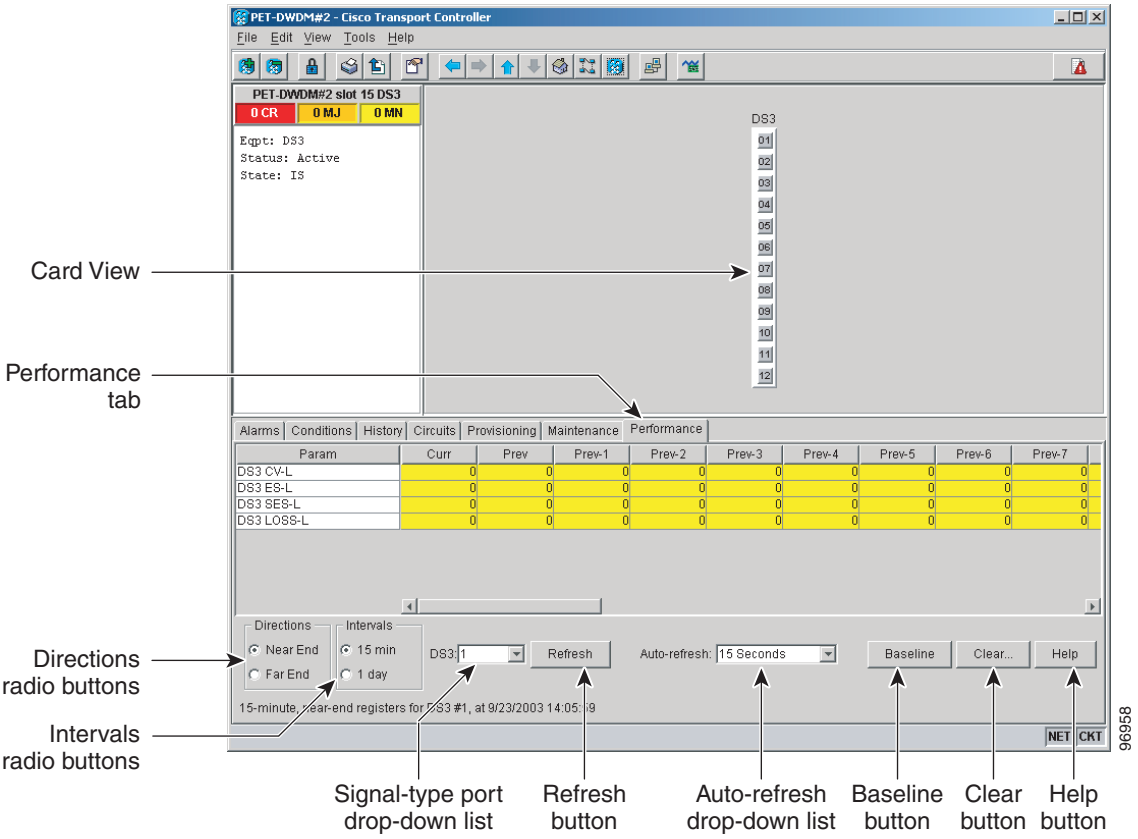
Step 2 Complete the following procedures depending on card type:

- For DS3XM-12 cards, complete the following procedures:
  - DLP-A394 View DS-N/SONET PM Parameters for the DS3XM-12 Card, page 20-103
  - DLP-A395 View BFDL PM Parameters for the DS3XM-12 Card, page 20-105
- For EC-1 cards, complete the "DLP-A122 Enable/Disable Intermediate Path Performance Monitoring" task on page 18-9 as needed to enable or disable monitoring of synchronous transport signal (STS) traffic through intermediate nodes.
- For all other electrical cards, continue with Step 3.

Step 3 In node view, double-click the electrical card where you want to view PM counts. The card view appears.

Step 4 Click the **Performance** tab (Figure 9-1).

Figure 9-1 Viewing Electrical Card Performance Monitoring Information



Step 5 In the signal-type drop-down lists, choose the applicable port on the card you selected.

Step 6 Click **Refresh**.

Step 7 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 9-2.

Stop. You have completed this procedure.

NTP-A198 Monitor Ethernet Performance

Purpose	This procedure enables you to view node transmit and receive performance during selected time intervals on an Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits and VT Tunnels" and Chapter 11, "Change Node Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node that you want to monitor. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A256 View Ethernet Statistics PM Parameters" task on page 19-39.

Step 3 Complete the "DLP-A257 View Ethernet Utilization PM Parameters" task on page 19-40.

Step 4 Complete the "DLP-A258 View Ethernet History PM Parameters" task on page 19-40.

Step 5 Complete the "DLP-A320 View ML-Series Ether Ports PM Parameters" task on page 20-10.

Step 6 Complete the "DLP-A321 View ML-Series POS Ports PM Parameters" task on page 20-11.

Step 7 Complete the "DLP-A562 View ML-Series RPR Span PM Parameters" task on page 22-76.

Step 8 Complete the "DLP-A391 View CE-Series Ether Ports and POS Ports Statistics PM Parameters" task on page 20-99.

Step 9 Complete the "DLP-A392 View CE-Series Ether Ports and POS Ports Utilization PM Parameters" task on page 20-100.

Step 10 Complete the "DLP-A393 View CE-Series Ether Ports and POS Ports History PM Parameters" task on page 20-102.

Stop. You have completed this procedure.

NTP-A279 Create or Delete Ethernet RMON Thresholds

Purpose	This procedure creates or deletes Ethernet RMON thresholds for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Perform any of the following tasks as needed:

- DLP-A533 Create Ethernet RMON Alarm Thresholds, page 22-36
- DLP-A529 Delete Ethernet RMON Alarm Thresholds, page 22-30

Stop. You have completed this procedure.

NTP-A250 Monitor OC-N Performance

Purpose	This procedure enables you to view node near-end or far-end performance during selected time intervals on an OC-N card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits and VT Tunnels" and Chapter 11, "Change Node Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node that you want to monitor. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A121 Enable/Disable Pointer Justification Count Performance Monitoring" task on page 18-7 as needed to enable or disable clock synchronization monitoring.

Step 3 Complete the "DLP-A122 Enable/Disable Intermediate Path Performance Monitoring" task on page 18-9 as needed to enable or disable monitoring of STS traffic through intermediate nodes.

Step 4 Complete the "DLP-A507 View OC-N PM Parameters" task on page 22-1.

To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 9-2.

Stop. You have completed this procedure.

NTP-A347 Monitor Multirate Performance

Purpose	This procedure enables you to view node near-end or far-end performance during selected time intervals on an MRC-N card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits and VT Tunnels" and Chapter 11, "Change Node Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node that you want to monitor. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A121 Enable/Disable Pointer Justification Count Performance Monitoring" task on page 18-7 as needed to enable or disable clock synchronization monitoring.

Step 3 Complete the "DLP-A122 Enable/Disable Intermediate Path Performance Monitoring" task on page 18-9 as needed to enable or disable monitoring of STS traffic through intermediate nodes.

Step 4 Complete the "DLP-A557 View Multirate PM Parameters" task on page 22-71.

To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 9-2.

Stop. You have completed this procedure.

NTP-A285 Monitor FC_MR-4 Performance

Purpose	This procedure enables you to view node transmit and receive performance during selected time intervals on an FC_MR-4 card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits and VT Tunnels" and Chapter 11, "Change Node Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node that you want to monitor. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A350 View FC_MR-4 Statistics PM Parameters" task on page 20-36.

Step 3 Complete the "DLP-A351 View FC_MR-4 Utilization PM Parameters" task on page 20-37.

Step 4 Complete the "DLP-A352 View FC_MR-4 History PM Parameters" task on page 20-38.

Stop. You have completed this procedure.

NTP-A289 Create or Delete FC_MR-4 RMON Thresholds

Purpose	Use this procedure to create or delete FC_MR-4 RMON thresholds for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Perform any of the following tasks as needed:

- DLP-A357 Create FC_MR-4 RMON Alarm Thresholds, page 20-41
- DLP-A358 Delete FC_MR-4 RMON Alarm Thresholds, page 20-45

Stop. You have completed this procedure.

NTP-A357 Enable or Disable AutoPM

Purpose	This procedure allows you to enable or disable automatic autonomous performance monitoring (AutoPM) reports.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Click the **Provisioning > Defaults** tabs.

Step 3 In the Defaults Selector area, click **NODE > General** and choose **NODE.general.AutoPM**.

Step 4 In the Default Value field, select **True** to enable AutoPM.

Step 5 Click **Apply**.

Step 6 Follow Steps 1 through 5 to disable AutoPM. Select **False** in the Default Value field in Step 4 before proceeding to Step 5.

Stop. You have completed this procedure.

CHAPTER 10

Change Card Settings

This chapter explains how to change line provisioning, thresholds, service states, and line rates on Cisco ONS 15454 cards.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A88 Modify Line Settings and PM Parameter Thresholds for Electrical Cards, page 10-2—As needed, complete this procedure to change line and threshold settings for all electrical cards (EC-1, DS-1, DS-3, DS3i-N-12, and DS3XM).
2. NTP-A89 Modify Line Settings and PM Parameter Thresholds for Optical Cards, page 10-3—As needed, complete this procedure to change line and threshold settings for all optical cards.
3. NTP-A118 Modify Alarm Interface Controller–International Settings, page 10-4—As needed, complete this procedure to change external alarms and controls and/or orderwire settings.
4. NTP-A91 Upgrade DS-1 and DS-3 Protect Cards from 1:1 Protection to 1:N Protection, page 10-4—As needed, complete this procedure to change the protection type on DS-1 or DS-3 cards.
5. NTP-A315 Modify Port Settings and PM Parameter Thresholds for FC_MR-4 Cards, page 10-5—As needed, complete this procedure to change FC_MR-4 card port and threshold settings.
6. NTP-A321 Change Card or PPM Service State, page 10-6—As needed, complete this procedure to change the service state on a card or pluggable port module (PPM).
7. NTP-A322 Manage Pluggable Port Modules, page 10-6—As needed, complete this procedure to provision a multirate PPM, assign the optical line rate, change the optical line rate, and delete PPMs.
8. NTP-A346 Provision the Soak Timer for an ML-Series Card, page 10-7—As needed, complete this procedure to provision the soak timer for an ML-Series card.
9. NTP-A352 View PPM Information on the LCD, page 10-8—As needed, complete this procedure to view wavelength and rate for a PPM on a multirate optical card.
10. NTP-A354 Set or Check Cross-Connect Mode for XC-VXC-10G Cards, page 10-8—As needed, complete this procedure to provision the node's cross-connect mode if mixed mode grooming is required.

NTP-A88 Modify Line Settings and PM Parameter Thresholds for Electrical Cards

Purpose	This procedure changes the line and threshold settings for electrical cards.
Tools/Equipment	None
Prerequisite Procedures	NTP-A17 Install the Electrical Cards, page 2-11
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Changing card settings can be service affecting. You should make all changes during a scheduled maintenance window.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to change the electrical card settings. If you are already logged in, proceed to Step 2.

Step 2 As needed, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Perform any of the following tasks as needed:

- DLP-A165 Change Line and Threshold Settings for a DS1-14 or DS1N-14 Card, page 18-29
- DLP-A166 Change Line and Threshold Settings for a DS3-12 or DS3N-12 Card, page 18-33
- DLP-A167 Change Line and Threshold Settings for a DS3E-12 or DS3N-12E Card, page 18-37
- DLP-A168 Change Line and Threshold Settings for the DS3XM-6 Card, page 18-42
- DLP-A387 Change Line and Threshold Settings for the DS3XM-12 Card, page 20-88
- DLP-A526 Change Line and Threshold Settings for the DS3i-N-12 Cards, page 22-23
- DLP-A388 Change Line and Threshold Settings for the DS3/EC1-48 Cards, page 20-93
- DLP-A169 Change Line and Threshold Settings for the EC1-12 Card, page 18-47
- DLP-A376 Change Line and Threshold Settings for the DS1/E1-56 Cards, page 20-61

Step 4 As needed, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Stop. You have completed this procedure.

NTP-A89 Modify Line Settings and PM Parameter Thresholds for Optical Cards

Purpose	This procedure changes the line and threshold settings for optical (OC-N) cards.
Tools/Equipment	None
Prerequisite Procedures	NTP-A16 Install Optical Cards and Connectors, page 2-8
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Changing card settings can be service affecting. You should make all changes during a scheduled maintenance window.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to change the OC-N card settings. If you are already logged in, proceed to Step 2.

Step 2 As needed, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Perform any of the following tasks as needed:

- DLP-A379 Change Line Transmission Settings for OC-N Cards, page 20-72
- DLP-A171 Change Threshold Settings for OC-N Cards, page 18-51
- DLP-A459 Change Optics Thresholds Settings for OC-192, MRC-12, and MRC-2.5G-4 Cards, page 21-40
- DLP-A527 Change the OC-N Card ALS Maintenance Settings, page 22-28
- DLP-A172 Change an Optical Port to SDH, page 18-53

Step 4 As needed, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Stop. You have completed this procedure.

NTP-A118 Modify Alarm Interface Controller–International Settings

Purpose	This procedure provisions the AIC-I card to receive input from or send output to external devices wired to the backplane (called external alarms and controls or environmental alarms). It also changes orderwire settings.
Tools/Equipment	None
Prerequisite Procedures	NTP-A258 Provision External Alarms and Controls on the Alarm Interface Controller–International, page 8-8 DLP-A83 Provision Orderwire, page 17-79
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to change the AIC-I card settings. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Perform any of the following tasks as needed:

- DLP-A208 Change External Alarms Using the AIC-I Card, page 19-6
- DLP-A209 Change External Controls Using the AIC-I Card, page 19-7
- DLP-A210 Change AIC-I Card Orderwire Settings, page 19-7

Step 4 As needed, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Stop. You have completed this procedure.

NTP-A91 Upgrade DS-1 and DS-3 Protect Cards from 1:1 Protection to 1:N Protection

Purpose	This procedure converts DS-1 and DS-3 protect cards from 1:1 to 1:N protection.
Tools/Equipment	None
Prerequisite Procedures	DLP-A71 Create a 1:1 Protection Group, page 17-73
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to convert the DS-1 or DS-3 cards from 1:1 to 1:N protection. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Perform any of the following tasks as needed:

- DLP-A176 Convert DS1-14 Cards From 1:1 to 1:N Protection, page 18-53
- DLP-A177 Convert DS3-12 Cards From 1:1 to 1:N Protection, page 18-55
- DLP-A178 Convert DS3-12E Cards From 1:1 to 1:N Protection, page 18-56
- DLP-A448 Convert DS3XM-6 or DS3XM-12 Cards From 1:1 to 1:N Protection, page 21-28

Step 4 As needed, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Stop. You have completed this procedure.

NTP-A315 Modify Port Settings and PM Parameter Thresholds for FC_MR-4 Cards

Purpose	This procedure changes the line and threshold settings for storage area network (SAN) cards, including the FC_MR-4.
Tools/Equipment	None
Prerequisite Procedures	NTP-A274 Install the FC_MR-4 Card, page 2-15
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Changing card settings can be service affecting. You should make all changes during a scheduled maintenance window.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to change the OC-N card settings. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Perform any of the following tasks as needed:

- DLP-A438 Change General Port Settings for the FC_MR-4 Card, page 21-17
- DLP-A439 Change Distance Extension Port Settings for the FC_MR-4 Card, page 21-19
- DLP-A440 Change Enhanced FC/FICON Port Settings for the FC_MR-4 Card, page 21-21
- DLP-A357 Create FC_MR-4 RMON Alarm Thresholds, page 20-41
- DLP-A358 Delete FC_MR-4 RMON Alarm Thresholds, page 20-45

Step 4 As needed, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Stop. You have completed this procedure.

NTP-A321 Change Card or PPM Service State

Purpose	This procedure changes a card or port's service state, which is an autonomously generated state that gives the overall condition of the port.
Tools/Equipment	None
Prerequisite Procedures	Chapter 2, "Install Cards and Fiber-Optic Cable"
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note On the OC192-XFP, MRC-12, and MRC-2.5G-4 cards, the PPM is equivalent to an optical port.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to change the card service state.

Step 2 From node view, click the **Inventory** tab.

Step 3 Choose an Administrative state from the Admin State drop-down list for the card or PPM that you want to change: **IS** (In-Service) or **OOS,MT** (Out-of-Service,Maintenance).

Step 4 Click **Apply**.

Step 5 If an error message appears indicating that the card state cannot be changed from its current state, click **OK**.

Depending on the Administrative state that you choose, the card or port/PPM transitions to a different service state. For more information about the service states and card state transitions, refer to the "Administrative and Service States" appendix of the *Cisco ONS 15454 Reference Manual*.

Stop. You have completed this procedure.

NTP-A322 Manage Pluggable Port Modules

Purpose	This procedure provisions, changes, and deletes PPMs for the MRC-12, MRC-2.5G-4, and OC192-XFP cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A461 Preprovision an SFP or XFP Device, page 21-43 or DLP-A469 Install a GBIC or SFP/XFP Device, page 21-58
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to provision, change, or delete PPMs. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab:

a. Verify that the alarm filter is not turned on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

c. Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export alarm and condition information.

Step 4 As needed, complete the "DLP-A574 Provision a PPM on the MRC-12 or MRC-2.5G-4 Card" task on page 22-88. Single-rate PPMs do not require provisioning.

Step 5 As needed, complete the "DLP-A575 Provision the Optical Line Rate on the MRC-12 or MRC-2.5G-4 Card" task on page 22-89 to assign an OC-3, OC-12, or OC-48 line rate to a multirate PPM.

Step 6 As needed, complete the "DLP-A576 Change the Optical Line Rate on the MRC-12 or MRC-2.5G-4 Card" task on page 22-90 to change the line rate on a multirate PPM. You cannot change the optical line rate on single-rate PPMs.

Step 7 As needed, complete the "DLP-A577 Delete a PPM from the MRC-12, MRC-2.5G-4, or OC192-XFP Card" task on page 22-90.

Stop. You have completed this procedure.

NTP-A346 Provision the Soak Timer for an ML-Series Card

Purpose	This procedure provisions the soak timer for ports on an ML-Series card. The soak period is the amount of time that the ML-Series port remains in the Down state after an error-free signal is continuously received before transitioning to the Up state.
Tools/Equipment	None
Prerequisite Procedures	NTP-A246 Install Ethernet Cards and Connectors, page 2-13
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to provision the soak timer for an ML-Series card. If you are already logged in, continue with Step 2.

Step 2 In node view, double-click the ML-Series card that you want to provision.

Step 3 Click the **Provisioning** tab.

Step 4 Click the **Ether Ports** or **POS Ports** subtab and complete the following:

- PSAS—In the appropriate port row, check this check box to enable Pre-Service Alarm Suppression (PSAS), which suppresses all alarms on the port for the time designated in the Soak Time column.
- Soak Time—In the same row, choose the desired soak time (in hours and minutes). Use this column when you have checked PSAS to suppress alarms. When the port detects a signal, the countdown begins for the designated soak time. Soak time hours can be set from 0 to 48. Soak time minutes can be set from 0 to 45 in 15 minute increments.

Step 5 Click **Apply**.

Stop. You have completed this procedure.

NTP-A352 View PPM Information on the LCD

Purpose	This procedure displays the line rate and the configured reach for OC-N and MRC cards (MRC-12, MRC-2.5G-4) on the LCD, located on the front of the fan-tray assembly.
Tools/Equipment	None
Prerequisite Procedures	NTP-A16 Install Optical Cards and Connectors, page 2-8
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the ONS 15454 front panel, repeatedly press the **Slot** button until the slot number of the card where the PPM resides appears on the LCD.

Step 2 Repeatedly press the **Port** button. When you see "Status - Lambda" display on the LCD, press the **Status** button to select that option.

Step 3 Press **Status** to toggle between "Lambda" and "Line Rate and Reach."

Step 4 Press **Status** to select one of those options.

Step 5 Press the **Port** button as needed to display the information about the desired port.

Stop. You have completed this procedure.s

NTP-A354 Set or Check Cross-Connect Mode for XC-VXC-10G Cards

Purpose	This procedure is used to set or verify cross-connect mode provisioning required for mixed grooming mode.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to change the XC-VXC-10G card settings. If you are already logged in, continue with Step 2.

Step 2 Navigate to the node view in CTC.

Step 3 Click **Provisioning > Cross-Connect**. The Cross-Connect dialog box is displayed.

Step 4 If necessary, click the **Mixed Mode** radio button in the Cross-Connect dialog box and click **Apply**.

Stop. You have completed this procedure.

CHAPTER 11

Change Node Settings

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter explains how to modify node provisioning for the Cisco ONS 15454. To provision a new node, see Chapter 4, "Turn Up a Node." To change default network element settings and to view a list of those settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Before You Begin

Before performing the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A81 Change Node Management Information, page 11-2—Complete this procedure as needed to change node name, contact information, latitude, longitude, date, time, and login legal disclaimer.
2. NTP-A201 Change CTC Network Access, page 11-2—Complete this procedure as needed to change the IP address, default router, subnet mask, network configuration settings, and static routes.
3. NTP-A319 Modify OSI Provisioning, page 11-3—Complete this procedure as needed to modify Open System Interconnection (OSI) parameters including the OSI routing mode, Target Identifier Address Resolution Protocol (TARP), routers, subnets, and IP over OSI tunnels.
4. NTP-A202 Customize the CTC Network View, page 11-4—As needed, complete this procedure to create domains and customize the appearance of the network map, including specifying a different default map, creating domains, selecting your own map or image, consolidating links, toggling global and local domain settings, and changing the background color.
5. NTP-A203 Modify or Delete Card Protection Settings, page 11-5—Complete as needed.
6. NTP-A292 Modify or Delete Communications Channel Terminations and Provisionable Patchcords, page 11-5—Complete this procedure as needed to modify or delete Section DCC (SDCC) or Line DCC (LDCC) terminations or provisionable patchcords.
7. NTP-A85 Change Node Timing, page 11-6—Complete as needed.

8. NTP-A205 Modify Users and Change Security, page 11-7—Complete this procedure as needed to make changes to user settings, including security level and security policies, to change Remote Authentication Dial In User Service (RADIUS) server settings, and to delete users.
9. NTP-A87 Change SNMP Settings, page 11-7—Complete as needed.

NTP-A81 Change Node Management Information

Purpose	This procedure changes the node name, date, time, contact information, and the login legal disclaimer.
Tools/Equipment	None
Prerequisite Procedures	NTP-A25 Set Up Name, Date, Time, and Contact Information, page 4-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Complete the "DLP-A140 Change the Node Name, Date, Time, and Contact Information" task on page 18-16, as needed.

Step 4 Complete the "DLP-A265 Change the Login Legal Disclaimer" task on page 19-49, as needed.

Step 5 After confirming the changes, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Stop. You have completed this procedure.

NTP-A201 Change CTC Network Access

Purpose	This procedure changes essential network information, including IP settings, static routes, and Open Shortest Path First (OSPF) options.
Tools/Equipment	None
Prerequisite Procedures	NTP-A169 Set Up CTC Network Access, page 4-8
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Additional ONS 15454 networking information and procedures, including IP addressing examples, static route scenarios, OSPF protocol, and Routing Information Protocol (RIP) options are provided in the *Cisco ONS 15454 Reference Manual*.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Perform any of the following tasks as needed:

- DLP-A266 Change IP Settings, page 19-50
- DLP-A142 Modify a Static Route, page 18-17
- DLP-A143 Delete a Static Route, page 18-17
- DLP-A144 Disable OSPF, page 18-18
- DLP-A250 Set Up or Change Open Shortest Path First Protocol, page 19-35
- DLP-A382 Delete a Proxy Tunnel, page 20-78
- DLP-A383 Delete a Firewall Tunnel, page 20-79
- DLP-A434 Lock Node Security, page 21-12
- DLP-A435 Modify Backplane Port IP Settings in Secure Mode, page 21-13
- DLP-A436 Disable Node Security Mode, page 21-15

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Stop. You have completed this procedure.

NTP-A319 Modify OSI Provisioning

Purpose	This procedure modifies the ONS 15454 OSI parameters including the OSI routing mode, TARP, routers, subnets, and IP over CLNS tunnels.
Tools/Equipment	None
Prerequisite Procedures	NTP-A318 Provision OSI, page 4-17
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Additional information about the ONS 15454 implementation of OSI is provided in the "Management Network Connectivity" chapter of the *Cisco ONS 15454 Reference Manual*.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Perform any of the following tasks as needed:

- DLP-A535 Provision or Modify TARP Operating Parameters, page 22-43
- DLP-A536 Add a Static TID to NSAP Entry to the TARP Data Cache, page 22-45
- DLP-A537 Remove a Static TID to NSAP Entry from the TARP Data Cache, page 22-46

- DLP-A538 Add a TARP Manual Adjacency Table Entry, page 22-46
- DLP-A543 Remove a TARP Manual Adjacency Table Entry, page 22-51
- DLP-A544 Change the OSI Routing Mode, page 22-51
- DLP-A545 Edit the OSI Router Configuration, page 22-52
- DLP-A546 Edit the OSI Subnetwork Point of Attachment, page 22-53
- DLP-A547 Edit an IP-Over-CLNS Tunnel, page 22-54
- DLP-A548 Delete an IP-Over-CLNS Tunnel, page 22-55

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Stop. You have completed this procedure.

NTP-A202 Customize the CTC Network View

Purpose	This procedure modifies the Cisco Transport Controller (CTC) network view, including grouping nodes into domains for a less-cluttered display, changing the network view background color, and using a custom image for the network view background.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Complete the following tasks, as needed:

- DLP-A145 Change the Network View Background Color, page 18-18
- DLP-A528 Change the Default Network View Background Map, page 22-30
- DLP-A268 Apply a Custom Network View Background Map, page 19-52
- DLP-A148 Create Domain Icons, page 18-19
- DLP-A149 Manage Domain Icons, page 18-20
- DLP-A269 Enable Dialog Box Do-Not-Display Option, page 19-52
- DLP-A498 Switch Between TDM and DWDM Network Views, page 21-65
- DLP-A495 Consolidate Links in Network View, page 21-62

Stop. You have completed this procedure.

NTP-A203 Modify or Delete Card Protection Settings

Purpose	This procedure modifies and deletes card protection settings.
Tools/Equipment	None
Prerequisite Procedures	NTP-A324 Create Protection Groups, page 4-13
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Modifying and deleting protection groups can be service affecting.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Perform any of the following tasks as needed:

- DLP-A150 Modify a 1:1 Protection Group, page 18-21
- DLP-A152 Modify a 1:N Protection Group, page 18-22
- DLP-A154 Modify a 1+1 Protection Group, page 18-23
- DLP-A561 Modify an Optimized 1+1 Protection Group, page 22-75
- DLP-A155 Delete a Protection Group, page 18-23

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Stop. You have completed this procedure.

NTP-A292 Modify or Delete Communications Channel Terminations and Provisionable Patchcords

Purpose	This procedure changes or deletes SDCC and LDCC terminations and deletes provisionable patchcords on the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A377 Provision Section DCC Terminations, page 20-69 or DLP-A378 Provision Line DCC Terminations, page 20-71 or DLP-A367 Create a Provisionable Patchcord, page 20-51
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Deleting a data communications channel (DCC) termination can cause you to lose visibility of nodes that do not have other DCCs or network connections to the CTC computer.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the following tasks to modify DCC settings:

- DLP-A374 Change a Section DCC Termination, page 20-60.
- DLP-A375 Change a Line DCC Termination, page 20-60.

Step 3 As needed, complete the following tasks to delete DCC terminations:

- DLP-A156 Delete a Section DCC Termination, page 18-24.
- DLP-A359 Delete a Line DCC Termination, page 20-45.

Step 4 As needed, complete the "DLP-A368 Delete a Provisionable Patchcord" task on page 20-52.

Stop. You have completed this procedure.

NTP-A85 Change Node Timing

Purpose	This procedure changes the SONET timing settings for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A28 Set Up Timing, page 4-13
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Internal timing is Stratum 3 and not intended for permanent use. All ONS 15454s should be timed to a Stratum 2 or better primary reference source.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 As needed, complete the "DLP-A157 Change the Node Timing Source" task on page 18-24.

Step 4 If you need to change any internal timing settings, follow the "DLP-A70 Set Up Internal Timing" task on page 17-72 for the settings you need to modify.

Step 5 If you need to verify timing after removing a node from a bidirectional line switched ring (BLSR) or path protection configuration, see the "DLP-A195 Verify Timing in a Reduced Ring" task on page 18-66.

Step 6 Complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Stop. You have completed this procedure.

NTP-A205 Modify Users and Change Security

Purpose	This procedure modifies user and security properties for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A30 Create Users and Assign Security, page 4-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Perform any of the following tasks as needed:

- DLP-A462 View and Terminate Active Logins, page 21-44
- DLP-A271 Change Security Policy on a Single Node, page 19-53
- DLP-A272 Change Security Policy on Multiple Nodes, page 19-54
- DLP-A512 Change Node Access and PM Clearing Privilege, page 22-5
- DLP-A457 Grant Superuser Privileges to a Provisioning User, page 21-39
- DLP-A158 Change User Password and Security Level on a Single Node, page 18-26
- DLP-A160 Change User Password and Security Level on Multiple Nodes, page 18-27
- DLP-A159 Delete a User from a Single Node, page 18-26
- DLP-A161 Delete a User from Multiple Nodes, page 18-28
- DLP-A456 Configure the Node for RADIUS Authentication, page 21-37; this task includes instructions for modifying or deleting a RADIUS server.

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Stop. You have completed this procedure.

NTP-A87 Change SNMP Settings

Purpose	This procedure modifies Simple Network Management Protocol (SNMP) settings for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A256 Set Up SNMP, page 4-16
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Perform any of the following tasks as needed:

- DLP-A273 Modify SNMP Trap Destinations, page 19-56
- DLP-A163 Delete SNMP Trap Destinations, page 18-28

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Stop. You have completed this procedure.

CHAPTER 12

Upgrade Cards and Spans

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter explains how to upgrade common control cards, DS3-12 and DS3N-12 cards, and optical spans for the Cisco ONS 15454.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A220 Upgrade the XCVT Card to the XC10G Card, page 12-2—Complete as needed.
2. NTP-A333 Upgrade the XC/XCVT/XC10G Card to the XC-VXC-10G Card, page 12-3—Complete as needed.
3. NTP-A296 Upgrade the TCC2 Card to the TCC2P Card, page 12-5—Complete as needed.
4. NTP-A93 Upgrade the DS3-12 Card to the DS3-12E Card, page 12-7— Complete as needed.
5. NTP-A308 Upgrade Low-Density Electrical Cards to High-Density Electrical Cards, page 12-9—Complete as needed to upgrade low-density cards in a 1:N configuration to high-density cards.
6. NTP-A254 Downgrade a DS3-12E/DS3NE Card to a DS3-12/DS3N-12 Card, page 12-10—Complete as needed to downgrade a DS3E card or to back out of a DS3-12 to DS3-12E card upgrade.
7. NTP-A94 Upgrade OC-N Cards and Spans Automatically, page 12-12—Complete this procedure as needed to upgrade OC-N cards within path protection configurations, bidirectional line switched rings (BLSRs), and 1+1 protection groups.
8. NTP-A95 Upgrade OC-N Spans Manually, page 12-15—Complete this procedure as needed to perform error recovery for the Span Upgrade Wizard or back out of a span upgrade (downgrade).
9. NTP-A370 Upgrade OC-N Cards Manually, page 12-18—Complete this procedure as needed to upgrade the OC-N cards manually.

Note Always upgrade the standby cross-connect card first. Active cross-connect (XC10G/XCVT/XCVXL/XCVXC) cards should not be physically removed unless you first perform an XCVT/XC10G/XCVXL/XCVXC side switch or TCC2/TCC2P reset. You may remove the card once it comes to standby. Alternatively, perform a lockout on all circuits originating from the node whose active cross-connect or active TCC2/TCC2P needs to be removed. Performing a lockout on all spans also accomplishes the same goal. No lockout is necessary for switches initiated through CTC or through TL1.

NTP-A220 Upgrade the XCVT Card to the XC10G Card

Purpose	This procedure upgrades an XCVT card to an XC10G card.
Tools/Equipment	Two XC10G cards
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Caution Always upgrade the standby cross-connect card. Removing an active cross-connect card can cause a protection switch unless a lockout is in place. If the standby card is being upgraded, a lockout is unnecessary.

Note The XC10G requires the 15454-SA-ANSI or the 15454-SA-HD shelf assembly.

Note The UNEQ-P alarm is raised during a cross-connect card upgrade if you have E100T-12/E1000-2 cards installed in the node. The alarm will clear within a few seconds.

Note The Interconnection Equipment Failure alarm might appear during the upgrade procedure, but will clear when the upgrade is complete and the node has matching cross-connect cards installed.

Note Downgrading from XC10G cards to XCVT cards is not supported. Contact the Cisco Technical Assistance Center (TAC) for more information (see the "Obtaining Documentation and Submitting a Service Request" section on page lxiv).

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will perform the upgrade. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Determine the standby XCVT card. The ACT/STBY LED of the standby XCVT card is amber, while the ACT/STBY LED of the active XCVT card is green.

Step 4 Physically replace the standby XCVT card on the ONS 15454 with an XC10G card:

a. Open the XCVT card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

c. Open the ejectors on the XC10G card.

d. Slide the XC10G card into the slot along the guide rails.

e. Close the ejectors.

Note On the XC10G card, the fail LED above the ACT/STBY LED becomes red, blinks for some time (20 to 30 seconds), and turns off. The ACT/STBY LED turns amber and remains on. In node view, the XC10G appears as the standby XCVT.

Step 5 In node view, click the **Maintenance > Cross-Connect** tabs.

Step 6 From the Cross Connect Cards menu, choose **Switch**.

Step 7 Click **Yes** in the Confirm Switch dialog box. Traffic switches to the XC10G card you inserted in Step 4. The ACT/STBY LED on this card changes from amber to green.

Step 8 Physically remove the now standby XCVT card from the ONS 15454 and insert the second XC10G card into the empty XCVT card slot:

a. Open the XCVT card ejectors.

b. Slide the XCVT card out of the slot.

c. Open the ejectors on the XC10G card.

d. Slide the XC10G card into the slot along the guide rails.

e. Close the ejectors.

The upgrade is complete when the second XC10G card boots up and becomes the standby XC10G card. In node view, both the active and standby cards will change to XC10G.

Note After you change out the first card, CTC continues to display the XCVT card in both slots. The display does not change to reflect the XC10G cards until the second card is upgraded and the XC10G card in that slot boots up.

Stop. You have completed this procedure.

NTP-A333 Upgrade the XC/XCVT/XC10G Card to the XC-VXC-10G Card

Purpose	This procedure upgrades the XC or XCVT or XC10G card to an XC-VXC-10G card.
Tools/Equipment	Two XC-VXC-10G cards
Prerequisite Procedures	None

Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Note The XC-VXC-10G requires the 15454-SA-ANSI or the 15454-SA-HD shelf assembly.

Note The UNEQ-P alarm is raised during a cross-connect card upgrade if you have E100T-12/E1000-2 cards installed in the node. The alarm will clear within a few seconds.

Note The CTNEQPT-MISMATCH, CTNEQPT-PBWORK, or CTNEQPT-PBPROT alarms might appear during the upgrade procedure, but will clear when the upgrade is complete and the node has matching cross-connect cards installed.

Note The SWMTXMOD-PROT and SWMTXMOD-WORK alarms might appear when the standby and active cross-connect cards are replaced, but will clear after the cards are replaced.

Note Downgrading from XC-VXC-10G cards to XC or XCVT or XC10G cards is not supported. Contact the Cisco TAC for more information (see the "Obtaining Documentation and Submitting a Service Request" section on page lxiv).

Caution Always upgrade the standby cross-connect card. Removing an active cross-connect card can cause a protection switch unless a lockout is in place. If the standby card is being upgraded, a lockout is unnecessary.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will perform the upgrade. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Complete the "DLP-A600 Perform BLSR Lockout" task on page 23-1 to avoid short wrap condition if the XC or XCVT or XC10G card that are being replaced are on the node which is part of BLSR ring.

Step 4 Determine the standby XC or XCVT or XC10G card. The ACT/STBY LED of the standby XC or XCVT or XC10G card is amber, while the ACT/STBY LED of the active XC or XCVT or XC10G card is green.

Step 5 Physically replace the standby XC or XCVT or XC10G card on the ONS 15454 with an XC-VXC-10G card:

- **a.** Open the XC or XCVT or XC10G card ejectors.
- **b.** Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.
- **c.** Open the ejectors on the XC-VXC-10G card.
- **d.** Slide the XC-VXC-10G card into the slot along the guide rails.

e. Close the ejectors.

Note On the XC-VXC-10G card, the fail LED above the ACT/STBY LED becomes red, blinks for some time (20 to 30 seconds), and turns off. The ACT/STBY LED turns amber and remains on.

Step 6 In node view, click the **Maintenance > Cross-Connect** tabs.

Step 7 From the Cross Connect Cards menu, choose **Switch**.

Note When upgrading from XC or XCVT or XC10G card to an XC-VXC-10G card with Path Protection circuits and a cross connect side switch is performed, the path protected circuits may switch from a working to protect path causing traffic hit.

Step 8 Click **Yes** in the Confirm Switch dialog box. Traffic switches to the XC-VXC-10G card that you inserted in Step 4. The ACT/STBY LED on this card changes from amber to green.

Step 9 Physically remove the now standby XC or XCVT or XC10G card from the ONS 15454 and insert the second XC-VXC-10G card into the empty XC or XCVT or XC10G card slot:

a. Open the XC or XCVT or XC10G card ejectors.

b. Slide the XC or XCVT or XC10G card out of the slot.

c. Open the ejectors on the XC-VXC-10G card.

d. Slide the XC-VXC-10G card into the slot along the guide rails.

e. Close the ejectors.

The upgrade is complete when the second XC-VXC-10G card boots up and becomes the standby XC-VXC-10G card. In node view, both the active and standby cards change to XC-VXC-10G.

Note After you change out the first card, CTC continues to display the XC or XCVT or XC10G card in both slots. The display does not change to reflect the XC-VXC-10G cards until the second card is upgraded and the XC-VXC-10G card in that slot boots up.

Step 10 Complete the "DLP-A601 Remove BLSR Lockout" task on page 23-2 to remove BLSR Lockout performed in Step 3.

Stop. You have completed this procedure.

NTP-A296 Upgrade the TCC2 Card to the TCC2P Card

Purpose	This procedure upgrades the TCC2 card to the TCC2P card. The TCC2 and TCC2P cards support ONS 15454 Software R4.0 and later software versions.
Tools/Equipment	Two SONET TCC2P cards Two TCC2 cards
Prerequisite Procedures	None

Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Note Downgrading from TCC2P cards to TCC2 cards is not supported. Contact Cisco TAC for more information (see the "Obtaining Documentation and Submitting a Service Request" section on page lxiv).

Caution Active TCC2 card should not be physically removed unless you first perform a soft reset of TCC2 card. You may remove the TCC2 card after it becomes a standby card.

Step 1 Verify that the LAN wires on the backplane are installed properly. The TCC2 card does not autodetect miswired LAN connections. If a LAN connection is miswired, a LAN Connection Polarity Reversed condition appears. See the "DLP-A21 Install LAN Wires on the Backplane" task on page 17-25 for instructions.

Step 2 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 3 Ensure that no alarms or abnormal conditions are present. See the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63 for instructions.

Step 4 Before you begin the upgrade, complete the "NTP-A108 Back Up the Database" procedure on page 15-5. Make sure ONS 15454 Software R4.0 or later is installed on the node. Refer to the release-specific software upgrade document. TCC2 and TCC2P cards are not compatible with releases prior to Software R4.0.

Step 5 Physically replace the standby TCC2 card on the ONS 15454 with a TCC2P card:

- **a.** Check the LED on the faceplate. The ACT/STBY LED on the faceplate of the TCC2 card indicates whether the card is in active or standby mode. A green ACT/STBY LED indicates an active card and an amber light indicates a standby card.
- **b.** Open the standby TCC2 card ejectors.
- **c.** Slide the card out of the slot. This raises the IMPROPRMVL alarm which will clear when the upgrade is complete.
- **d.** Open the ejectors on the TCC2P card to be installed.
- **e.** Slide the TCC2P card into the slot along the guide rails.
- **f.** Close the ejectors.
- **g.** In CTC node view, Ldg (loading) appears on the recently installed TCCP2 card.

Note During a TCC2 upgrade, the CONTBUS-IO-A or CONTBUS-IO-B TCC A (or B) To Shelf Slot Communication Failure alarm is raised as the TCC2 briefly loses communication with the backplane. This alarm usually clears after approximately 13 minutes. If the condition does not clear after a period, log onto http://www.cisco.com/tac for more information or call Cisco TAC at (800) 553-2447.

Note It takes approximately 10 minutes for the active TCC2 card to transfer the database to the newly installed TCC2P card. During this operation, the LEDs on the TCC2P flash Fail and then the active/standby LED flashes. When the transfer completes, the TCC2P card reboots and goes into standby mode after approximately three minutes. Do not remove the card from the shelf during a database transfer.

Caution If your active TCC2 card resets during the upgrade before the new TCC2P card has come to a full standby mode, remove the new TCC2P card immediately.

Step 6 When the newly installed TCC2P card is in standby, go to the active TCC2 and right-click the card.

Step 7 From the drop-down list, click **Reset Card**.

Wait for the TCC2 card to reboot. The ONS 15454 switches the standby TCC2P card to active mode. The TCC2 card verifies that it has the same database as the TCC2P card and then switches to standby.

Step 8 Verify that the remaining TCC2 card is now in standby mode (the ACT/STBY LED changes to amber).

Step 9 Perform Step 5 to physically replace the remaining TCC2 card with the second TCC2P card.

The ONS 15454 boots up the second TCC2P card. The second TCC2P card must also copy the database, which can take approximately 10 minutes. Do not remove the card from the shelf during a database transfer.

Step 10 If power-related alarms occur after the second TCC2P card is installed, check the voltage on the backplane. See the "DLP-A33 Measure Voltage" task on page 17-36 for instructions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for information about clearing alarms.

Stop. You have completed this procedure.

NTP-A93 Upgrade the DS3-12 Card to the DS3-12E Card

Purpose	This procedure upgrades the DS3-12 card to the DS3-12E card or the DS3N-12 card to the DS3N-12E card. This procedure can also be used to enable the capabilities of a DS3-12E card that was installed in a shelf with Software R3.1 or earlier.
Tools/Equipment	DS3-12E or DS3N-12E card
Prerequisite Procedures	NTP-A17 Install the Electrical Cards, page 2-11
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note Upgrades must be performed between two N-type cards or two non-N-type cards. You cannot upgrade between an N-type card and a non-N-type card. When physically replacing a card, the new card must be in the same slot as the old card. The DS3-12E card upgrade supports 1:1 and 1:N protection schemes. The procedure is non-service-affecting for protected cards; that is, the upgrade will cause a switch less than 50 ms in duration.

Note In CTC, the DS3-12E/DS3N-12E card is displayed as DS3E/DS3NE.

Caution Protect cards must be upgraded before working cards because working cards cannot have more capabilities than their protect card.

Note During the upgrade, some minor alarms and conditions appear and then clear on their own; however, there should be no service-affecting (SA, Major, or Critical) alarms if you are upgrading protected cards. (Upgrading an unprotected card can be service affecting.) If any service-affecting alarms occur, Cisco recommends backing out of the procedure. See the "NTP-A254 Downgrade a DS3-12E/DS3NE Card to a DS3-12/DS3N-12 Card" procedure on page 12-10.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Determine if the card you are upgrading is protected or unprotected:

- **a.** Protected cards are listed under Protection Groups on the **Maintenance > Protection** tab. The slot, port, and status (that is, Protect/Standby, Working/Active) of each card is listed in the Selected Group area.
- **b.** An unprotected card is not listed in the Protection Groups/Selected Group area on the **Maintenance > Protection** tab.

Caution Traffic will be lost during an upgrade on an unprotected card.

Step 4 If the card you are upgrading is unprotected, skip this step and go to Step 5, ignoring references to the protect card and protect slot. If the card you are upgrading is protected, make sure the protect card is not active. If the card status is Protect/Active, perform a switch so that the working card becomes active:

- **a.** Double-click the protection group.
- **b.** Click the Protect/Active card.
- **c.** Click **Switch.**
- **d.** Click **Yes** in the confirmation dialog box.

Step 5 Physically remove the protect DS3-12 or the protect DS3N-12 card:

- **a.** Open the DS3-12 or DS3N-12 card ejectors.
- **b.** Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

Step 6 Right-click the protect slot and choose **Change Card** from the drop-down list.

Step 7 Choose the new card (DS3-12E or DS3N-12E) from the Change to drop-down list.

Step 8 Click **OK**.

Step 9 Insert the new DS3-12E or DS3N-12E card into the protect slot:

- **a.** Open the ejectors on the DS3-12E or DS3N-12E card.

b. Slide the DS3-12E or DS3N-12E card into the slot along the guide rails.

Step 10 Close the ejectors.

Wait for the IMPROPRMVL alarm to clear and the card to become standby.

Step 11 If you switched traffic in Step 4, clear the switch:

a. On the **Maintenance > Protection** tabs, double-click the protection group that contains the reporting card.

b. Click the selected group.

c. Click **Clear** and click **Yes** at the confirmation dialog box.

Step 12 Repeat Steps 3 through 11 for the working card.

Stop. You have completed this procedure.

NTP-A308 Upgrade Low-Density Electrical Cards to High-Density Electrical Cards

Purpose	This procedure upgrades DS-1 and DS3-12 electrical cards in a 1:N protection scheme (where N = 1 or 2) to high-density electrical cards (DS3/EC1-48, DS1/E1-56, and DS3XM-12 cards). This procedure also upgrades DS3XM-6 cards in a 1:1 protection scheme to DS3XM-12 cards, and EC-1 cards to DS3/EC1-48 cards.
Tools/Equipment	DS3/EC1-48 card(s), as needed DS3XM-12 card(s), as needed DS1/E1-56 card(s), as needed High-density shelf assembly (15454-SA-HD) High-density EIA (MiniBNC, UBIC-V, UBIC-H) installed
Prerequisite Procedures	NTP-A17 Install the Electrical Cards, page 2-11
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Protect cards must be upgraded before working cards because working cards cannot have more capabilities than their protect card.

Note During the upgrade some minor alarms and conditions appear and then clear on their own; however, there should be no Service-Affecting (SA, Major, or Critical) alarms if you are upgrading protected cards. (Upgrading an unprotected card can be service affecting.) If any service-affecting alarms occur, Cisco recommends backing out of the procedure.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 As needed, complete the "DLP-A553 Upgrade DS3XM-6 Cards in a 1:1 Configuration to High-Density DS3XM-12 Electrical Cards" task on page 22-62.

Step 4 As needed, complete the "DLP-A554 Upgrade EC-1 Cards in a 1:1 Configuration to DS3/EC1-48 Cards" task on page 22-65.

Step 5 Repeat Steps 3 through 4 for additional electrical cards you want to upgrade. (If you are upgrading cards in a 1:N configuration, the card is typically in Slot 2/Slot 16.)

Stop. You have completed this procedure.

NTP-A254 Downgrade a DS3-12E/DS3NE Card to a DS3-12/DS3N-12 Card

Purpose	This task downgrades a DS3-12E or DS3NE card. Downgrading can be performed to back out of an upgrade.The procedure for downgrading is the same as upgrading except you choose DS3-12 or DS3N-12 from the Change Card drop-down list.
Tools	None
Prerequisite Procedures	NTP-A17 Install the Electrical Cards, page 2-11
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note All ports must be provisioned as UNFRAMED and have Path Trace disabled.

Note Working cards must be downgraded before protect cards.

Tip The procedure for downgrading is the same as upgrading except you choose DS3-12 or DS3N-12 from the Change Card drop-down list.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Determine if the card you are downgrading is protected or unprotected:

a. A protected card is listed in the Protection Groups area on the **Maintenance > Protection** tab. The slot, port, and status (that is, Protect/Standby, Working/Active) of each card is listed in the Selected Group area.

b. An unprotected card is not listed in the Protection Groups/Selected Group area in the **Maintenance > Protection** tab.

Caution Traffic is lost during an upgrade on an unprotected card.

Step 4 If the card you are upgrading is unprotected, skip this step and go to Step 5, ignoring references to the protect card and protect slot. If the card you are upgrading is protected, make sure that the protect card is not active. If the card status is Protect/Active, perform a switch so that the working card becomes active:

a. Double-click the protection group.

b. Click the Protect/Active card.

c. Click **Switch** and **Yes** in the Confirmation dialog box.

Step 5 Physically remove the working DS3-12E card or the working DS3N-12E card:

a. Open the DS3-12E or DS3N-12E card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the downgrade is complete.

Step 6 Right-click the slot to be downgraded and choose **Change Card** from the drop-down list.

Step 7 Choose **DS3-12** or **DS3N-12** from the Change to drop-down list.

Step 8 Click **OK**.

Step 9 Insert the DS3-12 or DS3N-12 card into the working slot:

a. Open the ejectors on the DS3-12 or DS3N-12 card.

b. Slide the DS3-12 or DS3N-12 card into the slot along the guide rails.

Step 10 Close the ejectors. Wait for the IMPROPRMVL alarm to clear and the card to become active.

Step 11 If you switched traffic in Step 4, clear the switch:

a. In the **Maintenance > Protection** tabs, double-click the protection group that contains the reporting card.

b. Click the selected group.

c. Click **Clear** and click **Yes** in the confirmation dialog box.

Step 12 Repeat Steps 3 through 11 to downgrade the protect card if applicable.

Stop. You have completed this procedure.

NTP-A94 Upgrade OC-N Cards and Spans Automatically

Purpose	This procedure upgrades cards, two-fiber BLSR spans, four-fiber BLSR spans, path protection spans, and 1+1 protection group spans. The Span Upgrade Wizard only supports OC-N span upgrades. It does not support electrical upgrades.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade (for example, XC10G or XC-VXC-10G cards and OC-48 any slot [AS] cards) Attenuators might be needed for some applications
Prerequisite Procedures	The span upgrade procedure requires at least two technicians (one at each end of the span) who can communicate with each other during the upgrade.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Caution Do not perform any other maintenance operations, such as facility or terminal loopbacks, or add any circuits during a card or span upgrade.

Note OC-N transmit and receive levels should be in their acceptable range as shown in the specifications for each card in Table 2-5 on page 2-20.

Note During upgrade, when replacing the PPMs, ensure that the reach of the PPMs match.

Note During the upgrade, the IMPROPRMVL alarm might be raised. It will clear automatically.

Note A four-port OC-3 to eight-port OC-3 upgrade, or an OC-12 to four-port OC-12 upgrade can only be performed from Slots 1 to 4 and 14 to 17 because the OC3-8 and OC12-4 card can only be installed in these slots. Ensure that the OC-3 and OC-12 cards are in these slots before performing a span upgrade to the OC3-8 and OC12-4. The four OC-3 ports will be mapped to Ports 1 to 4 on the eight-port OC-3 card. The OC-12 port will be mapped to Port 1 on the four-port OC-12 card.

Note BLSR PCA circuits, if present, will remain in their existing STSs. Therefore, they will be located on the working path of the upgraded span and will have full BLSR protection. To route PCA circuits on protection channels in the upgraded span, delete and recreate the circuits after the span upgrade. For

example, if you upgrade an OC-48 span to an OC-192, PCA circuits on the protection STSs (STSs 25 to 48) in the OC-48 BLSR will remain in their existing STSs (STSs 25 to 48), which are working, protected STSs in the OC-192 BLSR. Deleting and recreating the OC-48 PCA circuits moves the circuits to STSs 96 to 192 in the OC-192 BLSR. To delete circuits, see the "NTP-A278 Modify and Delete Overhead Circuits and Server Trails" procedure on page 7-5. To create circuits, see Chapter 6, "Create Circuits and VT Tunnels."

Note Before performing automatic Span Upgrade, make sure that the TCC card is not soft resetting or pulled out and there are no fiber cuts or node power cycles.

Step 1 Determine the type of upgrade you need to make and be sure you have the necessary cards. Valid card upgrades include:

- Four-port OC-3 to eight-port OC-3
- Single-port OC-12 to four-port OC-12
- Single-port OC-12 to OC-48
- Single-port OC-12 to OC-192
- Single-port OC-12 to OC-48 on MRC-12
- Single-port OC-12 to OC-48 on MRC-4-2.5G
- OC-48 to MRC-12
- OC-48 to MRC-4-2.5G
- MRC-4 to MRC-12
- MRC-4-2.5G to MRC-12
- OC-48 to OC192SR1/STM64IO Short Reach or OC192/STM64 Any Reach
- OC-192 to OC192SR1/STM64IO Short Reach or OC192/STM64 Any Reach
- MRC-12 to OC192SR1/STM64IO Short Reach or OC192/STM64 Any Reach
- MRC-4-2.5G to OC192SR1/STM64IO Short Reach or OC192/STM64 Any Reach

Note MRC-4-2.5G card upgrade to MRC-12 card is possible only if Port 1 is the only provisioned port on the MRC-4-2.5G card.

Note MRC-12 and MRC-4-2.5G card upgrades to OC192SR1/STM64IO Short Reach or OC192/STM64 Any Reach is possible only if Port 1 is the only provisioned port on the MRC-12 and MRC-4-2.5G cards.

Valid span upgrades include:

- Single-port OC-12 to OC-48
- Single-port OC-12 to OC-192
- Single-port OC-12 to four-port OC-12
- Single-port OC-12 to OC-48 on MRC-12
- OC-3 to OC-12 on MRC-4-2.5G

- OC-3 to OC-48 on Port 1 of MRC-4-2.5G
- OC-12 to OC-48 on Port 1 of MRC-4-2.5G
- OC-48 to OC-192
- OC-48 to MRC-12
- OC-48 to MRC-2.5G-12
- OC-48 to OC192SR1/STM64IO Short Reach or OC192/STM64 Any Reach
- OC-192 to OC192SR1/STM64IO Short Reach or OC192/STM64 Any Reach
- MRC-4-2.5G to MRC-12

Caution You cannot upgrade a four-port OC-12 span. If the ring contains any OC12-4 cards and you need to upgrade all the spans in the ring, you will need to downgrade the OC12-4 card to a single-port OC-12 card (which is only possible if only one port on the OC12-4 card is being used).

Step 2 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 3.

Note The Span Upgrade option will only be visible and available if the hardware necessary for the upgrade is present; for example, no upgrade is possible from an OC-48 span unless XC10G or XC-VXC-10G cards are installed in the nodes at both ends of the span.

Step 3 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 4 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, signal failure (SF), signal degrade (SD), and FORCED-REQ-RING are present. See the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63 for instructions.

Note During the upgrade/downgrade some minor alarms and conditions display and then clear automatically. No service-affecting alarms (SA, Major, or Critical) should occur other than BLSROSYNC, which will clear when the upgrade/downgrade of all nodes is complete. If any other service-affecting alarms occur, Cisco recommends backing out of the procedure.
A four-node BLSR can take up to five minutes to clear all of the BLSROSYNC alarms. Allow extra time for a large BLSR to clear all of the BLSROSYNC alarms.

Note When a fixed port or STMN card with several minor and major alarms is upgraded to an MRC card, all the alarms with the exception of the AID applicable to the MRC card is cleared as soon as the upgrade is complete.

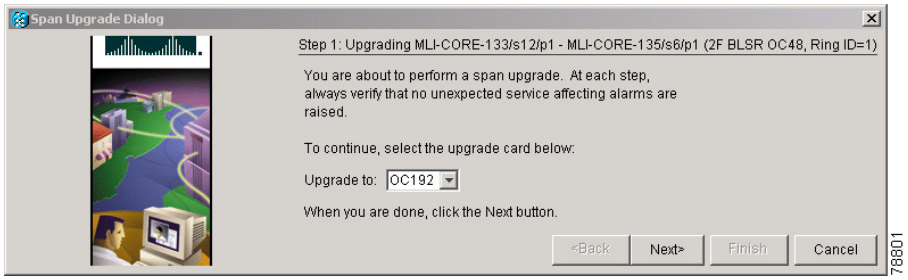
Step 5 In network view, right-click the span you want to upgrade.

Step 6 Choose **Span Upgrade** from the drop-down list.

The Span Upgrade wizard shown in Figure 12-1 appears. The information displayed in Figure 12-1depends on the card that is upgraded. Follow the instructions in the wizard to complete the span upgrade.

Note The Back button is only enabled in Step 2 of the wizard; because you cannot back out of an upgrade using the wizard, close the wizard and initiate the manual procedure if you need to back out of the upgrade at any point beyond Step 2.

Figure 12-1 Span Upgrade Wizard



Caution As indicated by the wizard, when installing cards you must wait for the cards to boot up and become active before proceeding to the next step. For the cards that support SFPs, prior to the installation of fiber the SFPs need to be checked for proper type (MM/SM/wavelength, etc.).

Note Remember to attach the fiber after installing the OC-N cards.

Note The span upgrade process resets the line's CV-L threshold to factory default. The CV-L threshold is reset because the threshold is dependent on line rate.

Step 7 Repeat Steps 5 through 6 for additional spans in the ring.

Stop. You have completed this procedure.

NTP-A95 Upgrade OC-N Spans Manually

Purpose	This procedure upgrades OC-N speeds within BLSRs, path protection configurations, and 1+1 protection groups by upgrading OC-N cards. Complete a manual upgrade task if you need to perform error recovery for the Span Upgrade Wizard or back out of a span upgrade (downgrade).
Tools/Equipment	Replacement cards
Prerequisite Procedures	The manual span upgrade procedure requires at least two technicians (one at each end of the span) who can communicate with each other during the upgrade.
Required/As Needed	As needed

Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note OC-N card transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in Table 2-5 on page 2-20.

Note In this context, the word "span" represents the OC-N path between two nodes. The phrase "span endpoint" represents the nodes on each end of a span.

Note If any of the cross-connect cards reboot during the span upgrade, you must reset each one when the span upgrade procedure is complete for all the nodes in the ring.

Step 1 Determine the type of span you need to upgrade and make sure you have the necessary cards. Valid span upgrades include:

- Four-port OC-3 to eight-port OC-3
- Single-port OC-12 to four-port OC-12
- Single-port OC-12 to OC-48
- Single-port OC-12 to OC-192
- Single-port OC-12 to MRC-12
- Single-port OC-12 to MRC-4-2.5G
- OC-48 to OC-192
- OC-192 to OC192SR1/STM64IO Short Reach or OC192/STM64 Any Reach
- MRC-12 to OC-192 or OC192-XFP
- MRC-4-2.5G to OC-192 or OC192-XFP

Caution You cannot upgrade a four-port OC-12 span. If the ring contains any OC12-4 cards and you need to upgrade all the spans in the ring, you will need to downgrade the OC12-4 card to a single-port OC-12 card (which is not possible unless only one port on the OC12-4 card is being used).

Step 2 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 3.

Step 3 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 4 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present. See the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63 for instructions.

Note During the upgrade/downgrade, some minor alarms and conditions display and then clear automatically. No service-affecting alarms (SA, Major, or Critical) should occur other than BLSROSYNC, which will clear when the upgrade/downgrade of all nodes is complete. If any other service-affecting alarms occur, Cisco recommends backing out of the procedure. A four-node BLSR can take up to five minutes to clear all of the BLSROSYNC alarms. Allow extra time for a large BLSR to clear all of the BLSROSYNC alarms. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for information about alarms.

Step 5 Complete the appropriate task:

- DLP-A293 Perform a Manual Span Upgrade on a Two-Fiber BLSR, page 19-57
- DLP-A294 Perform a Manual Span Upgrade on a Four-Fiber BLSR, page 19-58
- DLP-A295 Perform a Manual Span Upgrade on a Path Protection Configuration, page 19-59
- DLP-A296 Perform a Manual Span Upgrade on a 1+1 Protection Group, page 19-60
- DLP-A297 Perform a Manual Span Upgrade on an Unprotected Span, page 19-62

Note The span upgrade process resets the line's CV-L threshold to factory default. The CV-L threshold is reset because the threshold is dependent on line rate.

Note The Span Upgrade option will only be visible and available if the hardware necessary for the upgrade is present; for example, no upgrade is possible from an OC48 span unless XC10G or XC-VXC-10G cards are installed in the nodes at both ends of the span.

Note A four-port OC-3 to eight-port OC-3 span upgrade or an OC-12 to four-port OC-12 span upgrade can only be performed from Slots 1 to 4 and 14 to17, because the OC3-8 and OC12-4 cards can only be installed in these slots. Ensure that the OC-3 and OC-12 cards are in these slots before performing a span upgrade to the OC3-8 and OC12-4. The four OC-3 ports will be mapped to Ports 1-4 on the eight-port OC-3 card. The OC-12 port will be mapped to Port 1 on the four-port OC-12 card.

Stop. You have completed this procedure.

NTP-A370 Upgrade OC-N Cards Manually

Purpose	This procedure upgrades OC-N cards. OC-N card upgrades can be performed only on OC-N drop cards. If the OC-N card is used as a trunk card or is involved in a two-fiber or four-fiber BLSR, perform a span upgrade.
Tools/Equipment	• Higher-rate cards • XC10G or XC-VXC-10G cards • Attenuators may be required for some upgrades.
Prerequisite Procedures	"DLP-A60 Log into CTC" task on page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Caution Do not perform any other maintenance operations, such as facility or terminal loopbacks, or add any circuits during a card upgrade.

Note OC-N transmit and receive levels must be in their acceptable range as shown in the specifications for each card in Table 2-5 on page 2-20.

Note The card upgrade process resets the line CV-L threshold to factory default. The CV-L threshold is reset because the threshold is dependent on line rate.

Note

- A four-port OC-3 to eight-port OC-3 upgrade, or an OC-12 to four-port OC-12 upgrade can only be performed in Slots 1 to 4 and Slots 14 to 17 because the OC3-8 or OC12-4 card can only be installed in these slots. Ensure that the OC-3 or OC-12 card is in these slots before performing a card upgrade to the OC3-8 or OC12-4 card. The four OC-3 ports will be mapped to Ports 1 to 4 on the eight-port OC-3 card. The OC-12 port will be mapped to Port 1 on the four-port OC-12 card.
- When performing a card upgrade from OC-12, OC-48, MRC-12, or MRC-4-2.5G to OC-192, ensure that the OC-12, OC-48, MRC-12, or MRC-4-2.5G card is in Slot 5, 6, 12, or 13.
- A four-port OC-3 card can be upgraded to a MRC-12 or MRC-4-2.5G card in Slots 1 to 6 and Slots 12 to 17. An eight-port OC-3 or a four-port OC-12 card can be upgraded to a MRC-12 or MRC-4-2.5G card in Slots 1 to 4 and 14 to 17. Ensure that the OC-3 and OC-12 cards are in these slots before performing a card upgrade to the MRC-12 or MRC-4-2.5G card. Port migrations are described in Table 12-1.

Table 12-1 Port Migration Information

Original Card	Old Port Numbers	Slot Type	Upgraded Card	New Port Numbers	Cross-Connect Card
OC3-4	1 to 4	Trunk/Drop	MRC-12/MRC-4-2.5G	1 to 4	XC10G/XC-VXC-10G
OC3-4	1 to 4	Drop	MRC-12	1, 4, 7, 10	XCVT
OC3-4	1 to 4	Drop	MRC-4-2.5G	1 to 4	XCVT
OC3-4	1 to 4	Trunk	MRC-12/MRC-4-2.5G	1 to 4	XCVT
OC3-8	1 to 8	Drop	MRC-12	1 to 8	XC10G/XC-VXC-10G
OC12-4	1 to 4	Drop	MRC-12	1, 4, 7, 10	XC10G/XC-VXC-10G
OC12-4	1 to 4	Drop	MRC-4-2.5G	1 to 4	XC10G/XC-VXC-10G
OC3-4	1 to 4	Drop	OC3-8	1 to 4	XC10G/XC-VXC-10G
OC-12	1	Drop	OC12-4	1	XC10G/XC-VXC-10G
OC-12	1	Drop	MRC-4-2.5G	1	XC10G/XC-VXC-10G
OC-12	1	Drop	MRC-12	1	XC10G/XC-VXC-10G
OC-12	1	Drop	OC-48	1	XC10G/XC-VXC-10G
OC-12	1	Drop	OC-192	1	XC10G/XC-VXC-10G
OC 48	1	Drop	MRC-12	1	XC10G/XC-VXC-10G
OC 48	1	Drop	MRC-4-2.5G	1	XC10G/XC-VXC-10G
OC-48	1	Drop	OC-192	1	XC10G/XC-VXC-10G
MRC-4[1]	1 to 4	Drop	MRC-12	1, 4, 7, 11	XC10G/XC-VXC-10G
MRC-4-2.5G[1]	1 to 4	Drop	MRC-12	1, 4, 7, 11	XC10G/XC-VXC-10G
MRC-12	1	Drop	OC-192	1	XC10G/XC-VXC-10G
MRC-4-2.5G	1	Drop	OC-192	1	XC10G/XC-VXC-10G

1. Supported from R9.2 onwards.

Step 1 Determine the type of upgrade you need to perform and make sure you have the necessary cards. Valid card upgrades include:

- Four-port OC-3 to eight-port OC-3, MRC-4-2.5G, or MRC-12
- Eight-port OC-3 to MRC-12
- Single-port OC-12 to four-port OC-12, OC-48, OC-192, MRC-12, or MRC-4-2.5G
- Four-port OC-12 to MRC-4-2.5G or MRC-12
- OC-48 to MRC-12, MRC-4-2.5G, OC-192 Short Reach, or OC-192 Any Reach
- MRC-4 to MRC-12
- MRC-4-2.5G to MRC-12, OC-192 Short Reach, or OC-192 Any Reach (Port 1 is the only provisioned port on the MRC-4-2.5G card)
- OC-192 to OC-192 Short Reach or OC-192 Any Reach

- MRC-12 to OC-192 Short Reach or OC-192 Any Reach (Port 1 is the only provisioned port on the MRC-12 card)

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, and SD are present. See the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63. During the upgrade, the IMPROPRMVL alarm may be raised but will clear automatically.

Step 4 In the node view, right-click the card you want to upgrade and choose the **Change Card** option. The Change Card dialog box appears.

Note The Change Card option is available only if the hardware necessary for the upgrade is present; for example, no upgrade is possible from an OC-12 card unless the XC-10G or XC-VXC-10G cards are installed in the node.

Step 5 Choose the card to upgrade to from the Change to drop-down list.

Step 6 Choose the rate from the Port Rate drop-down list. This field is available only for multi-rate cards.

Step 7 Click **OK** to upgrade the OC-N card to the selected higher-rate OC-N card or MRC card. An MEA (EQPT) alarm is raised because the physical card type does not match the card type provisioned for that slot in CTC.

Step 8 Replace the physical OC-N card with the card selected in Step 7. This clears the MEA (EQPT) alarm. When replacing the PPMs for the upgraded card, ensure that the reach of the PPMs match the values for the upgraded card.

Stop. You have completed this procedure.

CHAPTER 13

Convert Network Configurations

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter explains how to convert from one SONET topology to another in a Cisco ONS 15454 network. For initial network turn up, see Chapter 5, "Turn Up a Network."

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A335 Convert a 1+1 Point-to-Point to a Linear ADM Automatically, page 13-2—Complete as needed.
2. NTP-A154 Convert a 1+1 Point-to-Point to a Linear ADM Manually, page 13-5—Complete as needed if the in-service topology upgrade wizard is not available or you need to back out of the wizard.
3. NTP-A303 Convert an Unprotected Point-to-Point or 1+1 Linear ADM to a Two-Fiber BLSR Automatically, page 13-7—Complete as needed.
4. NTP-A155 Convert a 1+1 Point-to-Point or a Linear ADM to a Two-Fiber BLSR Manually, page 13-9—Complete as needed if the in-service topology upgrade wizard is not available or you need to back out of the wizard.
5. NTP-A342 Convert a Point-to-Point or Linear ADM to a Path Protection Configuration Automatically, page 13-11—Complete as needed.
6. NTP-A156 Convert a Point-to-Point or Linear ADM to a Path Protection Configuration Manually, page 13-12—Complete as needed if the in-service topology upgrade wizard is not available or you need to back out of the wizard.
7. NTP-A267 Convert a Path Protection Configuration to a Two-Fiber BLSR Automatically, page 13-13—Complete as needed.
8. NTP-A210 Convert a Path Protection Configuration to a Two-Fiber BLSR Manually, page 13-15—Complete as needed if the in-service topology upgrade wizard is not available or you need to back out of the wizard.

9. NTP-A374 Convert a BLSR to Path Protection Manually, page 13-17—Complete as needed.
10. NTP-A211 Convert a Two-Fiber BLSR to a Four-Fiber BLSR Automatically, page 13-18—Complete as needed.
11. NTP-A159 Modify a BLSR, page 13-20—Complete as needed to change the BLSR ring name, ring or span reversion times, or node ID.
12. NTP-A376 Upgrading a BLSR Ring Using an MRC-12 Card, page 13-21—Complete as needed to upgrade the BLSR ring using an MRC-12 card.

NTP-A335 Convert a 1+1 Point-to-Point to a Linear ADM Automatically

Purpose	This procedure converts a 1+1 point-to-point (terminal) configuration (two nodes) to a 1+1 linear add-drop multiplexer (ADM) (3 nodes) without losing traffic.
Tools/Equipment	Compatible hardware Attenuators might be needed for some applications.
Prerequisite Procedures	This procedure requires that the node to be added is reachable (has IP connectivity with CTC). Two technicians who can communicate with each other during the upgrade might be needed if the PC running CTC and the ONS 15454 nodes are not at the same location.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note OC-N transmit and receive levels should be in their acceptable range as shown in the specifications for each card in the Table 2-5 on page 2-20.

Note If overhead circuits exist on the network, this procedure is service affecting. The overhead circuits will drop traffic and have a status of PARTIAL after the upgrade is complete.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at one of the two point-to-point nodes. If you are already logged in, continue with Step 2.

Step 2 In network view, right-click the span between the two nodes where you want to add the new node. A dialog box appears.

Step 3 Select **Upgrade Protection**. A drop-down list appears.

Step 4 Select **Terminal to Linear** and the first page of the Upgrade Protection: Terminal to Linear wizard appears.

Step 5 The first page of the wizard lists the following conditions for adding a new node:

- The terminal network has no critical or major alarms.
- The node that you will add has no critical or major alarms.
- The node has compatible software version with that of the terminal nodes.
- The node has four unused optical ports matching the speed of the 1+1 protection and no communication channel has been provisioned on these four ports.
- Fiber is available to connect the added node to the terminal nodes.

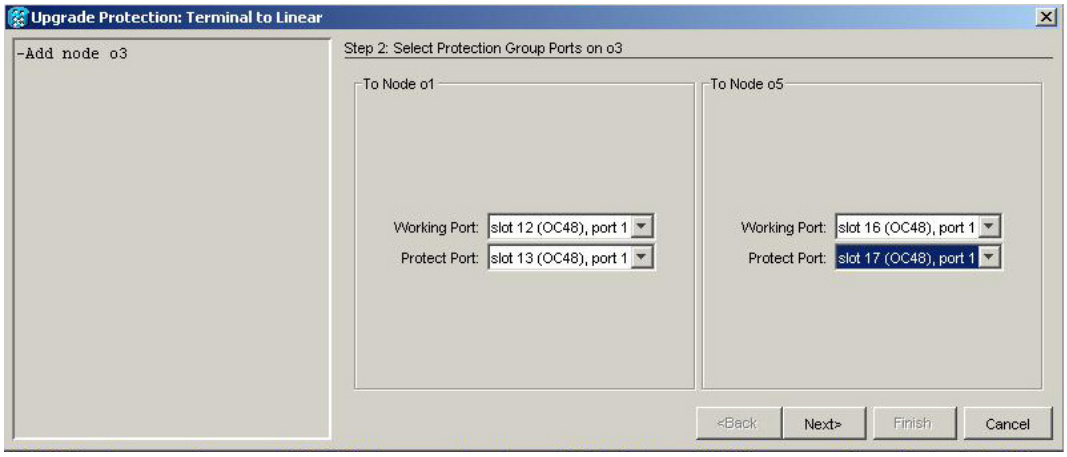
If all of these conditions are met and you wish to continue with the procedure, click **Next**.

Note If you are attempting to add an unreachable node, you must first log in to the unreachable node using a separate CTC session and configure that node. Delete any existing protection groups as described in the "DLP-A155 Delete a Protection Group" task on page 18-23. Delete any existing DCC terminations as described in the "DLP-A156 Delete a Section DCC Termination" task on page 18-24 and the "DLP-A359 Delete a Line DCC Termination" task on page 20-45.

Step 6 Enter the node host name or IP address or choose the name of the new node from the drop-down list. If you type in the name, make sure it is identical to the actual node name. The node name is case sensitive.

Step 7 Click **Next**. The Select Protection Group Ports page (Figure 13-1) appears.

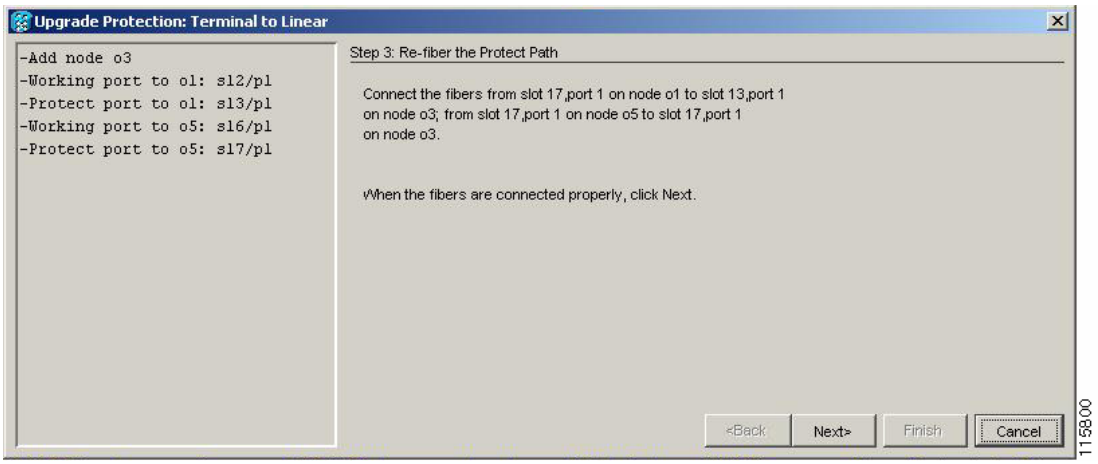
Figure 13-1 Selecting Protection Group Ports



Step 8 Select the working and protect ports on the new node in the drop-down lists that you want to connect to each terminal node.

Step 9 Click **Next**. The Re-fiber the Protected Path dialog box appears (Figure 13-2).

Figure 13-2 Refibering the Protect Path



Step 10 Follow the instructions in the Re-fiber the Protected Path dialog box for connecting the fibers between the nodes.

Step 11 When the fibers are connected properly, click **Next**. The Update Circuit(s) on *Node-Name* dialog box appears.

Note The Back button is not enabled in the wizard. You can click the **Cancel** button at this point and choose the **Yes** button if you want to cancel the Upgrade Protection procedure. If the procedure fails after you have physically moved the fiber-optic cables, you must restore the fiber-optic cables to the original positions and verify (through CTC) that traffic is on the working path of the nodes before restarting the process. To check traffic status, go to node view, click the **Maintenance > Protection** tabs. In the Protection Groups area, click the 1+1 protection group. You can see the status of the traffic in the Selected Group area.

Step 12 Click **Next** on the Update Circuit(s) on *Node-Name* page to continue with the procedure.

Step 13 The Force Traffic to Protect Path page states that it is about to force the traffic from the working to protect path for the terminal nodes. When you are ready to proceed, click **Next**.

Step 14 Follow each step as instructed by the wizard as it guides you through the process of refibering the working path between nodes and forcing the traffic back to the working path.

Step 15 The Force Traffic to Working Path page states that it is about to force the traffic from the protect to working path for the terminal nodes. When you are ready to proceed, click **Next**.

Step 16 The Completed page appears. This page is the final one in the process. Click **Finish.**

Stop. You have completed this procedure.

NTP-A154 Convert a 1+1 Point-to-Point to a Linear ADM Manually

Purpose	This procedure upgrades a 1+1 point-to-point configuration (two nodes) to a linear ADM configuration (three or more nodes) manually, that is, without using the in-service topology upgrade wizard. Use this procedure if the wizard is unavailable or if you need to back out of the wizard.
Tools/Equipment	None
Prerequisite Procedures	NTP-A124 Provision a Point-to-Point Network, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution This procedure is service-affecting.

Note Optical transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in Table 2-5 on page 2-20.

Note In a point-to-point configuration, two OC-N cards are connected to two OC-N cards on a second node. The working OC-N ports have data communications channel (DCC) terminations, and the OC-N cards are in a 1+1 protection group.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at one of the two point-to-point nodes. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63.

Step 3 Log into the node that will be added to the point-to-point configuration (the new node).

Note If you are attempting to add an unreachable node you must first log in to the unreachable node using a separate CTC session and configure that node. Delete any existing protection groups as described in the "DLP-A155 Delete a Protection Group" task on page 18-23. Delete any existing DCC terminations as described in the "DLP-A156 Delete a Section DCC Termination" task on page 18-24 or the "DLP-A359 Delete a Line DCC Termination" task on page 20-45.

Step 4 Complete the "NTP-A323 Verify Card Installation" procedure on page 4-2 to ensure that the new node has two OC-N cards with the same rate as the point-to-point nodes.

Step 5 Complete the "NTP-A35 Verify Node Turn-Up" procedure on page 5-2 for the new node.

Step 6 Physically connect the fibers between the point-to-point node and the new node. The fiber connections should be connected from working card to working card and protect card to protect card.

Step 7 On the new node, create a 1+1 protection group for the OC-N cards in the point-to-point node that will connect to the point-to-point node. See the "DLP-A73 Create a 1+1 Protection Group" task on page 17-76.

Step 8 Complete the "DLP-A377 Provision Section DCC Terminations" task on page 20-69 for the working OC-N cards in the new node that will connect to the linear ADM network. Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-A378 Provision Line DCC Terminations" task on page 20-71.

Note DCC failure alarms appear until you create DCC terminations in the point-to-point node during Step 9.

Step 9 In node view, display the point-to-point node that will connect to the new node.

Step 10 Complete the "NTP-A323 Verify Card Installation" procedure on page 4-2 to ensure that the point-to-point node has OC-N cards installed that can connect to the new node.

Step 11 Create a 1+1 protection group for the OC-N cards that will connect to the new node. See the "DLP-A73 Create a 1+1 Protection Group" task on page 17-76 for instructions.

Step 12 Create DCC terminations on the working OC-N card that will connect to the new node. See the "DLP-A377 Provision Section DCC Terminations" task on page 20-69.

Step 13 From the View menu, choose **Go to Node View** to open the new node in node view.

Step 14 Complete the "NTP-A28 Set Up Timing" procedure on page 4-13 for the new node. If the new node is using line timing, make the working OC-N card the timing source.

Step 15 From the View menu, choose **Go to Network View**. Verify that the newly created linear ADM configuration is correct. One green span line should appear between each linear node.

Step 16 Click the **Alarms** tab.

- **a.** Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.
- **b.** Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 17 Repeat the procedure to add an additional node to the linear ADM.

Stop. You have completed this procedure.

NTP-A303 Convert an Unprotected Point-to-Point or 1+1 Linear ADM to a Two-Fiber BLSR Automatically

Purpose	This procedure converts an unprotected point-to-point (two nodes) or linear ADM (three or more nodes) to a two-fiber bidirectional line switched ring (BLSR) without disrupting traffic.
Tools/Equipment	None
Prerequisite Procedures	NTP-A44 Provision Path Protection Nodes, page 5-20
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Before beginning this procedure, you should have a unique ring name to identify the new BLSR and a unique node ID number for each node in the ring.

Note Before beginning this procedure, optical transmit and receive levels should be in their acceptable range as shown in Table 2-5 on page 2-20.

Note If overhead circuits exist on the network, this procedure is service affecting. The overhead circuits will drop traffic and have a status of PARTIAL after the upgrade is complete.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node on the point-to-point or linear ADM. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63.

Step 3 Complete the "DLP-A155 Delete a Protection Group" task on page 18-23 at the nodes that support the point-to-point or linear ADM span to remove any protection groups that may exist.

Step 4 Complete the "DLP-A377 Provision Section DCC Terminations" task on page 20-69 at the nodes that support the point-to-point or linear ADM span. Provision the slot in each node that is not already in the SDCC Terminations list.

Step 5 From the Tools menu, choose **Topology Upgrade > Convert Path Protection to BLSR.** In the Topology Conversion dialog box, set the BLSR properties:

- Ring Type—(Display only.) The default is two-fiber.
- Speed—Choose the BLSR ring speed: OC-12, OC-48, or OC-192. The speed must match the OC-N speed of the BLSR trunk (span) cards.

Note If you are creating an OC-12 BLSR and will eventually upgrade it to OC-48 or OC-192, use the single-port OC-12 cards (OC12 IR/STM4 SH 1310, OC12 LR/STM4 SH 1310, or OC12 LR/STM4 LH 1550).

- Ring Name—Assign a ring name. The name can be from 1 to 6 characters in length. Any alphanumeric string is permissible, and upper and lower case letters can be combined. Do not use the character string "All" in either upper or lower case letters. This is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.
- Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path following a ring switch. The default is 5 minutes. Ring reversions can be set to Never.

Step 6 Click **Next**. If the network graphic appears, go to Step 7.

If CTC determines that a BLSR cannot be created, for example, not enough optical cards are installed or it finds circuits with path protection selectors, a "Cannot Create BLSR" message appears. If this occurs, complete the following steps:

a. Click **OK**.

b. In the Create BLSR window, click **Excluded Nodes**. Review the information explaining why the BLSR could not be created, then click **OK**.

c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.

d. Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 5-10, making sure all steps are completed accurately, then start this procedure again.

Step 7 In the network graphic, double-click a BLSR span line. If the span line is DCC connected to other BLSR cards that constitute a complete ring, the lines turn blue. If the lines do not form a complete ring, double-click span lines until a complete ring is formed. Click **Next.**

Step 8 The Path Protection to BLSR Topology Conversion dialog box appears. The dialog box states that the system is about to force traffic to the shortest path protection paths. Click **Next**.

Step 9 Another dialog box appears, stating that the force has been applied to the shortest path protection path. Click **Finish**.

If the BLSR window appears with the BLSR you created, go to the next step. If a "Cannot Create BLSR" or "Error While Creating BLSR" message appears:

a. Click **OK**.

b. In the Create BLSR window, click **Excluded Nodes**. Review the information explaining why the BLSR could not be created, then click **OK**.

c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.

d. Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 5-10, making sure all steps are completed accurately, then start this procedure again.

Note Some or all of the following alarms might briefly appear during BLSR setup: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, and BLSROSYNC.

Step 10 Verify the following:

- On the network view graphic, a green span line appears between all BLSR nodes.
- All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, and BLSROSYNC alarms are cleared. See the *Cisco ONS 15454 Troubleshooting Guide* for alarm troubleshooting.

Note The numbers in parentheses after the node name are the BLSR node IDs assigned by CTC. Every ONS 15454 in a BLSR is given a unique node ID, 0 through 31. To change it, complete the "DLP-A326 Change a BLSR Node ID" task on page 20-16.

Stop. You have completed this procedure.

NTP-A155 Convert a 1+1 Point-to-Point or a Linear ADM to a Two-Fiber BLSR Manually

Purpose	This procedure upgrades a 1+1 point-to-point configuration (two nodes) or a linear ADM configuration (three or more nodes) to a two-fiber BLSR manually, that is, without using the in-service topology upgrade wizard. Use this procedure if the wizard is unavailable or if you need to back out of the wizard.
Tools/Equipment	None
Prerequisite Procedures	NTP-A124 Provision a Point-to-Point Network, page 5-3 or NTP-A38 Provision a Linear ADM Network, page 5-6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note Optical transmit and receive levels should be in their acceptable range as shown in Table 2-5 on page 2-20.

Caution Traffic is not protected during this procedure.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at one of the nodes that you want to convert from a point-to-point or ADM to a BLSR. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5 for each node in the configuration.

Step 3 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63.

Step 4 On the network map, right-click a span adjacent to the node you are logged into. A shortcut menu appears.

Step 5 From the shortcut menu, click **Circuits**. The Circuits on Span window appears.

Step 6 Verify that the total number of active STS circuits does not exceed 50 percent of the span bandwidth. In the Circuits column there is a block titled "Unused." This number should exceed 50 percent of the span bandwidth.

If the span is an OC-48, no more than 24 STSs can be provisioned on the span. If the span is an OC-192, no more than 96 STSs can be provisioned on the span. If the span is an OC-12, no more than 6 STSs can be provisioned on the span.

Caution If the upper STSs are in use, this procedure cannot be completed. Bandwidth must be 50 percent unassigned to convert to a BLSR. Refer to local procedures for relocating circuits if these requirements are not met.

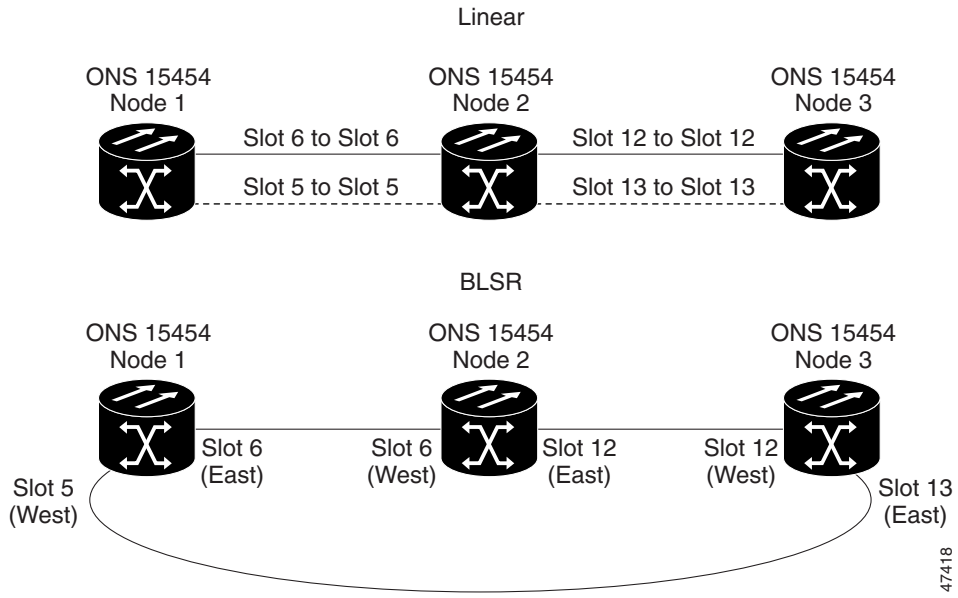
Step 7 Repeat Steps 4 through 6 for each node in the point-to-point or linear ADM that you will convert to a BLSR. When all nodes comply with Step 6, proceed to the next step.

Step 8 For every node in the point-to-point or linear ADM network that you want to convert to a BLSR, complete the following tasks:

- **a.** Complete the "DLP-A189 Verify that a 1+1 Working Slot is Active" task on page 18-58 for every 1+1 protection group that supports a span in the point-to-point or linear ADM network.
- **b.** Complete the "DLP-A155 Delete a Protection Group" task on page 18-23 at each port that supports the point-to-point or linear ADM span.
- **c.** Complete the "DLP-A214 Change the Service State for a Port" task on page 19-9 to put the protect ports out of service at each node that supports the point-to-point or linear ADM span.

Step 9 (Linear ADM only.) Physically remove the protect fibers from all nodes in the linear ADM; for example, the fiber running from Node 2/Slot 13 to Node 3/Slot 13 (as shown in Figure 13-3) can be removed.

Figure 13-3 Linear ADM to BLSR Conversion



Step 10 Create the ring by connecting the protect fiber from one end node to the protect port on the other end node. For example, the fiber between Node 1/Slot 5 and Node 2/Slot 5 (as shown in Figure 13-3) can be rerouted to connect Node 1/Slot 5 to Node 3/Slot 13.

Note If you need to remove any OC-N cards from the shelf, do so now. In this example, cards in Node 2/Slots 5 and 13 can be removed. See the "NTP-A116 Remove and Replace a Card" procedure on page 2-23.

Step 11 From the network view, click the **Circuits** tab and complete the "DLP-A532 Export CTC Data" task on page 22-34 to save the circuit data to a file on your hard drive.

Step 12 Complete the "DLP-A377 Provision Section DCC Terminations" task on page 20-69 at the end nodes. Provision the slot in each node that is not already in the SDCC Terminations list (in the Figure 13-3 example, Port 1 of Node 1/Slot 5 and Port 1 of Node 3/Slot 13).

Step 13 For circuits provisioned on an STS that is now part of the protection bandwidth (STSs 7 to 12 for an OC-12 BLSR, STSs 25 to 48 for an OC-48 BLSR, and STSs 97 to 192 for an OC-192 BLSR), delete and recreate each circuit:

a. Complete the "DLP-A333 Delete Circuits" task on page 20-21 for one circuit.

b. Create the circuit on STSs 1 to 6 for an OC-12 BLSR, STSs 1 to 24 for an OC-48 BLSR, or STSs 1 to 96 for an OC-192 BLSR on the fiber that served as the protect fiber in the linear ADM. See the "NTP-A344 Create a Manually Routed Optical Circuit" procedure on page 6-45 for instructions.

c. Repeat Steps a and b for each circuit residing on a BLSR protect STS.

Step 14 Complete the "NTP-A126 Create a BLSR" procedure on page 5-12 to put the nodes into a BLSR.

Stop. You have completed this procedure.

NTP-A342 Convert a Point-to-Point or Linear ADM to a Path Protection Configuration Automatically

Purpose	This procedure upgrades a point-to-point or linear ADM to a path protection configuration without disrupting traffic. You can upgrade STS, VT, and VT tunnel circuits to path protection. This option is a single circuit operation.
Tools/Equipment	None
Prerequisite Procedures	NTP-A124 Provision a Point-to-Point Network, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note When upgrading VT tunnels, CTC does not convert the VT tunnel to path protection, but instead creates a secondary tunnel for the alternate path. The result is two unprotected VT tunnels using alternate paths.

Note If overhead circuits exist on the network, this procedure is service affecting. The overhead circuits will drop traffic and have a status of PARTIAL after the upgrade is complete.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node on the point-to-point or linear ADM. If you are already logged in, continue with Step 2.

Step 2 If the point-to-point or linear ADM is 1+1 protected, complete the "DLP-A155 Delete a Protection Group" task on page 18-23. If the point-to-point or linear ADM is unprotected, continue with Step 4.

Step 3 Complete the "DLP-A377 Provision Section DCC Terminations" task on page 20-69 at the protect cards in all nodes that will be part of the path protection configuration. Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-A378 Provision Line DCC Terminations" task on page 20-71.

Step 4 From either network or node view, click the **Circuits** tab. Click the circuit you want to upgrade to select it.

Step 5 From the Tools menu, choose **Topology Upgrade > Convert Unprotected to Path Protection**.

Step 6 To set the path protection parameters, complete the "DLP-A218 Provision Path Protection Selectors" task on page 19-12.

Note When upgrading point-to-point or linear ADM circuits to a path protection topology, a traffic hit of greater than 300ms occurs if the "Provision working go & return on primary path" routing option is not checked in the Circuit Attributes pane.

Step 7 Click **Next**.

Step 8 Complete one of the following tasks:

a. To route the new path protection circuit manually, complete "DLP-A397 Manually Route a Path Protection Circuit for a Topology Upgrade" task on page 20-106.

b. To route the new path protection circuit automatically, complete "DLP-A398 Automatically Route a Path Protection Circuit for a Topology Upgrade" task on page 20-107.

Stop. You have completed this procedure.

NTP-A156 Convert a Point-to-Point or Linear ADM to a Path Protection Configuration Manually

Purpose	This procedure upgrades a point-to-point system to a path protection configuration manually, that is, without using the in-service topology upgrade wizard. Use this procedure if the wizard is unavailable or if you need to back out of the wizard.
Tools/Equipment	None
Prerequisite Procedures	NTP-A124 Provision a Point-to-Point Network, page 5-3 or NTP-A38 Provision a Linear ADM Network, page 5-6
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution This procedure is service affecting. All circuits are deleted and reprovisioned.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node on the point-to-point or linear ADM. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63.

Step 3 Complete the "DLP-A189 Verify that a 1+1 Working Slot is Active" task on page 18-58 for each node.

Step 4 Complete the "DLP-A155 Delete a Protection Group" task on page 18-23 for each 1+1 protection group that supports the point-to-point or linear ADM span.

Step 5 Complete the "DLP-A377 Provision Section DCC Terminations" task on page 20-69 at the protect cards in all nodes that will be part of the path protection configuration. Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-A378 Provision Line DCC Terminations" task on page 20-71.

Step 6 Complete the "DLP-A333 Delete Circuits" task on page 20-21 and the "NTP-A343 Create an Automatically Routed Optical Circuit" procedure on page 6-40 to delete and recreate the circuits one at a time.

Note A path protection configuration is the default configuration if the cards installed are installed and the DCCs are configured.

Stop. You have completed this procedure.

NTP-A267 Convert a Path Protection Configuration to a Two-Fiber BLSR Automatically

Purpose	This procedure converts a path protection configuration to a two-fiber BLSR without disrupting traffic.
Tools/Equipment	None
Prerequisite Procedures	NTP-A44 Provision Path Protection Nodes, page 5-20
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Open-ended path protection and path protection dual-ring interconnect (DRI) configurations do not support in-service topology upgrades.

Note Before beginning this procedure, you should have a unique ring name to identify the new BLSR and a unique node ID number for each node on the ring.

Note Before beginning this procedure, optical transmit and receive levels should be in their acceptable range as shown in Table 2-5 on page 2-20.

Note If overhead circuits exist on the network, this procedure is service affecting. The overhead circuits will drop traffic and have a status of PARTIAL after the upgrade is complete.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node on the path protection configuration. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63.

Step 3 In the Path Protection to BLSR Topology Conversion dialog box, set the BLSR properties:

- Ring Type—(Display only.) The default is two-fiber.
- Speed—Choose the BLSR ring speed: OC-12, OC-48, or OC-192. The speed must match the OC-N speed of the BLSR trunk (span) cards.

Note If you are creating an OC-12 BLSR and will eventually upgrade it to OC-48 or OC-192, use the single-port OC-12 cards (OC12 IR/STM4 SH 1310, OC12 LR/STM4 SH 1310, or OC12 LR/STM4 LH 1550).

- Ring Name—Assign a ring name. The name can be from 1 to 6 characters in length. Any alphanumeric string is permissible, and upper and lower case letters can be combined. Do not use the character string "All" in either upper or lower case letters. This is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.
- Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path following a ring switch. The default is 5 minutes. Ring reversions can be set to Never.

Step 4 Click **Next**. If the network graphic appears, go to Step 5.

If CTC determines that a BLSR cannot be created, for example, if not enough optical cards are installed or if it finds circuits with path protection selectors, a "Cannot Create BLSR" message appears. If this occurs, complete the following steps:

a. Click **OK**.

b. In the Create BLSR window, click **Excluded Nodes**. Review the information explaining why the BLSR could not be created, then click **OK**.

c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.

d. Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 5-10, making sure all steps are completed accurately, then start this procedure again.

Step 5 In the network graphic, double-click a BLSR span line. If the span line is DCC connected to other BLSR cards that constitute a complete ring, the lines turn blue. If the lines do not form a complete ring, double-click span lines until a complete ring is formed. Click **Next**.

Step 6 The Path Protection to BLSR Topology Conversion dialog box appears. The dialog box states that the system is about to force traffic to the shortest path protection paths. Click **Next**.

Step 7 Another dialog box appears, stating that the force has been applied to the shortest path protection path. Click **Finish.**

If the BLSR window appears with the BLSR you created, go to Step 8. If a "Cannot Create BLSR" or "Error While Creating BLSR" message appears, complete the following:

a. Click **OK**.

b. In the Create BLSR window, click **Excluded Nodes**. Review the information explaining why the BLSR could not be created, then click **OK**.

c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.

d. Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 5-10, making sure all steps are completed accurately, then start this procedure again.

Note Some or all of the following alarms might briefly appear during BLSR setup: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, and BLSROSYNC.

Step 8 Verify the following:

- On the network view graphic, a green span line appears between all BLSR nodes.
- All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, and BLSROSYNC alarms are cleared. See the *Cisco ONS 15454 Troubleshooting Guide* for alarm troubleshooting.

Note The numbers in parentheses after the node name are the BLSR node IDs assigned by CTC. Every ONS 15454 in a BLSR is given a unique node ID, 0 through 31. To change it, complete the "DLP-A326 Change a BLSR Node ID" task on page 20-16.

Stop. You have completed this procedure.

NTP-A210 Convert a Path Protection Configuration to a Two-Fiber BLSR Manually

Purpose	This procedure converts a path protection to a two-fiber BLSR manually, that is, without using the in-service topology upgrade wizard. Use this procedure if the wizard is unavailable or if you need to back out of the wizard.
Tools/Equipment	None
Prerequisite Procedures	NTP-A44 Provision Path Protection Nodes, page 5-20
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution This procedure is service affecting. All circuits in the ring are deleted and reprovisioned.

Caution Read through this procedure completely before beginning the conversion.

Note Prior to beginning this procedure, you should have a unique ring name to identify the new BLSR and a unique node ID number for each node on the ring.

Note Prior to beginning this procedure, optical transmit and receive levels should be in their acceptable range as shown in Table 2-5 on page 2-20.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node on the path protection configuration. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63.

Step 3 On the network map, right-click a span adjacent to the node you are logged into. A shortcut menu appears.

Step 4 From the shortcut menu, click **Circuits**. The Circuits on Span window appears.

Step 5 Verify that the total number of active STS circuits does not exceed 50 percent of the span bandwidth. In the Circuits column there is a block titled "Unused." This number should exceed 50 percent of the span bandwidth.

If the span is an OC-48, no more than 24 STSs can be provisioned on the span. If the span is an OC-192, no more than 96 STSs can be provisioned on the span. If the span is an OC-12, no more than 6 STSs can be provisioned on the span.

Caution If the first half of the capacity is exceeded, this procedure cannot be completed. Bandwidth must be 50 percent unassigned to convert to BLSR. Refer to local procedures for relocating circuits if these requirements are not met.

Step 6 Repeat Steps 1 through 5 for each node in the path protection configuration that you will convert to a BLSR. When all nodes comply with Step 5, continue with the next step.

Step 7 Save all circuit information:

a. In network view, click the **Circuits** tab.

b. Record the circuit information using one of the following options:

- From the File menu, click **Print** to print the circuits table. See the "DLP-A531 Print CTC Data" task on page 22-32 for more information.
- From the File menu, click **Export** and choose the data format: HTML, CSV (comma separated values), or TSV (tab separated values). Click **OK** and save the file in a temporary directory. See the "DLP-A532 Export CTC Data" task on page 22-34 for more information.

Step 8 Delete the circuits:

a. In network view, click the **Circuits** tab. All circuits on the ring appear.

b. With the **Ctrl** key pressed, click each circuit. Each line turns dark blue as it is selected.

c. After all circuits have been selected, click **Delete**. Allow several minutes for processing; the actual length of time depends on the number of circuits in the network.

Step 9 Complete the "NTP-A126 Create a BLSR" procedure on page 5-12 to create the BLSR.

Step 10 To recreate the circuits, see Chapter 6, "Create Circuits and VT Tunnels." and choose the applicable procedure for the circuit type you want to enter.

Note To add additional nodes to a BLSR, see the "NTP-A350 Add a BLSR Node" procedure on page 14-2.

Stop. You have completed this procedure.

NTP-A374 Convert a BLSR to Path Protection Manually

Purpose	This procedure converts BLSR to Path Protection manually.
Tools/Equipment	None
Prerequisite Procedures	NTP-A40 Provision BLSR Nodes, page 5-10
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You cannot convert a BLSR to Path Protection automatically or by using the in-service topology upgrade wizard.

Caution This procedure is service affecting. All circuits on the ring are deleted and reprovisioned.

Caution Read through this procedure completely before beginning the conversion.

Note Prior to beginning this procedure, you should have a unique ring ID name to identify the new Path Protection Node and a unique node ID number for each node on the ring.

Note Prior to beginning this procedure, optical transmit and receive levels should be in their acceptable range as shown in Table 2-5 on page 2-20.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node on the Path Protection. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63 task on page 19-62.

Step 3 Repeat Steps 1 and 2 for each node in the BLSR that you will convert to Path Protection.

Step 4 Save all circuit information:

a. In network view, click the **Circuits** tab.

b. Record the circuit information using one of the following options:

- From the File menu, click **Print** to print the circuits table. See the "DLP-A531 Print CTC Data" task on page 22-32 task on page 22-30.

- From the File menu, click **Export** and choose the data format: HTML, CSV (comma separated values), or TSV (tab separated values). Click **OK** and save the file in a temporary directory. See the "DLP-A532 Export CTC Data" task on page 22-34.

Step 5 Convert the BLSR.

a. From the View menu, choose **Go to Network View**. Click the **Provisioning > BLSR** tabs.

b. With the **Ctrl** key pressed, select all the BLSR that you want to convert and click **Delete**. In the confirmation dialog box that appears, click **Yes**.

Note If an error message is displayed, rectify the error and then delete the BLSR. For more information, refer to *Cisco ONS 15454 Troubleshooting Guide*.

c. As needed, perform one of the following steps to upgrade the circuit to Path Protection:

- Complete the "NTP-A342 Convert a Point-to-Point or Linear ADM to a Path Protection Configuration Automatically" task on page 13-11.
- Complete the "NTP-A156 Convert a Point-to-Point or Linear ADM to a Path Protection Configuration Manually" task on page 13-12.

Stop. You have completed this procedure.

NTP-A211 Convert a Two-Fiber BLSR to a Four-Fiber BLSR Automatically

Purpose	This procedure upgrades a two-fiber BLSR to a four-fiber BLSR without disrupting traffic. The conversion will be easier if the same east and west configuration is used on all nodes being upgraded.
Tools/Equipment	None
Prerequisite Procedures	NTP-A126 Create a BLSR, page 5-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note BLSR DRI configurations do not support in-service topology upgrades.

Note Two-fiber OC-48 or OC-192 BLSRs can be converted to four-fiber BLSRs. To convert, install two additional OC-48 or OC-192 cards at each two-fiber BLSR node, then log into CTC and convert the BLSR from two-fiber to four-fiber. The fibers that were divided into working and protect bandwidths for the two-fiber BLSR are now fully allocated for working BLSR traffic. A span upgrade can be performed before the two-fiber to four-fiber BLSR conversion.

Note BLSR protection channel access (PCA) circuits, if present, will remain in their existing STSs. Therefore, they will be located on the working path of the four-fiber BLSR and will have full BLSR protection. To route PCA circuits on protection channels in the four-fiber BLSR, delete and recreate the circuits after the upgrade. For example, if you upgrade a two-fiber OC-48 BLSR to four-fiber, PCA circuits on the protection STSs (STSs 25 to 48) in the two-fiber BLSR will remain in their existing STSs, which are working STSs in the four-fiber BLSR. Deleting and recreating the OC-48 PCA circuits moves the circuits to STSs 1 to 24 in the protect bandwidth of the four-fiber BLSR. To delete circuits, see the "DLP-A333 Delete Circuits" task on page 20-21. To create circuits, see Chapter 6, "Create Circuits and VT Tunnels."

Note Before beginning this procedure, optical transmit and receive levels should be in their acceptable range as shown in Table 2-5 on page 2-20.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at one of the two-fiber nodes that you want to convert.

Step 2 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63.

Step 3 Complete the "NTP-A16 Install Optical Cards and Connectors" procedure on page 2-8 to install two OC-48 or OC-192 cards at each BLSR node. You must install the same OC-N card rate as the two-fiber BLSR.

Step 4 Connect the fiber to the new cards. Use the same east-west connection scheme that was used to create the two-fiber connections. See the "NTP-A247 Install Fiber-Optic Cables" procedure on page 2-19.

Step 5 Complete the "DLP-A214 Change the Service State for a Port" task on page 19-9 to put the ports in service for each new OC-N card.

Step 6 Test the new fiber connections using procedures standard for your site.

Step 7 Convert the BLSR:

a. Display the network view and click the **Provisioning > BLSR** tabs.

b. Choose the two-fiber BLSR you want to convert then click the **Upgrade to 4 Fiber** button.

c. In the Upgrade BLSR dialog box, set the amount of time that will pass before the traffic reverts to the original working path after the condition that caused the switch has been resolved. The default is 5 minutes.

d. Click **Next**.

e. Assign the east and west protection ports:

- West Protect—Select the west BLSR port that will connect to the west protect fiber from the drop-down list.
- East Protect—Select the east BLSR port that will connect to the east protect fiber from the drop-down list.

f. Click **Finish**.

Step 8 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 9 Complete the "NTP-A176 Four-Fiber BLSR Acceptance Test" procedure on page 5-15.

Stop. You have completed this procedure.

NTP-A159 Modify a BLSR

Purpose	This procedure changes a BLSR ring name, node ID, or ring and span reversion times.
Tools/Equipment	None
Prerequisite Procedures	NTP-A126 Create a BLSR, page 5-12
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node in the BLSR you want to modify. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63.

Note Some or all of the following alarms appear during BLSR setup: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, and BLSROSYNC. The alarms clear after you configure all the nodes in the BLSR. For definitions of these alarms, see the *Cisco ONS 15454 Troubleshooting Guide*.

Step 3 To change the BLSR ring name or the ring or span reversion times, complete the following steps. If you want to change a node ID, continue with Step 4.

a. In network view, click the **Provisioning > BLSR** tabs.

b. Click the BLSR you want to modify and click **Edit**.

c. In the BLSR window, change any of the following:

- Ring Name—Assign a ring name. The name can be from 1 to 6 characters in length. The alphanumeric character strings that can be used are 0 to 9 and A to Z. You can combine numbers and letters and use upper or lower case letters. Do not use the character string "All" in either upper or lower case letters because it is a TL1 keyword. Do not choose a name that is already assigned to another BLSR.
- Reversion time—If needed, change the amount of time that will pass before the traffic reverts to the original working path after a ring switch.
- Span Reversion—(Four-fiber BLSRs only.) If needed, change the amount of time that will pass before the traffic reverts to the original working path after a span switch.

d. Click **Apply**.

e. If you changed the ring name, the BLSR window closes automatically. If you only changed a reversion time, close the window by choosing **Close** from the File menu.

Step 4 As needed complete the "DLP-A326 Change a BLSR Node ID" task on page 20-16; otherwise, continue with Step 5.

Step 5 In network view, verify the following:

- A green span line appears between all BLSR nodes.
- All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, BLSROSYNC, and Node ID Mismatch alarms are cleared.

Note For definitions of these alarms, see the *Cisco ONS 15454 Troubleshooting Guide*.

Stop. You have completed this procedure.

NTP-A376 Upgrading a BLSR Ring Using an MRC-12 Card

Purpose	This procedure upgrades a BLSR ring by changing the SFP of the MRC-12 card.
Tools/Equipment	None
Prerequisite Procedures	"DLP-A60 Log into CTC" task on page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A303 Initiate a BLSR Force Ring Switch" task on page 20-3 to perform a force switch on both the endpoint nodes of the span to be upgraded.

Step 2 Remove the fiber from both the endpoint nodes. Verify that traffic is still running on the circuit.

Step 3 Remove the existing lower rate SFPs and install higher rate SFPs in Port 1 of the MRC-12 card of both the endpoint nodes.

Step 4 In the shelf view of each endpoint node , double-click the MRC-12 card where you want to provision the port settings.

Step 5 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 6 In the Pluggable Port Modules area, select Port 1-1 and click **Edit**.

Step 7 Select OC-*n* (higher rate) as the new port rate.

Step 8 Click **OK**.

The new OC-*n* pluggables may require power normalization.

Step 9 Click the **Provisioning > Optics Thresholds** tabs.

Step 10 Click **Set** in the Set OPR column.

Step 11 Test the optical transmit and receive levels of the cards installed using an optical power meter.

Refer to Table 2-5 for OC-N card transmit and receive levels. If the receive level falls outside the acceptable range for that card, attenuate accordingly. This can also be checked on the MRC-12 card by changing to the card view of the MRC-12 card and clicking the **Maintenance > Transceiver** tabs. OPT is the TX power and OPR is the RX power.

Step 12 Complete the "DLP-A44 Install Fiber-Optic Cables for BLSR Configurations" task on page 17-46 to attach the fiber to the cards.

Wait for the IMPROPRMVL alarm to clear and the cards to become active.

Step 13 Complete the "DLP-A194 Clear a BLSR Force Ring Switch" task on page 18-65 to remove the forced switch from both the endpoint nodes of the upgraded span after the cards in the nodes have upgraded successfully and the alarms have cleared.

Step 14 Complete the "DLP-A217 BLSR Exercise Ring Test" task on page 19-10 to perform the exercise ring test to check the BLSR ring functionality without switching traffic

Step 15 Repeat this procedure for each span in the BLSR.

Stop. You have completed this procedure.

CHAPTER 14

Add and Remove Nodes

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter explains how to add and remove Cisco ONS 15454 nodes from bidirectional line switched rings (BLSRs), path protection configurations, and linear add-drop multiplexer (ADM) networks.

Before You Begin

Before performing any of the following procedures, complete the "NTP-A195 Document Card, Node, and Network Provisioning" procedure on page 8-2. Also investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A350 Add a BLSR Node, page 14-2—Complete as needed.
2. NTP-A240 Remove a BLSR Node, page 14-7—Complete as needed.
3. NTP-A351 Add a Path Protection Node, page 14-10—Complete as needed.
4. NTP-A294 Remove a Path Protection Node, page 14-13—Complete as needed.
5. NTP-A262 Add a Node to a Linear ADM, page 14-14—Complete as needed to add a node to the end of a linear ADM. This procedure can be used to add a node between two linear ADM nodes, but requires that circuits be deleted and recreated. To add a node without disrupting traffic, use the following procedure.
6. NTP-A323 Add a Node to a Linear ADM Using the Wizard, page 14-16—Complete as needed to add a node between two linear ADM nodes.
7. NTP-A313 Remove an In-Service Node from a Linear ADM, page 14-18—Complete as needed to remove a node from a linear ADM without disrupting traffic.

NTP-A350 Add a BLSR Node

Purpose	This procedure expands a BLSR by adding a node. All nodes in the ring must be on the same software version.
Tools/Equipment	Fiber for new node connections
Prerequisite Procedures	Cards must be installed and node turn-up procedures completed on the node that will be added to the BLSR. See Chapter 2, "Install Cards and Fiber-Optic Cable," and Chapter 4, "Turn Up a Node."
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Adding a BLSR node can be service affecting and should be performed during a maintenance window.

Step 1 Check the software version on the node you are adding to the BLSR from the node view Maintenance > Software subtab. If it is not the same version as the nodes in the ring, you must upgrade or downgrade the new node to the same version as the other nodes in the ring. Refer to the release-specific software upgrade guide for more information on upgrading the ONS node software.

Step 2 Draw a diagram of the BLSR where you will add the node. In the diagram, identify the east and west BLSR OC-N trunk (span) cards that will connect to the new node. This information is essential to complete this procedure without error. Figure 14-1 shows a drawing of a three-node, two-fiber BLSR that uses Slots 5 and 12 for the BLSR trunk cards. The dashed arrow shows the new fiber connections that will be made to add the fourth node to the BLSR.

Figure 14-1 Three-Node, Two-Fiber BLSR Before a Fourth Node Is Added

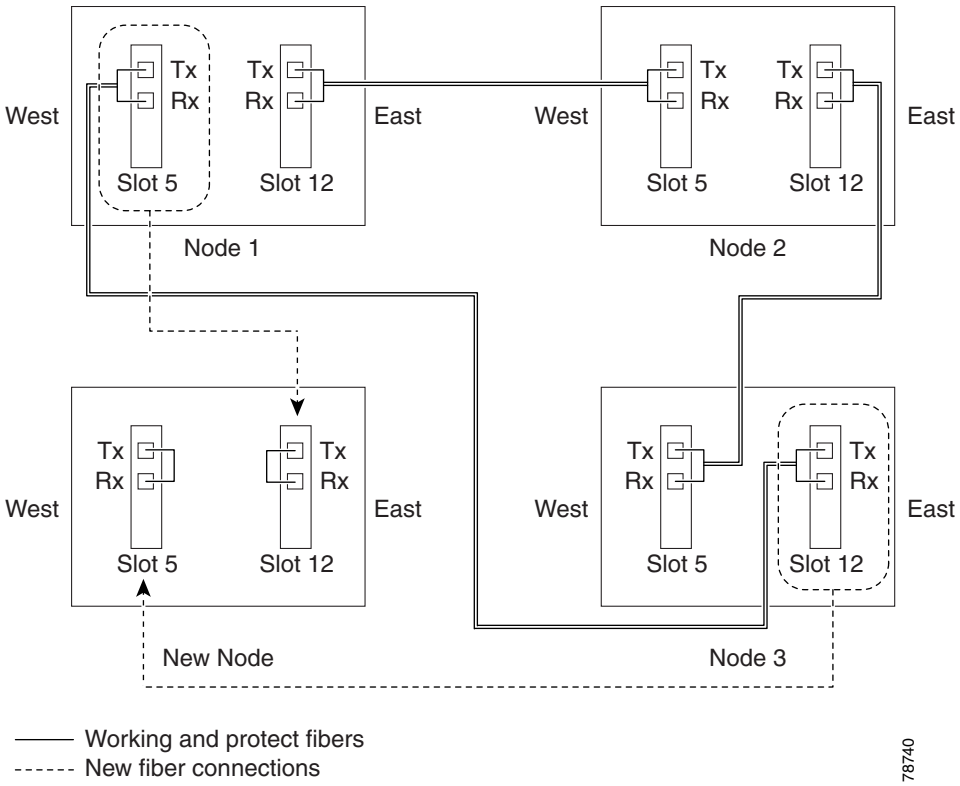
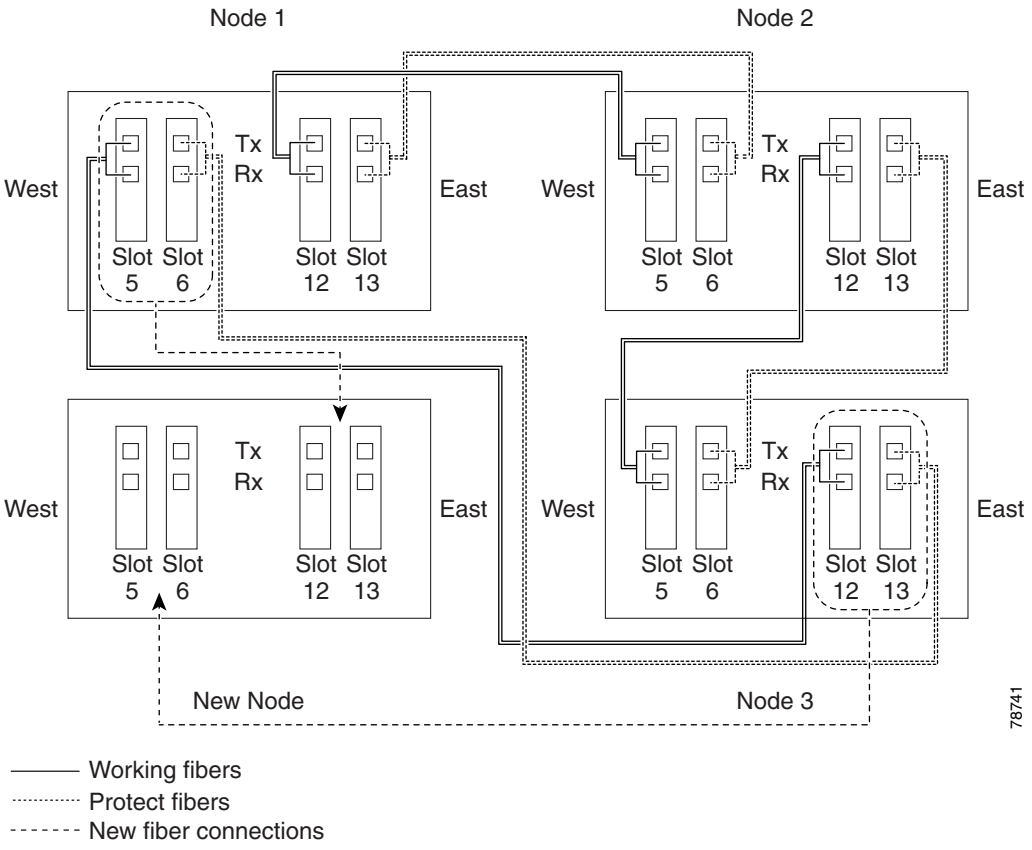


Figure 14-2 shows a sample drawing of a three-node, four-fiber BLSR. The dashed arrow shows the new fiber connections that will be made to add the fourth node. For four-fiber BLSRs, two fiber sets will be reconnected, the working fiber and the protect fiber.

Figure 14-2 Three-Node, Four-Fiber BLSR Before a Fourth Node is Added



Step 3 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5 for all the nodes in the ring.

Step 4 Verify the card installation on the new node using the "NTP-A323 Verify Card Installation" procedure on page 4-2. Verify that the OC-N cards that will be the BLSR trunk cards match the BLSR optical rate. For example, if the BLSR is OC-48, the new node must have OC-48 cards installed. If the OC-N cards are not installed or the optical rates do not match the BLSR, complete the "NTP-A16 Install Optical Cards and Connectors" procedure on page 2-8.

Step 5 Verify that fiber is available to connect the new node to the existing nodes. Refer to the diagram drawn in Step 2.

Step 6 Complete the "NTP-A35 Verify Node Turn-Up" procedure on page 5-2. In order to have CTC visibility to the new node after it is added, you must be an authorized user on the node and you must have IP connectivity to the node.

Step 7 Create a static route on the new node if the following conditions are present. If the conditions are not present, continue with Step 8.

- The IP address for the new node is on the same subnet as other nodes in the network.
- On the Provisioning > Network > General subtab, the Enable Socks Proxy on Port and External Network Element (ENE) options are not selected under Gateway Settings on the new node.
- A CTC computer is directly connected to the new node.
- CTC computers are directly connected to other nodes on the same subnet.

If these conditions are present, add static routes on the node that will be added to the BLSR, using the following settings:

- Destination IP address: *IP-address-of-the-CTC-computer-connected-to-the-new-node*
- Net Mask: **255.255.255.255**
- Next Hop: *IP-address-of-the-Cisco-ONS-15454*
- Cost: **1**

See the "DLP-A65 Create a Static Route" task on page 17-67. To view gateway settings, see the "DLP-A249 Provision IP Settings" task on page 19-30.

Step 8 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node in the BLSR.

Step 9 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63 to verify that the BLSR is free of major alarms or problems. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 8, "Manage Alarms" or, if necessary, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 10 From the View menu, choose **Go to Network View** and click the **Provisioning > BLSR** tabs.

Step 11 On paper, record the Ring Name, Ring Type, Line Rate, Ring Reversion, and Span Reversion (4 Fiber).

Step 12 From the Nodes column, record the Node IDs in the BLSR. The Node IDs are the numbers in parentheses next to the node name.

Step 13 Log into the new node:

- If the node has a LAN connection and appears on the network map, from the View menu, choose **Go to Other Node**, then enter the new node.
- If the new node is not connected to the network, log into it using the "DLP-A60 Log into CTC" task on page 17-60.

Step 14 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 15 Using the information recorded in Steps 11 and 12 and the diagram created in Step 2, create a BLSR on the new node. See the "DLP-A242 Create a BLSR on a Single Node" task on page 19-24.

Step 16 (Optional.) Create test circuits, making sure they pass through the BLSR trunk cards and run test traffic through the node to ensure the cards are functioning properly. See the "NTP-A344 Create a Manually Routed Optical Circuit" procedure on page 6-45 and the "NTP-A62 Test Optical Circuits" procedure on page 6-51 for information.

Step 17 Create the data communications channel (DCC) terminations on the new node. See the "DLP-A377 Provision Section DCC Terminations" task on page 20-69.

Note Creating the DCC terminations causes the SDCC Termination Failure and Loss of Signal alarms to appear. These alarms remains active until you connect the node to the BLSR.

Note If you map the K3 byte to another byte (such as E2), you must remap the line cards on either side of the new node to the same byte. See the "DLP-A89 Remap the K3 Byte" task on page 17-82.

Step 18 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a BLSR node that will connect to the new node.

Step 19 Referring to the diagram created in Step 2, complete the "DLP-A303 Initiate a BLSR Force Ring Switch" task on page 20-3 on the node that will connect to the new node on its west line (port). In the Figure 14-2 on page 14-4 example, the BLSR force ring would occur at Node 1, West line (Slot 5 and 6).

Step 20 Referring to the diagram created in Step 2, complete the "DLP-A303 Initiate a BLSR Force Ring Switch" task on page 20-3 on the node that will connect to the new node on its east line (port). In the Figure 14-2 on page 14-4 example, the BLSR force ring would occur at Node 3, East line (Slot 12 and 13).

Step 21 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 22 Following the diagram created in Step 2, remove the fiber connections from the two nodes that will connect to the new node.

a. Remove the west fiber from the node that will connect to the east port of the new node. In the Figure 14-1 on page 14-3 example, this is Node 1, Slot 5, and in Figure 14-2 on page 14-4 this is Node 1, Slots 5 and 6.

b. Remove the east fiber from the node that will connect to the west port of the new node. In the Figure 14-1 on page 14-3 example, this is Node 3, Slot 12, and in Figure 14-2 on page 14-4 this is Node 3, Slots 12 and 13.

Step 23 Connect fibers from the adjacent nodes to the new node following the diagram created in Step 2. Connect the west port to the east port and the east port to the west port. For four-fiber BLSRs, connect the protect fibers.

Step 24 After the newly added node appears in network view, double-click it to display the node in node view.

Step 25 Click the **Provisioning > BLSR** tabs.

Step 26 Click **Ring Map**. Verify that the new node appears on the Ring Map with the other BLSR nodes, then click **OK**.

Step 27 From the View menu, choose **Go to Network View** and check the following:

a. Click the **Provisioning > BLSR** tabs. Verify that the new node appears under the Node column.

b. Click the **Alarms** tab. Verify that BLSR alarms such as RING MISMATCH, E-W MISMATCH, PRC-DUPID (duplicate node ID), and APSCDFLTK (default K) do not appear.

If the new node does not appear in the Node column, or if BLSR alarms are present, log into the new node and verify that the BLSR is provisioned on it correctly with the information from Steps 11 and 12. If the node still does not appear, or if alarms persist, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 28 Click the **Circuits** tab. Wait until all the circuits are discovered. The circuits that pass through the new node will be shown as incomplete.

Note If the circuits take more than a minute to appear, log out of CTC, then log back in.

Step 29 In network view, right-click the new node and choose **Update Circuits With The New Node** from the shortcut menu. Verify that the number of updated circuits in the dialog box is correct.

Step 30 If incomplete circuits are still present, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 31 Click the **History** tab. Verify that BLSR_RESYNC conditions appear for every node in the BLSR.

Step 32 Complete the "DLP-A194 Clear a BLSR Force Ring Switch" task on page 18-65 to remove the ring switch from the east and west BLSR lines.

Step 33 According to local site practice, complete the "NTP-A175 Two-Fiber BLSR Acceptance Test" procedure on page 5-13 or the "NTP-A176 Four-Fiber BLSR Acceptance Test" procedure on page 5-15.

Stop. You have completed this procedure.

NTP-A240 Remove a BLSR Node

Purpose	This procedure removes a BLSR ring or multiple BLSR rings from a node.
Tools/Equipment	None
Prerequisite Procedures	NTP-A126 Create a BLSR, page 5-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution The following procedure minimizes traffic outages during node removals. You will delete all circuits that originate and terminate on the node that will be removed. In addition, you will verify that circuits passing through the node do not enter and exit the node on different STSs and/or VTs. If they do, you will delete and recreate the circuits, and traffic will be lost during this time.

Step 1 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5 for all the nodes in the ring.

Step 2 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node that you are going to remove from the BLSR.

Step 3 Complete the "DLP-A195 Verify Timing in a Reduced Ring" task on page 18-66.

Note If you remove a node that is the only building integrated timing supply (BITS) for the ring, you also remove the only source of synchronization for all the nodes in that ring. Circuits that leave the ring to connect to other networks synchronized to a Stratum 1 clock will experience a high level of pointer adjustments, which might adversely affect traffic performance.

Step 4 Create a diagram of the BLSR where you will remove the node. You can draw the BLSR manually, or print it from CTC by performing the following steps:

a. From the View menu, choose **Go to Network View**.

b. Click the **Provisioning** > **BLSR** tabs.

c. Choose the desired BLSR, then click **Edit**.

d. In the BLSR window, verify that all the port information is visible. If not, press **Ctrl** and drag the node icons to a new location so the information can be viewed.

e. Complete the "DLP-A531 Print CTC Data" task on page 22-32.

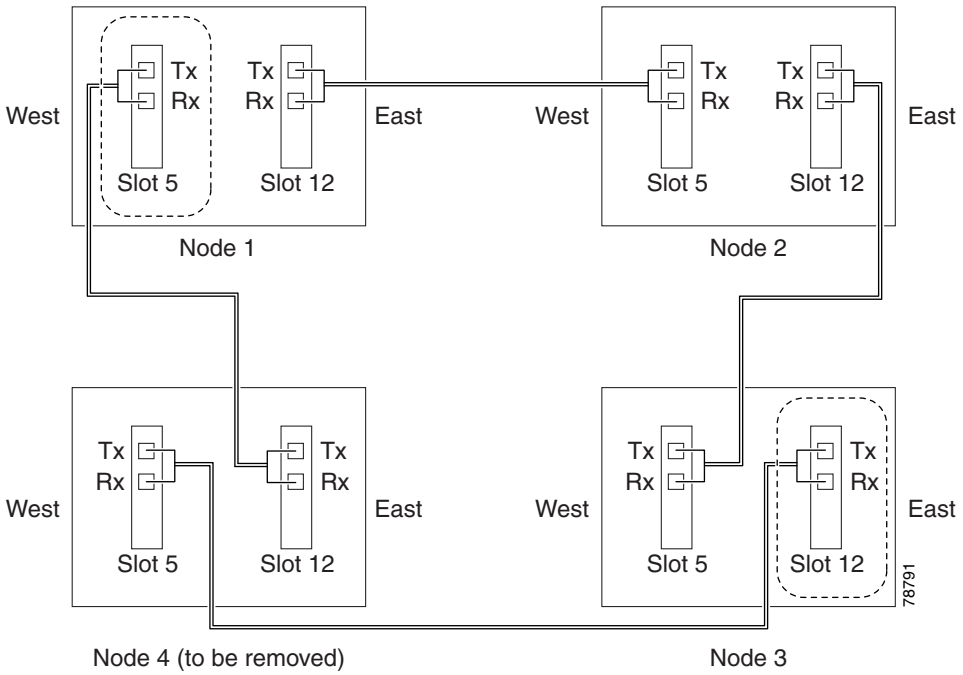
f. Close the BLSR window by choosing **Close** from the File menu.

Step 5 Referring to the BLSR diagram, identify the following:

- The node that is connected through its west port to the target (removal) node. For example, if you were removing Node 4 in Figure 14-3, Node 1 is the node connected through its west port to Node 4.
- The node that is connected through its east port to the target (removal) node. In Figure 14-3, Node 3 is the node connected through its east port to Node 4.

Write down the slot and port of the BLSR ring in the node.

Figure 14-3 Four-Node, Two-Fiber BLSR Before a Node Is Removed



Step 6 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63 to verify that the BLSR is free of alarms. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 8, "Manage Alarms" or, if necessary, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 7 From the View menu, choose **Go to Other Node**. Choose the node that you will remove and click **OK**.

Step 8 Click the **Circuits** tab. If the Scope setting is set to Network, choose **Node** from the Scope drop-down list. Make sure that the Filter button is off (not indented) to ensure that all circuits are visible.

Step 9 Delete all circuits that originate or terminate on the node. See the "DLP-A333 Delete Circuits" task on page 20-21.

Step 10 Complete the "DLP-A442 Verify Pass-Through Circuits" task on page 21-25 to verify that circuits passing through the target node enter and exit the node on the same STS and/or VT. K3 extension byte mapping is supported on all ONS 15600 OC-48 and OC-192 traffic cards, as well as the ONS 15454 OC-48 AS card.

Step 11 From the View menu, choose **Go to Network View**.

Step 12 Referring to the diagram created in Step 4, complete the "DLP-A303 Initiate a BLSR Force Ring Switch" task on page 20-3 at each node that connects to the target (removal) node to force traffic away from it. You must perform a Force switch at each port connected to the target node. For example, in Figure 14-3, you would perform a Force switch on the east port of Node 3 and the west port of Node 1.

Step 13 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 14 Remove the fiber connections between the node being removed and the two neighboring nodes.

Step 15 If the two nodes that will be connected after the BLSR node is removed have OC-48 AS trunk (span) cards and their K3 bytes were remapped, complete the "DLP-A422 Verify BLSR Extension Byte Mapping" task on page 21-7. If not, continue with Step 16.

Step 16 Reconnect the fiber of the two neighboring nodes directly, west port to east port. For example, in Figure 14-3, the east port of Node 3 (Slot 12) connects to the west port of Node 1 (Slot 5).

Step 17 Complete the following substeps:

a. From the View menu, choose **Go to Other Node**. Choose one of the newly connected nodes and click **OK**.

b. Click the **Provisioning > BLSR** tabs.

c. Choose the BLSR that originally contained the removed node, and then click **Ring Map**.

d. Wait until the removed node is no longer listed.

e. Repeat steps a through d for the other newly connected node in the BLSR.

Step 18 Complete the "DLP-A196 Delete a BLSR from a Single Node" task on page 18-67.

Step 19 Click the **History** tab. Verify that the BLSR_RESYNC condition appears for every node in the BLSR.

Step 20 Complete the "DLP-A194 Clear a BLSR Force Ring Switch" task on page 18-65 to remove the Force protection switches.

Step 21 According to local site practice, complete the "NTP-A175 Two-Fiber BLSR Acceptance Test" procedure on page 5-13.

Step 22 Complete the "DLP-A371 Remove Pass-through Connections" task on page 20-55.

Step 23 Log back into a node on the reduced ring. In the CTC Login dialog box, uncheck the **Disable Network Discovery** check box.

Note The deleted node will appear in network view until all SDCC terminations are deleted. To delete SDCC terminations, complete the "DLP-A156 Delete a Section DCC Termination" task on page 18-24.

Step 24 Click the **Circuits** tab and verify that no incomplete circuits are present. If incomplete circuits appear, repeat Steps 22 and 23.

Step 25 If you delete a node that was in a login node group, you will see incomplete circuits for that node in the CTC network view. Although it is no longer part of the ring, the removed node still reports to CTC until it is no longer in a login node group. If necessary, complete the "DLP-A372 Delete a Node from a Specified Login Node Group" task on page 20-56.

Step 26 To remove another node from a BLSR, repeat this procedure for the desired node.

Step 27 According to local site practice, complete the "NTP-A175 Two-Fiber BLSR Acceptance Test" procedure on page 5-13 or the "NTP-A176 Four-Fiber BLSR Acceptance Test" procedure on page 5-15.

Stop. You have completed this procedure.

NTP-A351 Add a Path Protection Node

Purpose	This procedure adds a node to a path protection configuration.
Tools/Equipment	None
Prerequisite Procedures	Cards must be installed and node turn-up procedures completed on the node that will be added to the path protection configuration. See Chapter 2, "Install Cards and Fiber-Optic Cable," and Chapter 4, "Turn Up a Node." NTP-A44 Provision Path Protection Nodes, page 5-20
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5 for all the nodes in the ring.

Step 2 Log into an existing node in the path protection configuration where you want to add a node. See the "DLP-A60 Log into CTC" task on page 17-60 for instructions. In order to have CTC visibility to the new node after it is added, you must be an authorized user on the node and you must have IP connectivity to the node.

Step 3 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63 to verify that the path protection configuration is free of major alarms or problems. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See the *Cisco ONS 15454 Troubleshooting Guide*, as necessary.

Step 4 Count the total number of circuits on the fiber that is cut between the existing nodes. To count the number of circuits, right click on the fiber that is cut, and click circuits.

Step 5 In network view, click the **Circuits** tab.

To view Partial circuits, click the Filter button and select **PARTIAL** from the **Status** drop-down list. The Partial circuits, if any, are displayed.

To view Partial_TL1 circuits, click the Filter button and select **PARTIAL_TL1** from the **Status** drop-down list. The Partial_TL1 circuits, if any, are displayed.

Resolve any partial circuits (both Partial and Partial_TL1) in the network before proceeding. However, if you want to continue with Step 6, match the number of partial circuits and circuit names that existed before and after adding a path protection node. This ensures that no additional partial circuits are created after this procedure is completed.

Step 6 Verify the card installation on the new node. See the "NTP-A323 Verify Card Installation" procedure on page 4-2. Check that the OC-N cards that will serve as the path protection trunk (span) cards match the path protection optical rate of the trunk cards to which the new node will be connected. For example, if the adjacent nodes have OC-48 trunk cards, the new node must have OC-48 cards installed. If the OC-N cards are not installed or the rate does not match the rate of the adjacent node trunk cards, complete the "NTP-A16 Install Optical Cards and Connectors" procedure on page 2-8 to install them.

Step 7 Verify that fiber is available to connect the new node to the existing nodes.

Step 8 Complete the "NTP-A35 Verify Node Turn-Up" procedure on page 5-2.

Step 9 Create a static route on the new node if the following conditions are present. If the conditions are not present, continue with Step 10.

- The IP address for the new node is on the same subnet as other nodes in the network.
- On the Provisioning > Network > General subtab, the Enable Socks Proxy on Port and External Network Element (ENE) options are not selected under Gateway Settings for the new node.
- A CTC computer is directly connected to the new node.
- CTC computers are directly connected to other nodes on the same subnet.

If these conditions are present, add static routes on the node that will be added to the path protection configuration, using the following settings:

- Destination IP address: *Local-PC-IP-address*
- Net Mask: **255.255.255.255**
- Next Hop: *IP-address-of-the-Cisco-ONS-15600-SDH*
- Cost: **1**

See the "DLP-A65 Create a Static Route" task on page 17-67. To view gateway settings, see the "DLP-A249 Provision IP Settings" task on page 19-30. The gateway settings area provisions the ONS 15600 SDH SOCKS proxy server features.

Step 10 Log into the new node:

- If the node has a LAN connection and appears on the network map, from the View menu, choose **Go to Other Node**, then enter the new node.
- If the new node is not connected to the network, log into it using the "DLP-A60 Log into CTC" task on page 17-60.

Step 11 Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, SF, and SD. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See the *Cisco ONS 15454 Troubleshooting Guide*, as necessary.

Step 12 In network view, click the **Circuits** tab.

To view Partial circuits, click the Filter button and select **PARTIAL** from the **Status** drop-down list. The Partial circuits, if any, are displayed.

To view Partial_TL1 circuits, click the Filter button and select **PARTIAL_TL1** from the **Status** drop-down list. The Partial_TL1 circuits, if any, are displayed.

Resolve any partial circuits (both Partial and Partial_TL1) in the network before proceeding. However, if you want to continue with Step 13, match the number of partial circuits and circuit names that existed before and after adding a path protection node. This ensures that no additional partial circuits are created after this procedure is completed.

Step 13 (Optional.) Create test circuits, making sure they pass through the path protection trunk cards, and run test traffic through the node to ensure that the cards are functioning properly. See the "NTP-A344 Create a Manually Routed Optical Circuit" procedure on page 6-45 and the "NTP-A62 Test Optical Circuits" procedure on page 6-51 for information.

Step 14 Create the DCC terminations on the new node. See the "DLP-A377 Provision Section DCC Terminations" task on page 20-69.

Step 15 From the View menu, choose **Go to Network View**.

Step 16 Complete the "DLP-A197 Initiate a Path Protection Force Switch" task on page 18-67 to switch traffic away from the span that will be broken to connect to the new node.

Step 17 Two nodes will connect directly to the new node; remove their fiber connections:

a. Remove the east fiber connection from the node that will connect to the west port of the new node.

b. Remove the west fiber connection from the node that will connect to the east port of the new node.

Step 18 Replace the removed fibers with the fibers that are connected to the new node.

Step 19 Log out of CTC and log back into a node in the network.

Step 20 From the View menu, choose **Go to Network View** to display the path protection nodes. The new node should appear in the network map. Wait for a few minutes to allow all the nodes to appear.

Step 21 Click the **Circuits** tab and wait for all the circuits to appear, including spans. Count the number of incomplete circuits.

Note UNEQ-P alarms might appear on the nodes in your network; this is normal, and the alarms will clear after the circuits are updated.

Step 22 Ensure that nodes involved in the node addition operation are in the initialized state. This is because, CTC does not consider nodes that are not initialized (they appear as gray icons in the CTC network map) when evaluating the circuits.

Note Step 23 is recommended to be performed only on nodes (the newly added node, and the existing two nodes in the network between which the new node is added) involved in the node addition operation. Disable network discovery while launching CTC, add only those nodes involved in the node addition operation.

Note CTC automatically creates VT Tunnels. The cross connects should not be created manually in the intermediate nodes.

Note Step 23 does not create the overlay ring circuits. To create overlay ring circuits that route traffic around multiple rings passing through one or more nodes more than once, see the "NTP-A361 Create an Overlay Ring Circuit" procedure on page 6-98.

Step 23 In the network view, right-click the new node and choose **Update Circuits With New Node** from the shortcut menu. Wait for the confirmation dialog box to appear. Verify that the number of updated circuits in the dialog box is correct (the circuit count should be same as obtained in Step 4).

Step 24 Click the **Circuits** tab and verify that no incomplete circuits are present. However, if the partial circuits still exist in the network, verify whether they were present in Step 5 and Step 12. This will ensure that no additional partial circuits are created by this procedure.

Note If the circuits take more than a minute to appear, log out of CTC, then log back in.

Step 25 Complete the "DLP-A198 Clear a Path Protection Force Switch" task on page 18-68 to clear the protection switch.

Step 26 According to local site practice, complete the "NTP-A177 Path Protection Acceptance Test" procedure on page 5-22.

Stop. You have completed this procedure.

NTP-A294 Remove a Path Protection Node

Purpose	This procedure removes a path protection or multiple path protection configurations from a node.
Tools/Equipment	None
Prerequisite Procedures	NTP-A44 Provision Path Protection Nodes, page 5-20
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution The following procedure minimizes traffic outages during node removals.

Caution If you remove a node that is the only BITS timing source for the ring, you also remove the only source of synchronization for all the nodes in that ring. Circuits that connect to other networks that are synchronized to a Stratum 1 clock will experience a high level of pointer adjustments, which might adversely affect customer service.

Step 1 Draw a diagram of the path protection configuration where you will remove the node. In the diagram, identify the following:

- The node that is connected through its west port to the node that will be removed.
- The node that is connected through its east port to the node that will be removed.

Step 2 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node in the network where you will remove a path protection node.

Step 3 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63 to verify that the path protection configuration is free of alarms. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 8, "Manage Alarms" or, if necessary, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 Complete the "DLP-A333 Delete Circuits" task on page 20-21 for circuits that originate or terminate in the node you will remove. (If a circuit has multiple drops, delete only the drops that terminate on the node you are deleting.)

Step 5 Complete the "DLP-A442 Verify Pass-Through Circuits" task on page 21-25 to verify that circuits passing through the target node enter and exit the node on the same STS.

Step 6 Complete the "DLP-A197 Initiate a Path Protection Force Switch" task on page 18-67 for all spans connected to the node you are removing.

Step 7 Remove all fiber connections between the node being removed and the two neighboring nodes.

Step 8 Reconnect the fiber of the two neighboring nodes directly, west port to east port.

Step 9 Exit CTC and log back in. See the "DLP-A60 Log into CTC" task on page 17-60 for instructions.

Step 10 Log into each newly connected node and click the **Alarms** tab. Verify that the span cards are free of alarms. Resolve any alarms before proceeding. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 11 Complete the "DLP-A195 Verify Timing in a Reduced Ring" task on page 18-66.

Step 12 Complete the "DLP-A198 Clear a Path Protection Force Switch" task on page 18-68 to clear the protection switch.

Step 13 Complete the "NTP-A177 Path Protection Acceptance Test" procedure on page 5-22.

Step 14 Complete the "DLP-A371 Remove Pass-through Connections" task on page 20-55.

Step 15 Log back into a node on the reduced ring. In the CTC Login dialog box, uncheck the **Disable Network Discovery** check box.

Note The deleted node will appear in network view until all SDCC terminations are deleted. To delete SDCC terminations, complete the "DLP-A156 Delete a Section DCC Termination" task on page 18-24.

Step 16 Click the **Circuits** tab and verify that no incomplete circuits are present. If incomplete circuits appear, repeat Steps 14 and 15.

Step 17 If you delete a node that was in a login node group, you will see incomplete circuits for that node in the CTC network view. Although it is no longer part of the ring, the removed node still reports to CTC until it is no longer in a login node group. If necessary, complete the "DLP-A372 Delete a Node from a Specified Login Node Group" task on page 20-56.

Step 18 To remove another node from a path protection configuration, repeat this procedure for the desired node.

Stop. You have completed this procedure.

NTP-A262 Add a Node to a Linear ADM

Purpose	This procedure adds a single ONS 15454 node to the end of an ONS 15454 linear add-drop multiplexer (ADM) network. If the linear ADM carries traffic, you cannot add a node between two linear ADM nodes using this procedure unless you delete and recreate the circuits. To avoid deleting and recreating the circuits, use the "NTP-A323 Add a Node to a Linear ADM Using the Wizard" procedure on page 14-16 to add a node between two linear ADM nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A38 Provision a Linear ADM Network, page 5-6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note Optical transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in Table 2-5 on page 2-20.

Note In a linear ADM configuration, two OC-N cards in 1+1 protection are connected to two OC-N cards in 1+1 protection on a second node. On the second node, two more OC-N cards are connected to a third node. The third node can be connected to a fourth node, and so on, depending on the number of nodes in the linear ADM. Slots 1 to 4 and 14 to 17 or Slots 5 to 6 and 12 to 13 can be used if connections between nodes are consistent. For example, Slot 5 on the first linear ADM node connects to Slot 5 on the second linear ADM node for the working path, and Slot 6 connects to Slot 6 for the protect path. The working OC-N ports have DCC terminations, and the OC-N cards are in a 1+1 protection group.

Step 1 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5 for all the nodes in the ring.

Step 2 At the new node, complete one of the following procedures:

- If the node has not been turned up, complete all procedures in Chapter 4, "Turn Up a Node."
- If the node has been turned up, complete the "NTP-A35 Verify Node Turn-Up" procedure on page 5-2.

Step 3 Verify that the new node has two OC-N cards with the same rate as the linear ADM. If the OC-N cards are not installed, complete the "NTP-A16 Install Optical Cards and Connectors" procedure on page 2-8.

Step 4 Complete "DLP-A73 Create a 1+1 Protection Group" task on page 17-76 for the two OC-N cards that will connect to the linear ADM node.

Step 5 Complete the "DLP-A377 Provision Section DCC Terminations" task on page 20-69 for the working OC-N card at the new node. Make sure to set the port service state in the Create SDCC Termination dialog box to **IS**. (Do not create a DCC termination on the protect card.)

Note DCC failure alarms appear until you create DCC terminations in the linear ADM node and connect the fiber during Step 12.

Step 6 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the linear ADM node that will connect to the new node. If you are already logged in, continue with Step 7.

Step 7 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63.

Step 8 Install the OC-N cards that will connect to the new node. See the "NTP-A16 Install Optical Cards and Connectors" procedure on page 2-8. If the cards are already installed, continue with Step 9.

Step 9 Connect the working card at the existing linear ADM node to the working card at the new node. See the "DLP-A428 Install Fiber-Optic Cables in a 1+1 Configuration" task on page 21-8.

Step 10 Connect the protect card at the existing linear ADM node to the protect card at the new node.

Step 11 Complete the "DLP-A73 Create a 1+1 Protection Group" task on page 17-76 for the two OC-N cards that connect to the new node.

Step 12 Complete the "DLP-A377 Provision Section DCC Terminations" task on page 20-69 for the working OC-N card that connects to the working card on the new node. Make sure to set the port service state in the Create SDCC Termination dialog box to **IS**. (Do not create a DCC termination for the protect card.)

Step 13 From the View menu, choose **Go to Network View.** Verify that the newly created linear ADM configuration is correct. Two green span lines should appear between each linear node.

Step 14 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 19-63 to verify that no unexpected alarms or conditions are present.

Stop. You have completed this procedure.

NTP-A323 Add a Node to a Linear ADM Using the Wizard

Purpose	This procedure adds a node between two nodes in a 1+1 protection group without losing traffic.
Tools/Equipment	Compatible hardware necessary for the upgrade Attenuators might be needed for some applications.
Prerequisite Procedures	The in-service topology upgrade procedure requires that the node to be added is reachable (has IP connectivity with CTC). Two technicians who can communicate with each other during the upgrade might be needed if the PC running CTC and the ONS 15454s are not at the same location.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note OC-N transmit and receive levels should be in their acceptable range as shown in the specifications for each card in Table 2-5 on page 2-20.

Note If overhead circuits exist on the network, an in-service topology upgrade is service affecting. The overhead circuits will drop traffic and have a status of PARTIAL after the upgrade is complete.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a linear ADM node that will connect to the new node. If you are already logged in, continue with Step 2.

Step 2 In network view, right-click the span between the two nodes where you want to add the new node. A dialog appears.

Step 3 Select **Upgrade Protection**. A drop-down list appears.

Step 4 Select **Terminal to Linear** and the first page of the upgrade protection: terminal to linear dialog box appears.

Step 5 The dialog box lists the following conditions for adding a new node:

- The terminal network has no critical or major alarms.
- The node that you will add has no critical or major alarms.
- The node has compatible software version with that of the terminal nodes.
- The node has four unused optical ports matching the speed of the 1+1 protection and no DCC has been provisioned on these four ports.
- Fiber is available to connect the added node to the terminal nodes.

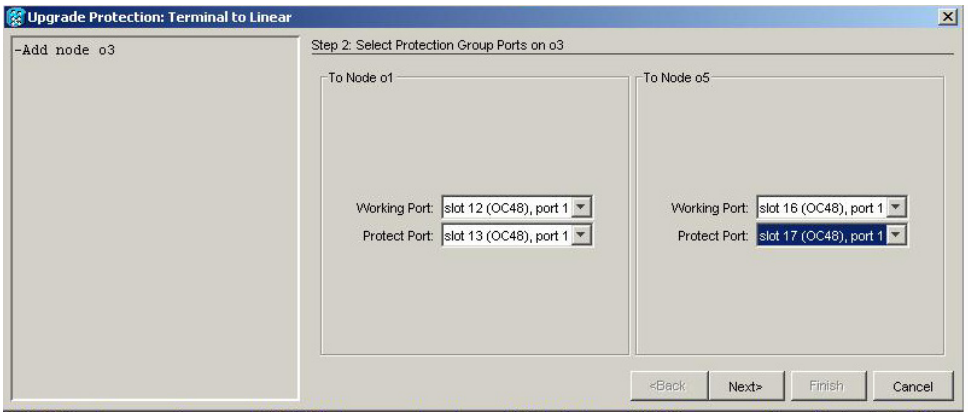
If all of these conditions are met and you wish to continue with the procedure, click **Next**.

Note If you are attempting to add an unreachable node, you must first log in to the unreachable node using a separate CTC session and configure that node. Delete any existing protection groups as described in "DLP-A155 Delete a Protection Group" task on page 18-23. Delete any existing DCC terminations as described in the "DLP-A156 Delete a Section DCC Termination" task on page 18-24 and the "DLP-A359 Delete a Line DCC Termination" task on page 20-45.

Step 6 Enter the node host name or IP address, or choose the name of the new node from the drop-down list. If you type in the name, make sure it is identical to the actual node name. The node name is case sensitive.

Step 7 Click **Next**. The Select Protection Group Ports page (Figure 14-4) appears.

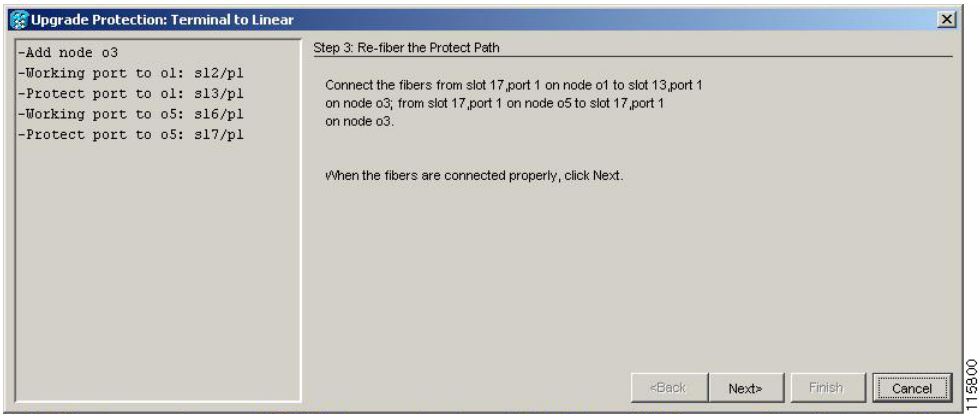
Figure 14-4 Selecting Protection Group Ports



Step 8 From the drop-down lists, select the working and protect ports on the new node that you want to connect to each terminal node.

Step 9 Click **Next**. The Re-fiber the Protected Path dialog box appears (Figure 14-5).

Figure 14-5 Refibering the Protect Path



Step 10 Follow the instructions in the dialog box for connecting the fibers between the nodes.

Step 11 When the fibers are connected properly, click **Next**. The Update Circuit(s) on *Node-Name* dialog box appears.

Note The Back button is not enabled in the wizard. You can click the **Cancel** button at this point and choose the **Yes** button if you want to cancel the upgrade protection procedure. If the procedure fails after you have physically moved the fiber-optic cables, you will need to restore the cables to the original positions and verify through CTC that traffic is on the working path of the nodes before restarting the process. To check traffic status, go to node view and click the **Maintenance > Protection** tabs. In the Protection Groups area, click the 1+1 protection group. You can see the status of the traffic in the Selected Group area.

Step 12 Click **Next** on the Update Circuit(s) on *Node-Name* page to continue with the procedure.

Step 13 The Force Traffic to Protect Path page states that it is about to force the traffic from the working to protect path for the terminal nodes. When you are ready to proceed, click **Next**.

Step 14 Follow each step as instructed by the wizard as it guides you through the process of refibering the working path between nodes and forcing the traffic back to the working path.

Step 15 The Force Traffic to Working Path page states that it is about to force the traffic from the protect to working path for the terminal nodes. When you are ready to proceed, click **Next**.

Step 16 The Completed page appears. This page is the final one in the process. Click **Finish.**

Stop. You have completed this procedure.

NTP-A313 Remove an In-Service Node from a Linear ADM

Purpose	This procedure removes a node from a linear ADM without losing traffic.
Tools/Equipment	None
Prerequisite Procedures	NTP-A38 Provision a Linear ADM Network, page 5-6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note The 1+1 protection group must be unidirectional in order to delete a node from a linear ADM. If your 1+1 protection group is bidirectional, see the "DLP-A154 Modify a 1+1 Protection Group" task on page 18-23 to change it to unidirectional. After you have removed the node from the linear group, you can change the protection setting back to bidirectional.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at a node in the network where you will remove the node.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 4 Click the **Conditions** tab. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 5 On the network map, double-click a node in the 1+1 protection group that is adjacent to the node you intend to remove from the group (the target node).

Step 6 In node view, click the **Maintenance > Protection** tabs.

Step 7 Initiate a Force switch on the working port:

a. In the Protection Groups area, click the 1+1 protection group.

b. In the Selected Group area, click the working port.

c. Next to Switch Commands, click **Force**.

d. In the Confirm Force Operation dialog box, click **Yes**.

e. In the Selected Group area, verify that the following appears:

- Protect port - Protect/Active [FORCE_SWITCH_TO_PROTECT] [PORT STATE]
- Working port - Working/Standby [FORCE_SWITCH_TO_PROTECT], [PORT STATE]

Step 8 Repeat Step 5 through Step 7 for the node that is connected directly to the other side of the target node.

Step 9 Remove the fiber from the working ports of the target node.

Step 10 Connect the fiber between the working ports of the two nodes that were directly connected to either side of the target node.

Step 11 On the node where you initiated a Force switch in Step 8, clear the switch:

a. Next to Switch Commands, click **Clear**.

b. In the Confirm Clear Operation dialog box, click **Yes**.

Step 12 Initiate a Force switch on the protect port:

a. In the Selected Group area, click the protect port. Next to Switch Commands, click **Force**.

b. In the Confirm Force Operation dialog box, click **Yes**.

c. In the Selected Group area, verify that the following appears:

- Protect port - Protect/Standby [FORCE_SWITCH_TO_WORKING], [PORT STATE]
- Working port - Working/Active [FORCE_SWITCH_TO_WORKING], [PORT STATE]

Step 13 From the View menu, choose **Go to Network View**.

Step 14 On the network map, double-click the other node where you initiated a Force switch.

Step 15 In node view, click the **Maintenance > Protection** tabs.

Step 16 Clear the Force switch on the working port:

a. In the Protection Groups area, click the 1+1 protection group.

b. In the Selected Group area, click the working port.

c. Next to Switch Commands, click **Clear**.

d. In the Confirm Clear Operation dialog box, click **Yes**.

Step 17 Complete Step 12 to initiate a Force switch on the protect port.

Step 18 Remove the fiber from the protect ports on the target node.

Step 19 Connect the fiber between the protect ports of the two nodes on each side of the target node.

Step 20 Clear the Force switch:

a. Next to Switch Commands, click **Clear**.

b. In the Confirm Clear Operation dialog box, click **Yes**.

c. In the Selected Group area, verify the following states:

- Protect port - Protect/Standby
- Working port - Working/Active

Step 21 Repeat Step 13 through Step 16 to clear the switch on the other node.

Step 22 Exit CTC.

Step 23 Relaunch CTC at any one of the nodes that were adjacent to the target node. The nodes will now show the circuit status as DISCOVERED when checked.

Stop. You have completed this procedure.

CHAPTER 15

Maintain the Node

This chapter provides procedures for maintaining the Cisco ONS 15454.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary for general troubleshooting information and alarm or error descriptions.

This section lists the chapter procedures (NTPs). Turn to a procedure to view its tasks (DLPs).

1. NTP-A107 Inspect and Replace the Air Filter, page 15-2—Complete as needed.
2. NTP-A108 Back Up the Database, page 15-5—Complete as needed.
3. NTP-A109 Restore the Database, page 15-6—Complete as needed.
4. NTP-A320 View and Manage OSI Information, page 15-9—Complete as needed.
5. NTP-A163 Restore the Node to Factory Configuration, page 15-10—Complete as needed to clear the database and upload a blank database and the latest software.
6. NTP-A300 Viewing the Audit Trail Records, page 15-11—Complete as needed.
7. NTP-A214 Off-Load the Audit Trail Record, page 15-13—Complete as needed.
8. NTP-A306 Off-Load the Diagnostics File, page 15-14—Complete as needed.
9. NTP-A302 Initiate or Clear an External Switching Command, page 15-14—Complete as needed to initiate Force switches, Manual switches, lock-ons, and lockouts.
10. NTP-A112 Clean Fiber Connectors, page 15-15—Complete as needed.
11. NTP-A332 Reset a Card in CTC, page 15-16—Complete as needed.
12. NTP-A215 View G-Series Ethernet Maintenance Information, page 15-17—Complete as needed.
13. NTP-A239 View E-Series Ethernet Maintenance Information, page 15-18—Complete as needed.
14. NTP-A218 Change the Node Timing Reference, page 15-18—Complete as needed.
15. NTP-A223 View the ONS 15454 Timing Report, page 15-19—Complete as needed.
16. NTP-A287 Replace an In-Service Cross-Connect Card, page 15-22—Complete as needed.
17. NTP-A288 Replace the Fan-Tray Assembly, page 15-23—Complete as needed.
18. NTP-A290 Replace the Alarm Interface Panel, page 15-27—Complete as needed.
19. NTP-A291 Replace the Plastic Lower Backplane Cover, page 15-32—Complete as needed.

20. NTP-A162 Replace the UBIC-V EIA, page 15-34—Complete as needed.
21. NTP-A336 Edit Network Element Defaults, page 15-36—Complete as needed to edit the factory-configured (default) network element settings for the Cisco ONS 15454.
22. NTP-A337 Import Network Element Defaults, page 15-38—Complete as needed to import the factory-configured (default) network element settings for the Cisco ONS 15454.
23. NTP-A338 Export Network Element Defaults, page 15-39—Complete as needed to export the factory-configured (default) network element settings for the Cisco ONS 15454.
24. NTP-A356 Test DS1/E1-56 and DS3XM-12 Electrical Card Ports, page 15-40—Complete as needed.

NTP-A107 Inspect and Replace the Air Filter

Purpose	This procedure ensures that the air filter is free from dirt and dust, which allows optimum air flow and prevents dirt and dust from entering the shelf.
Tools/Equipment	New air filter and pinned hex key tool
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Note The air filters are single-use only. They must not be cleaned and reused. This is a Telcordia NEBS requirement, GR-63-CORE Issue 4.

Note Air filters must be inspected every month. If they are dirty or clogged with dust, they must be replaced with a new air filter.

Caution If you install the air filter below 15454-CC-FTA (800-27558-xx), only filters with part numbers 700-23193-01 and 700-23194-01 can be used in this configuration.

Caution Although the filter can work with FTA3 if it is installed with either side facing up, it is recommended that you install it with the metal bracing facing up to preserve the surface of the filter. You must install the air filter with the metal bracing facing up with 15454-CC-FTA.

Note To install the air filter inside the air ramp unit (15454E-AIR-RAMP or 15454-AIR-RAMP), use the ETSI version of the air filter (15454-FTF2 or 15454E-FTF4).

Step 1 If the air filter is installed in the external filter brackets, slide the filter out of the brackets while being careful not to dislodge any dust that might have collected on the filter and proceed to Step 8. Figure 15-1 illustrates a fan-tray air filter in an external filter bracket.

Step 2 If the filter is installed below the fan tray and not in the external filter brackets, open the front door of the shelf assembly using the following substeps. If the front door is already open, proceed to Step 3.

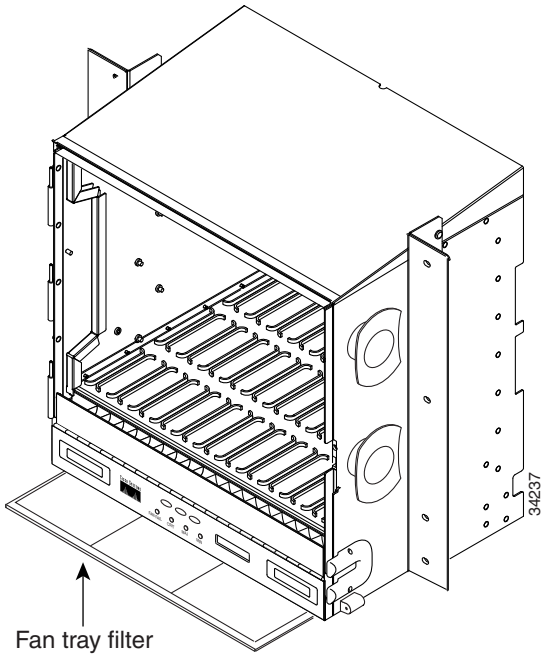
- **a.** Open the front door lock.

  The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.
- **b.** Press the door button to release the latch.
- **c.** Swing the door open.

Step 3 Remove the front door (optional). If you do not want to remove the door or it is already removed, proceed to Step 4.

- **a.** Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
- **b.** Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
- **c.** Secure the dangling end of the ground strap to the door or chassis with tape.

Figure 15-1 ANSI Shelf Fan-Tray Air Filter in an External Filter Bracket (Front Door Removed)



Step 4 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 5 Pull the handles and slide the fan-tray assembly one half inch (12.7 mm) out of the shelf assembly and wait until the fans stop.

Step 6 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

Step 7 Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that might have collected on the filter.

Step 8 Visually inspect the air filter material for dirt and dust.

Step 9 Replace the air filter with a new one if the air filter is dirty or clogged with dust.

Caution Do not leave the fan tray out of the chassis for an extended period of time because excessive heat can damage the ONS 15454 cards.

Step 10 Replace the air filter:

a. If the air filter is installed in the external filter brackets, slide the dry air filter all the way to the back of the brackets.

b. If the filter is installed below the fan-tray assembly, slide the dry/clean air filter into the recessed compartment at the bottom of the shelf assembly. Put the front edge of the air filter flush against the front edge of the recessed compartment. Push the fan tray back into the shelf assembly.

Caution If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and readjust the position of the filter until the fan tray fits correctly.

Note On a powered-up ONS 15454, the fans start immediately after the fan-tray assembly is correctly inserted.

Step 11 To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.

Step 12 Rotate the retractable handles back into their compartments.

Step 13 If you replace the door, also reattach the ground strap.

Step 14 Close and lock the door.

Step 15 Return to your originating procedure (NTP).

Stop. You have completed this procedure.

NTP-A108 Back Up the Database

Purpose	This procedure stores a backup version of the TCC2/TCC2P (software) database on the workstation running Cisco Transport Controller (CTC) or on a network server.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required. Cisco recommends performing a database backup at approximately weekly intervals and prior to and after configuration changes.
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Note You must back up and restore the database for each node on a circuit path in order to maintain a complete circuit.

Note The following parameters are not backed up and restored: node name, and Internet Inter-ORB Protocol (IIOP) port. If you change the node name and then restore a backed up database with a different node name, the circuits map to the new node name. Cisco recommends keeping a record of the old and new node names.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node you want to back up. If you are already logged in, continue with Step 2.

Step 2 Click the **Maintenance > Database** tabs.

Step 3 Click **Backup**.

Step 4 Save the database on the workstation's hard drive or on network storage. Use an appropriate file name with the .db file extension; for example, database.db.

Step 5 Click **Save**.

Step 6 Click **OK** in the confirmation dialog box.

Stop. You have completed this procedure.

NTP-A109 Restore the Database

Purpose	This procedure restores the TCC2/TCC2P software database, either partially or completely.
Tools/Equipment	None
Prerequisite Procedures	NTP-A108 Back Up the Database, page 15-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Caution E1000-2 cards lose traffic for approximately 90 seconds when an ONS 15454 database is restored. Traffic is lost during the period of spanning tree reconvergence. The CARLOSS alarm appears and clears during this period.

Caution If you are restoring the database on multiple nodes, wait approximately one minute after the TCC2/TCC2P reboot has completed on each node before proceeding to the next node.

Caution TCC2P cards can be used in single IP address (repeater) and dual IP address (secure) modes. The secure mode has advanced features that affect database restore. A database from a secure node cannot be loaded on an unsecure repeater node. An unsecure repeater node database can be loaded onto a secure node but the database will follow the node characteristics (that is, become secure). A secure database cannot be loaded onto a TCC2; only TCC2P cards support secure mode. For more information about the dual IP-address secure mode, see the "NTP-A169 Set Up CTC Network Access" procedure on page 4-8. Also refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual*.

Caution To avoid a node IP and secure IP ending up in the same domain after restoring a database, ensure that the node IP stored in the database differs in domain from that of the node in repeater mode. Also, after restoring a database, ensure that the node IP and secure IP differ in domain.

Note The following parameters are not backed up and restored: node name, and IIOP port. If you change the node name and then restore a backed up database with a different node name, the circuits map to the new renamed node. Cisco recommends keeping a record of the old and new node names.

Note ML-Series Ethernet cards must be reset after a database restore. For more information about restoring these cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Note If you want to revert to a previously used software load, consult the platform-specific upgrade documentation for instructions.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you are restoring the database. If you are already logged in, continue with Step 2.

Step 2 Ensure that no BLSR switch events are present; for example, ring-switch east or west. In network view, click the **Conditions** tab and click **Retrieve** to view a list of conditions.

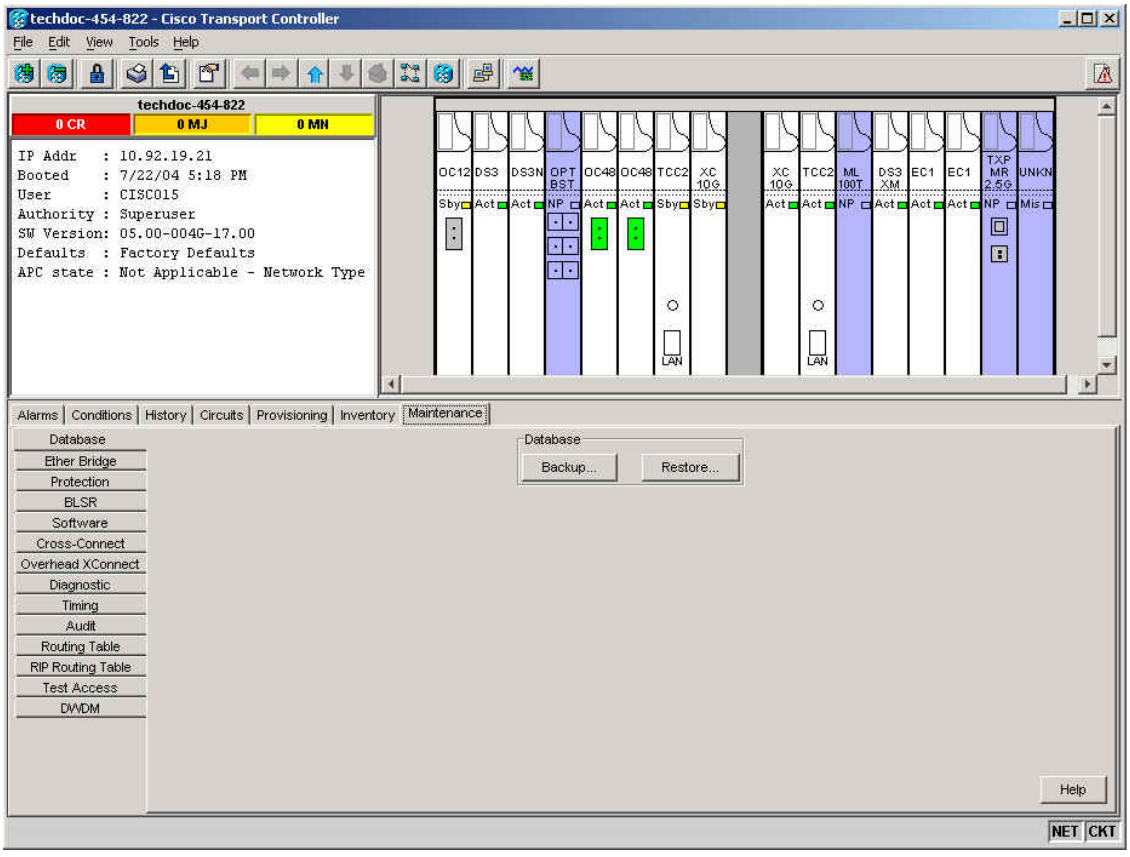
Step 3 If switch events need to be cleared, in node view click the **Maintenance > BLSR** tabs and view the West Switch and East Switch columns.

- **a.** If a switch event (not caused by a line failure) is present, choose **CLEAR** from the drop-down list and click **Apply**.
- **b.** If a switch event caused by the Wait to Restore (WTR) condition is present, choose **CLEAR** from the drop-down list and click **Apply**.

When a switch event is cleared, NO COMMAND appears in the column to indicate that the switch event is no longer in effect.

Step 4 In node view, click the **Maintenance > Database** tabs. Figure 15-2 shows this tab for the TCC2 card. (The TCC2P tab is similar.)

Figure 15-2 Restoring the TCC2 Database



Step 5 Click **Restore**.

Step 6 Locate the database file stored on the workstation hard drive or on network storage.

Note To clear all existing provisioning, locate and upload the database found on the latest ONS 15454 software CD.

Step 7 Click the database file to highlight it.

Step 8 Click **Open**. The DB Restore dialog box appears.

Caution Opening a restore file from another node or from an earlier backup might affect traffic on the login node.

Step 9 If you need a complete database restore, check the **Complete database (System and Provisioning)** checkbox. Continue with Step 11.

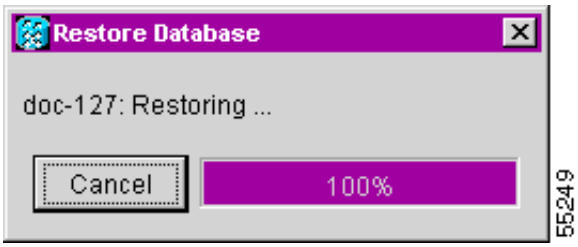
Note Complete database restore may be used only on a node that is removed from the network, and does not carry live provisioning traffic. This operation needs to be done by a live operator onsite, and must not use a remote connection.

Step 10 If you need to restore only the provisioning database (partial restore), do not check the **Complete database (System and Provisioning)** checkbox.

Step 11 Click **Ok**.

The Restore Database dialog box monitors the file transfer (Figure 15-3).

Figure 15-3 Restoring the Database—In-Process Notification



Step 12 Wait for the file to complete the transfer to the TCC2/TCC2P card.

Step 13 Click **OK** when the "Lost connection to node, changing to Network View" dialog box appears. Wait for the node to reconnect.

Step 14 If you cleared a switch in Step 3, reapply the switch as needed.

Stop. You have completed this procedure.

NTP-A320 View and Manage OSI Information

Purpose	This procedure allows you to view and manage OSI including the ES-IS and IS-IS routing information tables, TARP data cache and manual area table.
Tools/Equipment	None
Prerequisite Procedures	NTP-A108 Back Up the Database, page 15-5 NTP-A260 Set Up Computer for CTC, page 3-1 NTP-A318 Provision OSI, page 4-17
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Additional information about the ONS 15454 implementation of OSI is provided in the "Management Network Connectivity" chapter of the *Cisco ONS 15454 Reference Manual*.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 Perform any of the following tasks as needed:

- DLP-A549 View IS-IS Routing Information Base, page 22-56
- DLP-A550 View ES-IS Routing Information Base, page 22-56
- DLP-A551 Manage the TARP Data Cache, page 22-57

Stop. You have completed this procedure.

NTP-A163 Restore the Node to Factory Configuration

Purpose	This procedure reinitializes the ONS 15454 using the CTC reinitialization tool. Reinitialization uploads a new software package to the TCC2/TCC2P cards, clears the node database, and restores the factory default parameters.
Tools/Equipment	ONS 15454 SONET System Software CD, Version 9.1, 9.2, or 9.2.1 JRE 5.0 (JRE 1.6 for Release 9.2 and later) is recommended to log into the node after reinitialization is complete. The reinitialization tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 5.0 (JRE 1.6 for Release 9.2 and later).
Prerequisite Procedures	NTP-A108 Back Up the Database, page 15-5 NTP-A260 Set Up Computer for CTC, page 3-1 One of the following: • NTP-A234 Set Up CTC Computer for Local Craft Connection to the ONS 15454, page 3-3, or • NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

Caution Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinit tool chooses the first product-specific software package in the specified directory if you use the Search Path field instead of the Package and Database fields. You might accidentally copy an incorrect database if multiple databases are kept in the specified directory.

Caution Restoring a node to the factory configuration deletes all cross-connects on the node.

Caution Cisco recommends that you save the node database to safe location if you will not be restoring the node using the database provided on the software CD.

Note The following parameters are not backed up and restored when you delete the database and restore the factory settings: node name, IP address, subnet mask and gateway, and IIOP port. If you change the node name and then restore a backed up database with a different node name, the circuits map to the new renamed node. Cisco recommends keeping a record of the old and new node names.

Step 1 If you need to install or replace one or more TCC2/TCC2P cards, see the "DLP-A36 Install the TCC2/TCC2P Cards" task on page 17-37.

Step 2 If you are using Microsoft Windows, complete the "DLP-A244 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)" task on page 19-25.

Step 3 If you are using UNIX, complete the "DLP-A245 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)" task on page 19-27.

Stop. You have completed this procedure.

NTP-A300 Viewing the Audit Trail Records

Purpose	This procedure describes how to view Audit Trail records. Audit trail records are useful for maintaining security, recovering lost transactions, and enforcing accountability. Accountability refers to tracing user activities; that is, associating a process or action with a specific user.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

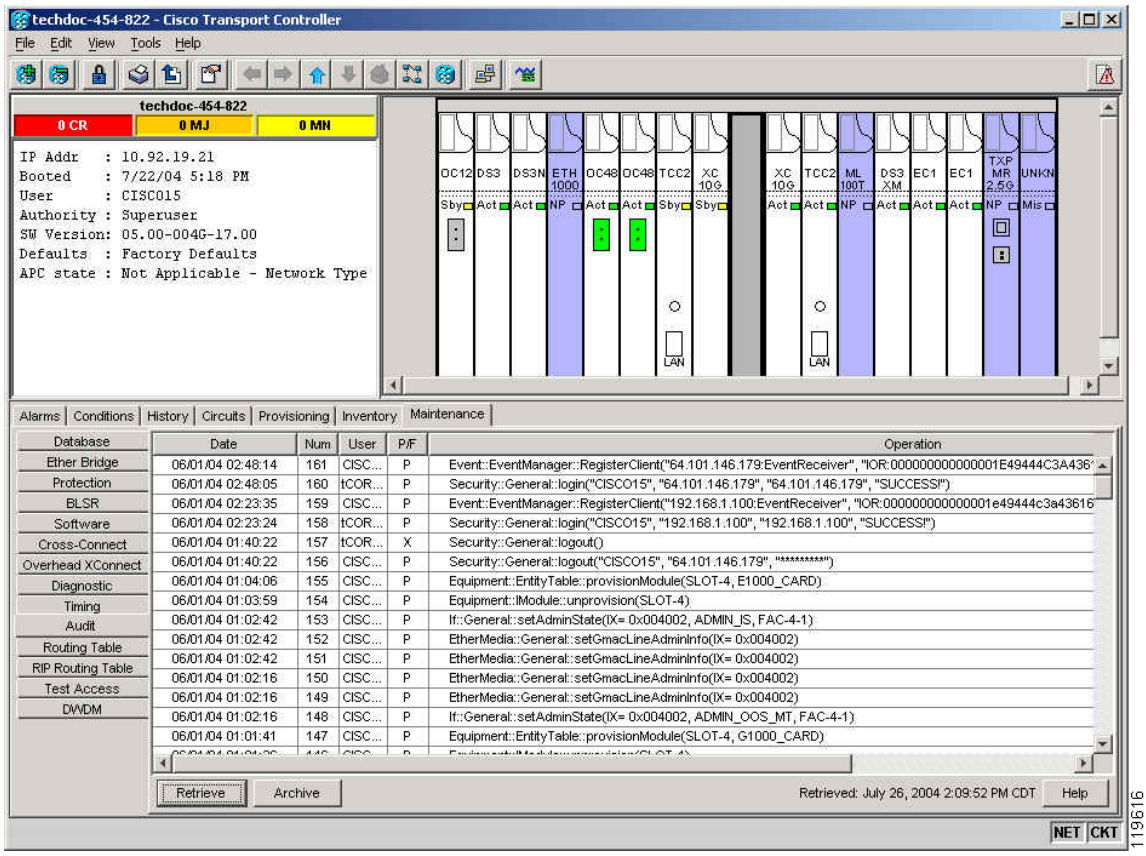
Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to view the audit trail log. If you are already logged in, continue with Step 2.

Step 2 In the node view, click the **Maintenance > Audit** tabs.

Step 3 Click **Retrieve**.

A window containing the most recent Audit Trail records appears as shown in Figure 15-4.

Figure 15-4 Viewing the Audit Trail Records



A definition of each column in the Audit Trail log is listed in Table 15-1.

Table 15-1 Audit Trail Column Definitions

Column	Definition
Date	Date when the action occurred in the format MM/dd/yy HH:mm:ss
Num	Incrementing count of actions
User	User ID that initiated the action
P/F	Pass/Fail (that is, whether or not the action was executed)
Operation	Action that was taken

Step 4 Right-click on the column headings to display the list in ascending-to-descending or descending-to-ascending order.

Step 5 Left-click on the column heading to display the following options:

- Reset Sorting—Resets the column to the default setting.
- Hide Column—Hides the column from view.
- Reset Columns Order/Visibility—Displays all hidden columns.
- Row Count—Provides a numerical count of log entries.

Step 6 Shift-click on the column heading for an incremental sort of the list.

Stop. You have completed this procedure.

NTP-A214 Off-Load the Audit Trail Record

Purpose	This procedure describes how to off-load up to 640 audit trail log entries in a local or network drive file to maintain a record of actions performed for the node. If the audit trail log is not off-loaded, the oldest entries are overwritten after the log reaches capacity.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to off-load the audit trail log. If you are already logged in, continue with Step 2.

Step 2 In the node view, click the **Maintenance > Audit** tabs.

Step 3 Click **Retrieve**.

Step 4 Click **Archive**.

Step 5 In the Archive Audit Trail dialog box, navigate to the directory (local or network) where you want to save the file.

Step 6 Enter a name in the File Name field.

You do not have to give the archive file a particular extension. It is readable in any application that supports text files, such as WordPad, Microsoft Word (imported), etc.

Step 7 Click **Save**.

The 640 entries are saved in this file. The next entries continue with the next number in the sequence, rather than starting over.

Note Archiving does not delete entries from the CTC audit trail log. However, entries can be self-deleted by the system after the log maximum is reached. If you archived the entries, you cannot reimport the log file back into CTC and will have to view the log in a different application.

Stop. You have completed this procedure.

NTP-A306 Off-Load the Diagnostics File

Purpose	This task describes how to off-load a diagnostic file. The diagnostic file contains a set of debug commands run on a node and its results. This file is useful to Cisco Technical Support (TAC) when troubleshooting problems with the node.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to off-load the diagnostics file. If you are already logged in, continue with Step 2.

Step 2 In the node view, click the **Maintenance > Diagnostic** tabs.

Step 3 Click **Node Diagnostic Logs**.

Note For Release 9.1, click **Retrieve Tech Support Log** and proceed to Step 5.

Step 4 The Node Diagnostics dialog box is displayed. Click **OK** to continue.

Step 5 Navigate to the directory (local or network) where you want to save the file.

Step 6 Enter a name in the File Name field.

You do not have to give the archive file a particular extension. It is a compressed file that can be unzipped and read by Cisco Technical Support.

Step 7 Click **Save**.

The status window shows a progress bar indicating the percentage of the file being saved.

Step 8 Click **OK**.

Stop. You have completed this procedure.

NTP-A302 Initiate or Clear an External Switching Command

Purpose	This procedure describes how to apply an external switching command to an optical or electrical card, including Manual and Force switches and lock-ons and lockouts.
Tools/Equipment	None
Prerequisite Procedures	NTP-A324 Create Protection Groups, page 4-13
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60.

Step 2 As needed, complete the "DLP-A365 Initiate an Optical Protection Switch" task on page 20-50.

Step 3 As needed, complete the "DLP-A366 Initiate an Electrical Protection Switch" task on page 20-50.

Step 4 To prevent traffic on a working or protect card from switching to the other card in the pair, complete the "DLP-A201 Apply a Lock-on" task on page 19-1.

Step 5 To prevent traffic from switching to the protect card, complete the "DLP-A202 Apply a Lockout" task on page 19-2.

Note A combination of lock-on and lockout is allowed in 1:1 and 1:N protection; for example, a lock-on on the working card and a lockout on the protect card is permissible.

Step 6 To remove a lock-on or lockout and return a protection group to its usual switching method, complete the "DLP-A203 Clear a Lock-on or Lockout" task on page 19-3.

Note A non-alarmed event (INHSW) is raised when a card is placed in a Lock On or Lock Out state.

Step 7 To lock out a span on a BLSR, which prevents traffic from switching to the locked out span, complete the "DLP-A299 Initiate a BLSR Span Lockout" task on page 19-63.

Step 8 As needed, complete the "DLP-A300 Clear a BLSR Span Lockout" task on page 20-1.

Step 9 As needed, complete the "DLP-A301 Initiate a BLSR Manual Ring Switch" task on page 20-2.

Step 10 As needed, complete the "DLP-A241 Clear a BLSR Manual Ring Switch" task on page 19-23.

Step 11 As needed, complete the "DLP-A303 Initiate a BLSR Force Ring Switch" task on page 20-3.

Step 12 As needed, complete the "DLP-A194 Clear a BLSR Force Ring Switch" task on page 18-65.

Step 13 As needed, complete the "DLP-A197 Initiate a Path Protection Force Switch" task on page 18-67.

Step 14 As needed, complete the "DLP-A198 Clear a Path Protection Force Switch" task on page 18-68.

Stop. You have completed this procedure.

NTP-A112 Clean Fiber Connectors

Purpose	This procedure cleans the fiber connectors.
Tools/Equipment	Inspection microscope
	Type A Fiber Optic Connector Cleaner (CLETOP reel)
	Optical swab
	Optical receiver cleaning stick
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Step 1 Using an inspection microscope, inspect each fiber connector for dirt, cracks, or scratches.

Step 2 Replace any damaged fiber connectors.

Note Replace all dust caps whenever the equipment is unused for 30 minutes or more.

Step 3 Complete the "DLP-A205 Clean Fiber Connectors with CLETOP" task on page 19-4 as necessary.

Step 4 Complete the "DLP-A206 Clean the Fiber Adapters" task on page 19-4 as necessary.

Note To clean multi-fiber optic connectors, complete the "DLP-A204 Clean Multi Fiber-Optic Cable Connectors" task on page 19-3 as necessary.

Caution Do not reuse optical swabs. Keep unused swabs off of work surfaces.

Stop. You have completed this procedure.

NTP-A332 Reset a Card in CTC

Purpose	This procedure resets cards in CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A36 Install the TCC2/TCC2P Cards, page 17-37 NTP-A16 Install Optical Cards and Connectors, page 2-8 NTP-A17 Install the Electrical Cards, page 2-11 NTP-A246 Install Ethernet Cards and Connectors, page 2-13 NTP-A274 Install the FC_MR-4 Card, page 2-15
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 As necessary, complete the "DLP-A364 Reset the TCC2/TCC2P Card Using CTC" task on page 20-49.

Step 3 To reset an optical, electrical, E-Series Ethernet, G-Series Ethernet, ML-Series Ethernet, CE-1000-4 Ethernet, or Storage Access Networking (SAN) cards, complete the "DLP-A460 Reset a Traffic Card Using CTC" task on page 21-42.

Step 4 As necessary complete the "DLP-A54 Hard-Reset a CE-100T-8 Card Using CTC" task on page 17-57.

Step 5 As necessary, complete the "DLP-A224 Soft-Reset a CE-100T-8 Card Using CTC" task on page 19-17.

Stop. You have completed this procedure.

NTP-A215 View G-Series Ethernet Maintenance Information

Purpose	This procedure enables you to view loopback, bandwidth, and J1 path trace information for G-Series Ethernet cards.
Tools/Equipment	None
Prerequisite Procedures	NTP-A246 Install Ethernet Cards and Connectors, page 2-13
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 In node view, double-click a G-Series Ethernet card. The card view appears.

Step 3 To view loopback status, click the **Maintenance > Loopback** tabs.

The Port and Service State columns identify the port number and current service state (In-Service and Normal [IS-NR], Out-of-Service and Management, Disabled [OOS-MA,DSBLD], or Out-of-Service and Management, Maintenance [OOS-MA,MT]) for each port. The Loopback Type column identifies the type of loopback (None, Terminal [Inward], or Facility [Line]) applied to each port on the card.

Step 4 To view Ethernet bandwidth utilization, click the **Maintenance > Bandwidth** tabs.

Step 5 Click **Retrieve Bandwidth Usage**.

The current STS bandwidth usage information appears.

Step 6 To view J1 path trace information, click the **Maintenance > Path Trace** tabs and then click **Retrieve**.

Stop. You have completed this procedure.

NTP-A239 View E-Series Ethernet Maintenance Information

Purpose	This procedure enables you to view maintenance information for E-Series Ethernet cards.
Tools/Equipment	None
Prerequisite Procedures	NTP-A246 Install Ethernet Cards and Connectors, page 2-13
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note The E-Series Maintenance tab is not implemented in this release.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the following tasks:

- DLP-A430 View Spanning Tree Information, page 21-9
- DLP-A309 View the Ethernet MAC Address Table, page 20-4
- DLP-A310 View Ethernet Trunk Utilization, page 20-5

Stop. You have completed this procedure.

NTP-A218 Change the Node Timing Reference

Purpose	This procedure enables automatic timing reference switching or returns the node timing to normal operation.
Tools/Equipment	None
Prerequisite Procedures	NTP-A28 Set Up Timing, page 4-13
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to enable timing switching. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A322 Manual or Force Switch the Node Timing Reference" task on page 20-13 as needed.

Step 3 Complete the "DLP-A323 Clear a Manual or Force Switch on a Node Timing Reference" task on page 20-13 as needed.

Stop. You have completed this procedure.

NTP-A223 View the ONS 15454 Timing Report

Purpose	This procedure displays the current status of the ONS 15454 timing references.
Tools/Equipment	None
Prerequisite Procedures	NTP-A28 Set Up Timing, page 4-13
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to view the node timing status. If you are already logged in, continue with Step 2.

Step 2 Click the **Maintenance > Timing > Report** tabs.

Step 3 In the Timing Report area, you can view node timing information. The date and time of the report appear at the top of the report. The time stamp is the same as the alarms time stamp and can be configured using the "DLP-A112 Display Alarms and Conditions Using Time Zone" task on page 18-2. Table 15-2 on page 15-19 describes the report fields and entries.

Step 4 To update the report, click **Refresh**.

Table 15-2 ONS 15454 Timing Report

Item	Description	Option	Option Description
Clock	Indicates the timing clock. The report section that follows applies to the timing clock indicated.	NE	The node timing clock.
		BITS-1 Out	The BITS-1 Out timing clock.
		BITS-2 Out	The BITS-2 Out timing clock.

Table 15-2 ONS 15454 Timing Report (continued)

Item	Description	Option	Option Description
Status	Indicates the status of the timing clock.	INIT_STATE	The timing reference has not been provisioned. For an NE reference, this status appears just before the first provisioning messages when the TCC2/TCC2P is booting. Timing is provisioned to the internal clock of the node.
		HOLDOVER_STATE	The clock was locked onto a valid timing reference for more than 140 seconds when a failure occurred. Holdover state timing is a computation based on timing during normal state combined with the node's internal clock. The node holds onto this frequency until the valid reference is restored. This status appears for NE references only.
		FREERUN_STATE	The node is running off its internal clock without any modification except the calibrated value to bring timing to 0 PPM. Freerun state can occur when a Force switch to the Internal clock is initiated, all references fail without the 140 seconds of holdover data, or only Internal timing references are defined. This status appears for NE references only.
		NO_SYNC_STATE	A synchronization timing reference is not defined. BITS-1 Out or BITS-2 Out default to this status until an OC-N card is defined as its reference on the Provisioning > Timing tab. This status appears for external references only.
		NE_SYNCH_STATE	BITS-1 Out and BITS-2 Out use the same timing source as the NE. This is displayed when NE Reference is selected for BITS-1 Out and BITS-2 Out Reference List on the Provisioning > Timing tab.
		NORMAL_STATE	The timing reference is locked onto one of its provisioned references. The reference cannot be Internal or no sync state.
		FAST_START_STATE	The node has switched references, but the reference is too far away to reach normal state within an acceptable amount of time. Fast Start is a fast acquisition mode to allow the node to quickly acquire the reference. After it achieves this goal, the node progresses to the normal state.
Status (cont.)		FAST_START_FAILED_STATE	A timing reference is too far away to reach in normal state. The fast start state could not acquire sufficient timing information within the allowable amount of time.
Status Changed At	Date and time of the last status change.	—	—

Table 15-2 ONS 15454 Timing Report (continued)

Item	Description	Option	Option Description
Switch Type	Type of switch.	AUTOMATIC	The timing switch was system-generated.
		Manual	The timing switch was a user-initiated Manual switch.
		Force	The timing switch was user-initiated Force switch.
Reference	Indicates the timing reference.	Three timing references (Ref-1, Ref-2, and Ref-3) are available on the Provisioning > Timing tab.	These options indicate the timing references that the system uses, and the order in which they are called. (For example, if Ref-1 becomes available, Ref-2 is called.)
Selected	Indicates whether the reference is selected.	Selected references are indicated with an X.	—
Facility	Indicates the timing facility provisioned for the reference on the Provisioning > Timing tab.	BITS-1	The timing facility is a building integrated timing supply (BITS) clock attached to the node's BITS-1 pins.
		BITS-2	The timing facility is a BITS clock attached to the node's BITS-2 pins.
		OC-N card with port #	If the node is set to line timing, this is the OC-N card and port provisioned as the timing reference.
		Internal clock	The node is using its internal clock.
State	Indicates the timing reference state.	IS	The timing reference is in service.
		OOS	The timing reference is out of service.
Condition	Indicates the timing reference state.	OKAY	The reference is valid to use as a timing reference.
		OOB	Out of bounds; the reference is not valid and cannot be used as a timing reference, for example, a BITS clock is disconnected.
Condition Changed	Indicates the date and time of the last status change in MM/DD/YY HH:MM:SS format.	—	—
SSM	Indicates whether SSM is enabled for the timing reference.	Enabled	SSM is enabled.
		Disabled	SSM is not enabled.

Table 15-2 ONS 15454 Timing Report (continued)

Item	Description	Option	Option Description
SSM Quality	Indicates the SSM timing quality.	8 to 10 SSM quality messages might be displayed.	For a list of SSM message sets, see the *Cisco ONS 15454 Reference Manual*.
SSM Changed	Indicates the date and time of the last SSM status change in MM/DD/YY HH:MM:SS format.	—	—

Stop. You have completed this procedure.

NTP-A287 Replace an In-Service Cross-Connect Card

Purpose	This procedure replaces an in service cross-connect card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A37 Install the XCVT, XC10G, or XC-VXC-10G Cards, page 17-40
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Caution Removing any active card from the ONS 15454 can result in traffic interruption. Use caution when replacing cards and verify that only the standby card is being replaced.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will replace the card.

Step 2 From the View menu choose **Go to Network View**.

Step 3 Click the **Alarms** tab, then complete the following substeps:

- **a.** Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.
- **b.** Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 4 Determine the active cross-connect card (XCVT/XC10G/XC-VXC-10G). The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is amber.

Note You can also place the cursor over the card graphic to display a popup identifying the card as active or standby.

Step 5 If you want to replace the active cross-connect card, you must switch it to standby first by completing the following substeps. If you want to replace the standby card, skip this step and continue with Step 6.

a. In the node view, click the **Maintenance > Cross-Connect** tabs.

b. Under Cross Connect Cards, choose **Switch**.

c. Click **Yes** in the Confirm Switch dialog box.

Note After the active XCVT/XC10G/XC-VXC-10G goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

Step 6 Physically remove the standby cross-connect card (XCVT/XC10G/XC-VXC-10G) from the ONS 15454.

Note An improper removal (IMPROPRMVL) alarm is raised when a card reseat is performed, unless the card is first deleted in CTC. The alarm clears after the card replacement is complete.

Step 7 Insert the replacement cross-connect card (XCVT/XC10G/XC-VXC-10G) into the empty slot.

The replacement card boots up and becomes ready for service after approximately one minute.

Stop. You have completed this procedure.

NTP-A288 Replace the Fan-Tray Assembly

Purpose	This procedure replaces a malfunctioning fan-tray assembly.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution The 15454-FTA3 and 15454-FTA3-T fan-tray assemblies can only be installed in ONS 15454 R3.1 and later shelf assemblies (15454-SA-ANSI, P/N: 800-19857-xx; 15454-SA-HD, P/N: 800-24848-xx). The fan-tray assembly includes a pin that prevents it from being installed in ONS 15454 shelf assemblies released before ONS 15454 R3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3-T or 15454-FTA3 in an incompatible shelf assembly.

Caution 15454-CC-FTA is compatible with Software R2.2.2 and greater. It is compatible with shelf assemblies 15454-SA-ANSI and 15454-SA-HD.

Caution As with the FTA3, the 15454-CC-FTA Fan Fail LED on the front of the fan-tray assembly illuminates when one or more fans fail to indicate that a fan-tray assembly or AIP replacement is required. But the Fan Fail LED on the 15454-CC-FTA will also illuminate when only one power source is connected to the chassis, and or any fuse blows. In such conditions, the Fan Alarm is triggered and the fans run at maximum speed.

Caution Do not force a fan-tray assembly into place. Doing so can damage the connectors on the fan tray and/or the connectors on the backplane.

Note The 15454-SA-ANSI or 15454-SA-HD shelf assembly and 15454-FTA3, 15454-FTA3-T, or 15454-CC-FTA fan-tray assembly are required with the ONS 15454 XC-10G, OC-192, and OC-48 any slot (AS) cards.

Note To replace the fan-tray assembly (FTA), it is not necessary to move any of the cable management facilities.

Step 1 Review Table 15-3 to ensure that you have compatible components when replacing the fan-tray assembly and note the alarms that will occur when an incompatibility occurs.

Note If you need to determine the hardware that has been installed on a node, click the Inventory tab in node view.

Table 15-3 Incompatibility Alarms

Shelf Assembly[1]	Fan Tray[2]	AIP[3]	10G Cards[4]	Ethernet Cards[5]	Alarms
—	—	No fuse	—	—	Mismatch of Equipment Attributes (MEA) on alarm interface panel (AIP)
NEBS3E or NEBS3	2A	2A	No	—	None
NEBS3E or NEBS3	2A	2A	Yes	—	MEA on 10G
NEBS3E or NEBS3	2A	5A	No	—	None
NEBS3E or NEBS3	2A	5A	Yes	—	MEA on 10G
ANSI or HD	2A	2A	No	—	None
ANSI or HD	2A	2A	Yes	2.5G compatible	MEA on fan tray, AIP, and Ethernet
ANSI or HD	2A	2A	Yes	10G compatible	MEA on fan tray and AIP
ANSI or HD	2A	5A	No	Either	None

Table 15-3 Incompatibility Alarms (continued)

Shelf Assembly[1]	Fan Tray[2]	AIP[3]	10G Cards[4]	Ethernet Cards[5]	Alarms
ANSI or HD	2A	5A	Yes	2.5G compatible	MEA on fan tray and Ethernet
ANSI or HD	2A	5A	Yes	10G compatible	MEA on fan tray
ANSI or HD	5A	2A	No	Either	MEA on AIP
ANSI or HD	5A	2A	Yes	2.5G compatible	MEA on AIP and Ethernet
ANSI or HD	5A	2A	Yes	10G compatible	MEA on AIP
ANSI or HD	5A	5A	No	Either	None
ANSI or HD	5A	5A	Yes	Either	None

1. 15454-SA-NEBS3E (P/N: 800-07149-xx) or 15454-SA-NEBS3 (P/N: 800-06741-xx) = shelf assemblies released before ONS 15454 Release 3.1
   15454-SA-ANSI (P/N: 800-19857-xx) = ONS 15454 Release 3.1 and later shelf assembly
   15454-SA-HD (P/N: 800-24848-xx) = ONS 15454 Release 3.1 and later shelf assembly
2. 5A Fan Tray = 15454-FTA3 (P/N: 800-19858-xx), 15454-FTA3-T (P/N: 800-21448-xx), 15454-FTA (P/N: 800-27561-xx), 15454-CC-FTA (P/N: 800-27558-xx)
   2A Fan Tray = 15454-FTA2 (P/Ns: 800-07145-xx, 800-07385-xx, 800-19591-xx, 800-19590-xx)
3. 5A AIP (P/N: 73-7665-xx), 2A AIP (P/N: 73-5262-xx)
4. 10G cards include the XC-10G, OC-192, and OC-48 AS.
5. 2.5G indicates cards that are compatible with the XC and XCVT cross-connect cards: E100T-12, E1000-2, E100T-G, E1000-2-G, G1K-4, ML100T-12, ML1000-2. 10G indicates cards that are compatible with the XC10G cross-connect card: E100T-G, E1000-2-G, G1K-4, ML100T-12, ML1000-2.

Step 2 Open the front door of the shelf assembly. If the shelf assembly does not have a front door, continue with Step 4.

- **a.** Open the front door lock.

  The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.
- **b.** Press the door button to release the latch.
- **c.** Swing the door open.

Step 3 Remove the front door (optional). If you do not want to remove the door, proceed to Step 4.

- **a.** Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
- **b.** Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
- **c.** Secure the dangling end of the ground strap to the door or chassis with tape.

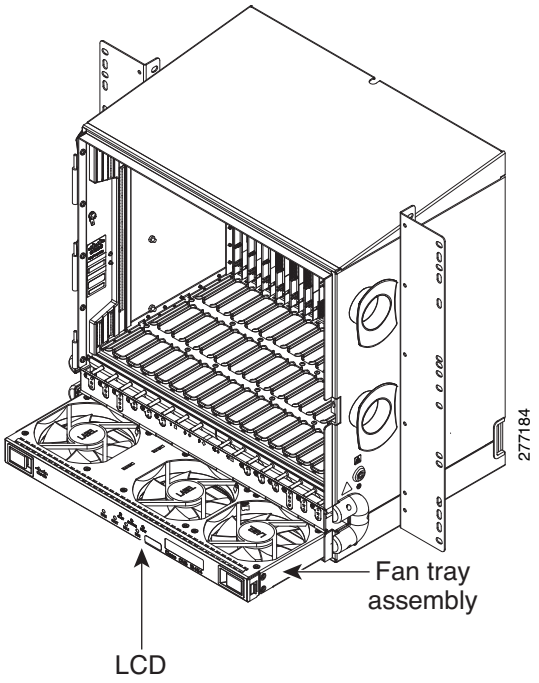
Step 4 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 5 Fold out the retractable handles at the outside edges of the fan tray.

Step 6 Pull the handles and slide the fan-tray assembly one half inch (12.7 mm) out of the shelf assembly and wait until the fans stop.

Step 7 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly. Figure 15-5 shows the location of the fan tray.

Figure 15-5 Removing or Replacing the Fan-Tray Assembly (Front Door Removed)



Step 8 If you are replacing the fan-tray air filter and it is installed beneath the fan-tray assembly, slide the existing air filter out of the shelf assembly and replace it before replacing the fan-tray assembly.

If you are replacing the fan-tray air filter and it is installed in the external bottom bracket, you can slide the existing air filter out of the bracket and replace it at anytime. For more information on the fan-tray air filter, see the "NTP-A107 Inspect and Replace the Air Filter" procedure on page 15-2.

Step 9 Slide the new fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.

Step 10 To verify that the tray has plugged into the backplane, check that the LCD on the front of the fan tray is activated.

Step 11 If you replace the door, be sure to reattach the ground strap.

Stop. You have completed this procedure.

Note The estimated replacement time by a skilled technician is 2 minutes.

NTP-A290 Replace the Alarm Interface Panel

Purpose	This procedure replaces the alarm interface panel (AIP) with a new AIP on an in-service node without affecting traffic; however, shared packet rings might need to be deleted and rebuilt after the repair procedure. Ethernet circuits that traverse nodes with a software release prior to R4.0 will be affected.
Tools/Equipment	#2 Phillips screwdriver
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Warning **The covers are an integral part of the safety design of the product. Do not operate the unit without the covers installed.**

Caution Do not use a 2A AIP with a 5A fan-tray assembly; doing so will cause a blown fuse on the AIP.

Caution If any nodes in an Ethernet circuit are not using Software R4.0 or later, there is a risk of Ethernet traffic disruptions. Contact the Cisco Technical Support at 1 800 553-2447 when prompted to do so in the procedure.

Caution Always use the supplied ESD wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Caution Do not perform this procedure on a node with live traffic. Hot-swapping the AIP can affect traffic and result in a loss of data. For assistance with AIP replacement contact Cisco Technical Support. See the "Obtaining Documentation and Submitting a Service Request" section on page lxiv.

Note Perform this procedure during a maintenance window. Resetting the active TCC2/TCC2P card can cause a service disruption of less then 50 ms to OC-N or DS-N traffic. Resetting the active TCC2/TCC2P card can cause a service disruption of 3 to 5 minutes on all Ethernet traffic due to spanning tree reconvergence if any nodes in the Ethernet circuit are not using Software R4.0 or later.

Step 1 Review Table 15-3 on page 15-24 to ensure that you have compatible components when replacing the fan-tray assembly and note the alarms that will occur when an incompatibility occurs.

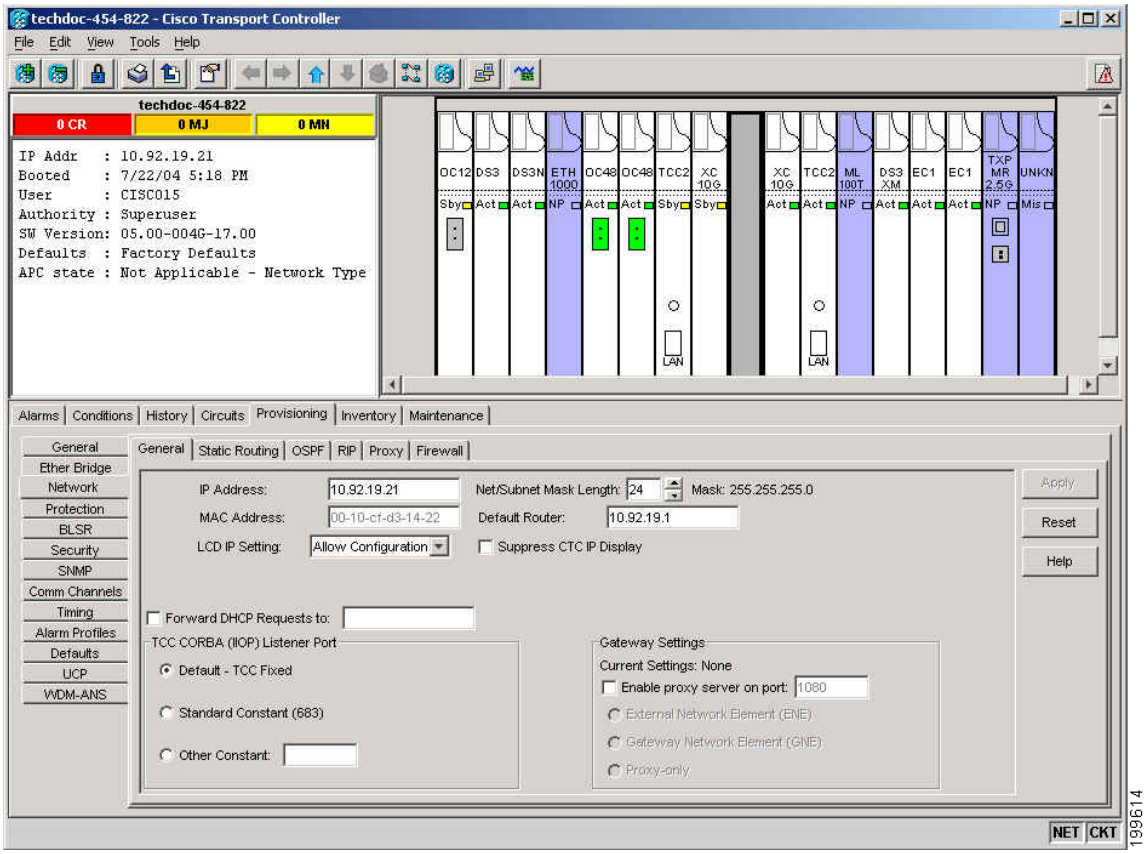
Step 2 Ensure that all nodes in the affected network are running the same software version by completing the following substeps before replacing the AIP and repairing circuits:

- **a.** Log into the node if you have not done so already by completing the "DLP-A60 Log into CTC" task on page 17-60.
- **b.** In network view, click the **Maintenance > Software** tabs. The working software version for each node is listed in the Working Version column.
- **c.** If you need to upgrade the software on a node, refer to the release-specific software upgrade document for software upgrade procedures. No hardware should be changed or circuit repair performed until after the software upgrade is complete. If you do not need to upgrade software or have completed the software upgrade, proceed to Step 3.

Step 3 Record the MAC address of the old AIP:

- **a.** If you are using a single IP address "repeater" configuration, click the **Provisioning > Network > General** tab.
- **b.** Record the MAC address shown in the General tab (Figure 15-6).

Figure 15-6 Find the MAC Address in a Single IP Address Configuration

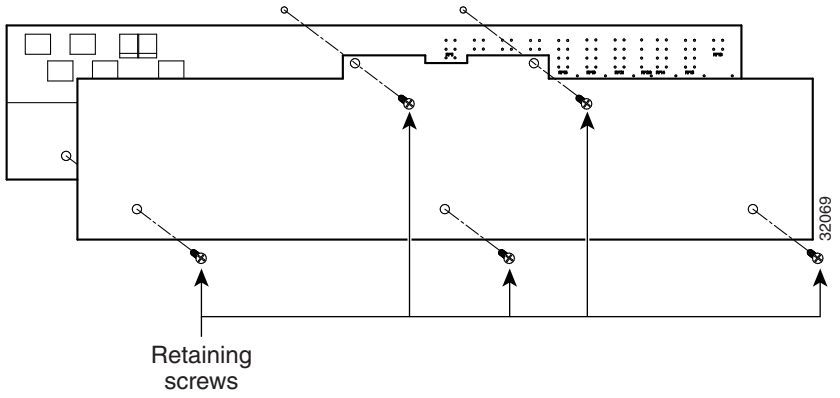


(If you are using a secure dual IP mode configuration, the MAC addresses are shown in the **Provisioning > Security > Data Comm** tab.)

Step 4 Call Cisco Technical Support for assistance in replacing the AIP and maintaining the original MAC address. See the "Obtaining Documentation and Submitting a Service Request" section on page lxiv.

Step 5 Unscrew the five screws that hold the lower backplane cover in place (Figure 15-7).

Figure 15-7 Lower Backplane Cover



Step 6 Grip the lower backplane cover and gently pull it straight away from the backplane.

Step 7 Unscrew the two screws that hold the AIP cover in place.

Step 8 Grip the cover and gently pull away from the backplane.

Note On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves, the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

Step 9 Grip the AIP and gently pull it away from the backplane.

Step 10 Disconnect the fan-tray assembly power cable from the AIP.

Step 11 Set the old AIP aside for return to Cisco.

Caution The type of shelf the AIP resides in determines the version of AIP that should replace the failed AIP. The 15454-SA-ANSI shelf (P/N: 800-19857) and 15454-SA-HD (P/N: 800-24848) currently use the 5A AIP, (P/N: 73-7665-01). The 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves and earlier use the 2A AIP (P/N: 73-5262-01).

Caution Do not put a 2A AIP (P/N: 73-5262-01) into a 15454-SA-ANSI shelf (P/N: 800-19857) or 15454-SA-HD (P/N: 800-24848); doing so will cause a blown fuse on the AIP.

Step 12 Attach the fan-tray assembly power cable to the new AIP.

Step 13 Place the new AIP on the backplane by plugging the panel into the backplane using the DIN connector.

Step 14 Replace the AIP cover over the AIP and secure the cover with the two screws.

Step 15 Replace the lower backplane cover and secure the cover with the five screws.

Caution Cisco recommends that TCC2/TCC2P card resets be performed in a maintenance window to avoid any potential service disruptions.

Step 16 Reset the standby TCC2/TCC2P card:

a. Right-click the standby TCC2/TCC2P card and choose **Reset Card**.

b. Click **Yes** in the Resetting Card dialog box. As the card resets, a loading (Ldg) indication appears on the card in CTC.

Note The reset takes approximately five minutes. Do not perform any other steps until the reset is complete.

Step 17 Complete the "DLP-A364 Reset the TCC2/TCC2P Card Using CTC" task on page 20-49 to reset the active TCC2/TCC2P card.

Step 18 From the **File** menu, choose **Exit** to exit the CTC session.

Step 19 Log back into the node. At the Login dialog box, choose **(None)** from the Additional Nodes drop-down list.

Step 20 Record the new MAC address:

a. In node view, click the **Provisioning > Network** tabs.

b. Record the MAC address shown in the General tab.

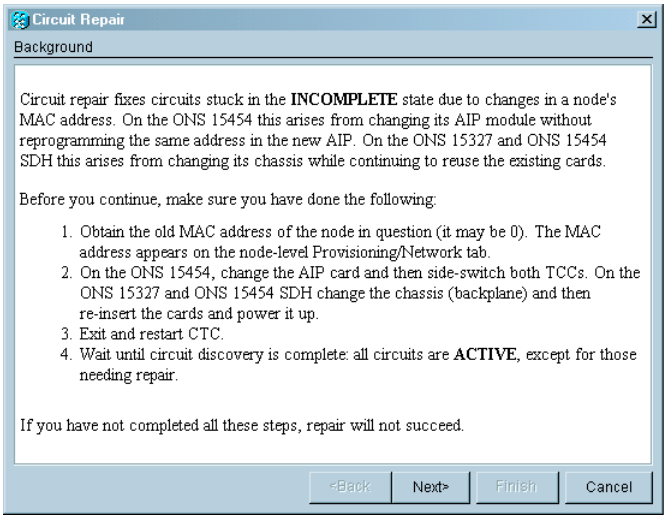
Note This location assumes a single IP, "repeater" configuration. For a secure, dual IP node, the IPs are viewable on the **Provisioning > Security > Data Comm** tab.

Step 21 In node view, click the **Circuits** tab. Note that all circuits listed have a status of PARTIAL.

Step 22 In node view, choose **Circuits > Repair Circuits** from the **Tools** menu. The Circuit Repair dialog box appears.

Step 23 Read the instructions in the Circuit Repair dialog box (Figure 15-8). If all the steps in the dialog box have been completed, click **Next**. Ensure that you have the old and new MAC addresses.

Figure 15-8 Repairing Circuits



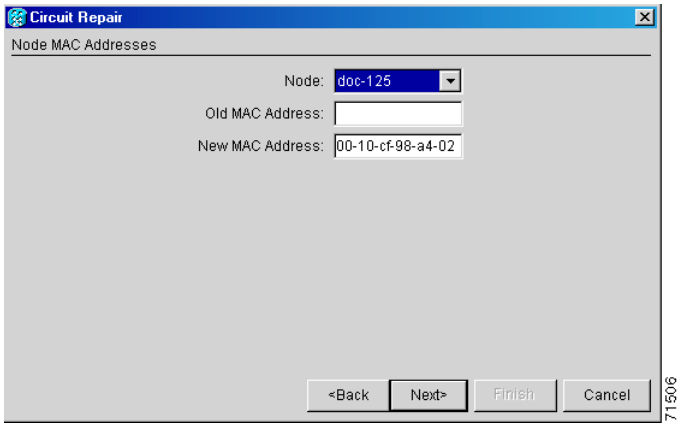
Step 24 The Node MAC Addresses dialog box appears (Figure 15-9):

a. From the Node drop-down list, choose the name of the node where you replaced the AIP.

b. In the Old MAC Address field, enter the old MAC address that was recorded in Step 3.

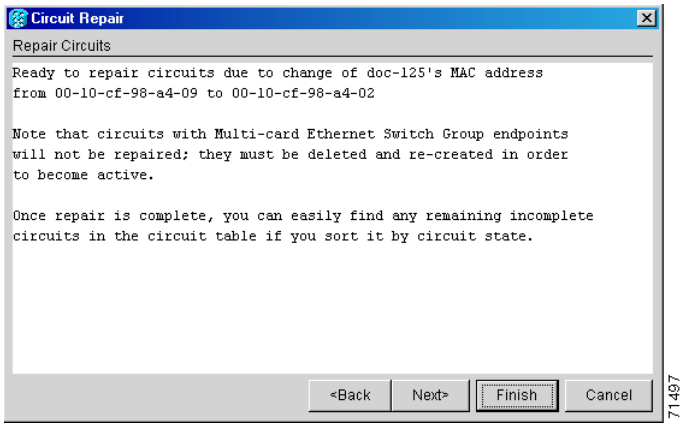
c. Click **Next**.

Figure 15-9 Recording the Old MAC Address Before Replacing the AIP



Step 25 The Repair Circuits dialog box appears (Figure 15-10). Read the information in the dialog box and click **Finish**.

Figure 15-10 Circuit Repair Information



Note The CTC session freezes until all circuits are repaired. Circuit repair can take up to five minutes or more depending on the number of circuits provisioned.

When the circuit repair is complete, the Circuits Repaired dialog box appears.

Step 26 Click **OK**.

Step 27 In the node view of the new node, click the **Circuits** tab. Check to ensure that all circuits listed have a status of DISCOVERED. If all circuits listed are not DISCOVERED, call the Cisco Technical Support to open a Return Material Authorization (RMA). See the "Obtaining Documentation and Submitting a Service Request" section on page lxiv.

Stop. You have completed this procedure.

NTP-A291 Replace the Plastic Lower Backplane Cover

Purpose	This procedure replaces the plastic cover located at the bottom rear of the ONS 15454.
Tools/Equipment	Phillips screwdriver
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

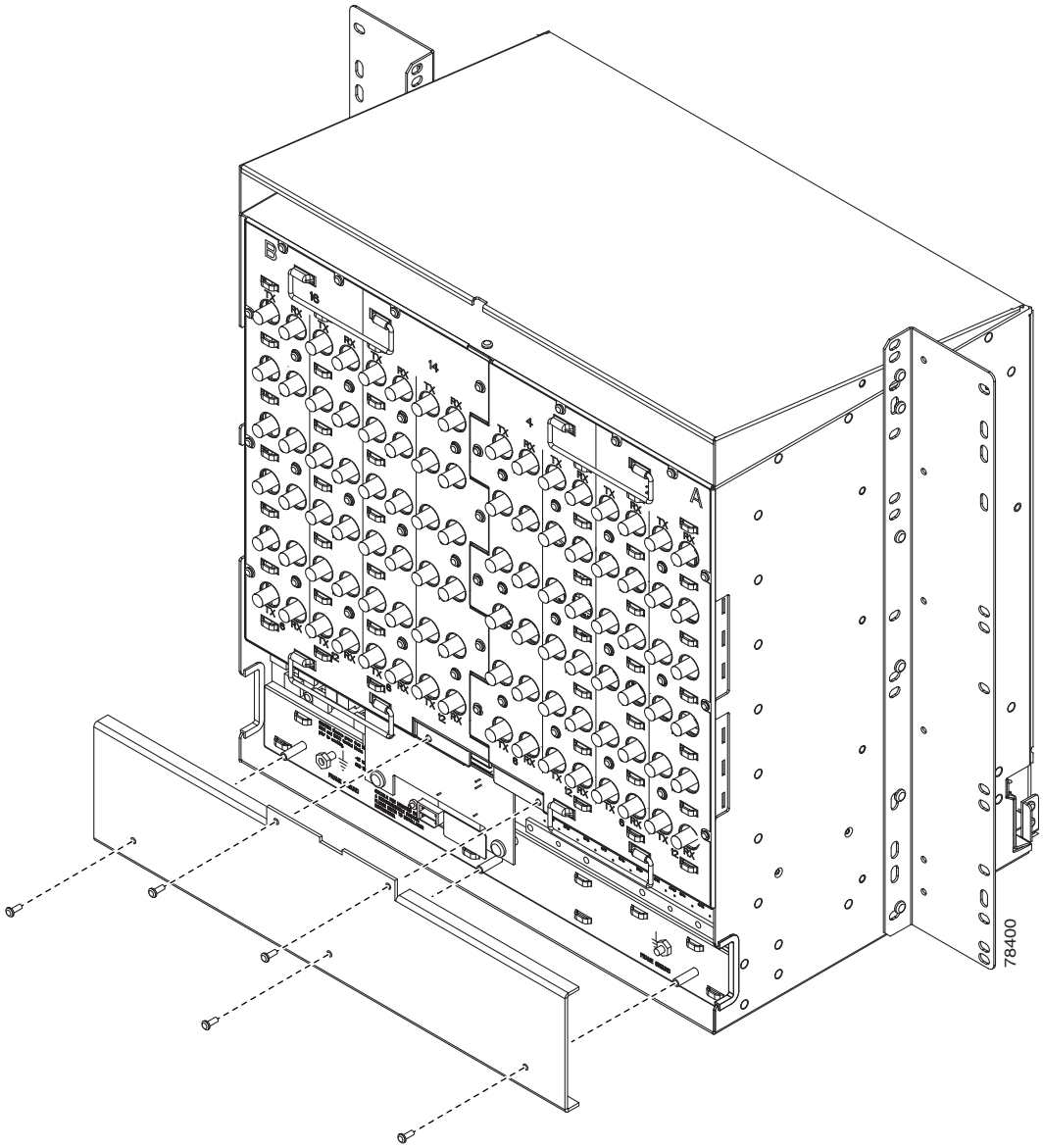
Step 1 Use the Phillips screwdriver to unscrew the five retaining screws that hold the plastic cover in place.

Step 2 Grasp the metal cover on each side.

Step 3 Gently pull the plastic cover away from the backplane.

Step 4 Place the plastic cover against the shelf assembly and align the screw holes on the cover and the shelf assembly (Figure 15-11).

Figure 15-11 Attaching Plastic Lower Backplane Cover



Step 5 Tighten the five retaining screws that hold the plastic cover in place.

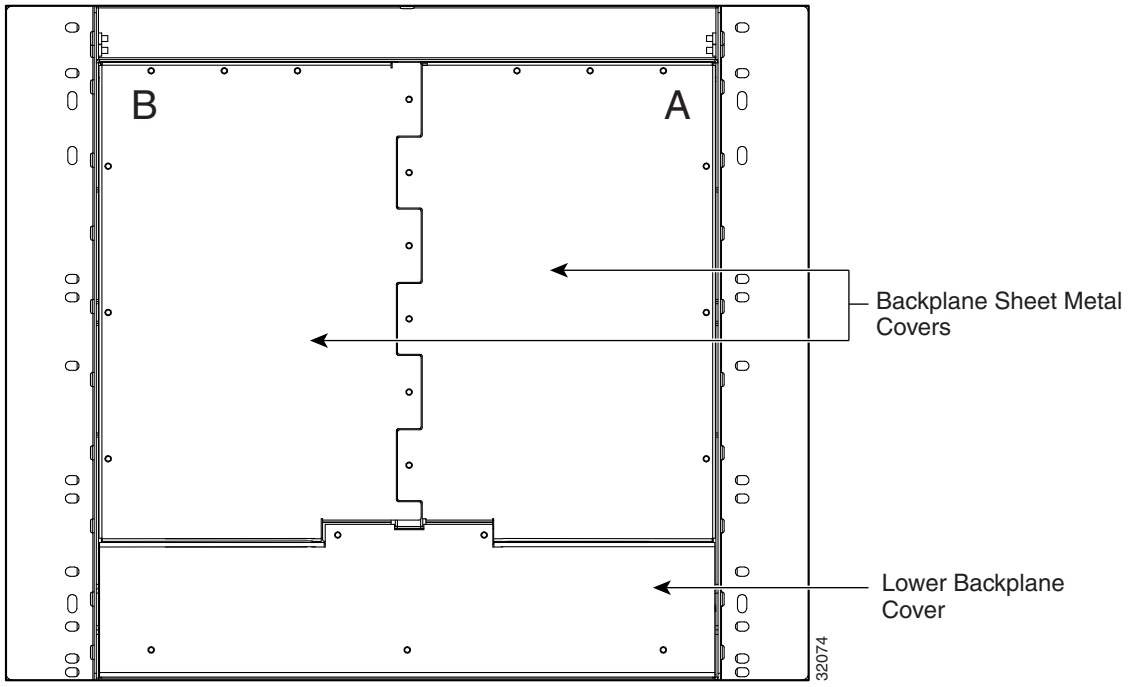
Stop. You have completed this procedure.

NTP-A162 Replace the UBIC-V EIA

Purpose	This procedure replaces the UBIC-V EIA.
Tools/Equipment	#2 Phillips screwdriver Small slot-head screwdriver Replacement UBIC-V EIA and accompanying screws
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

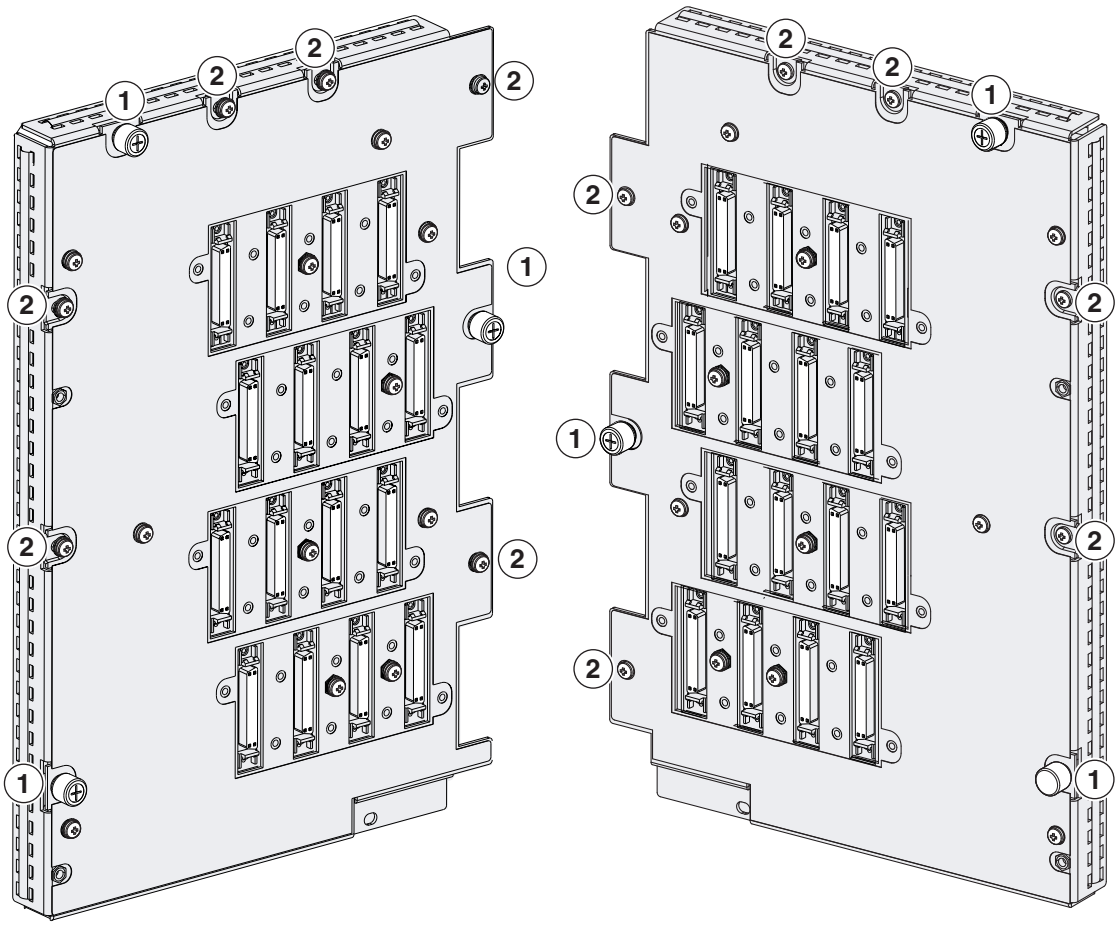
Step 1 To remove the lower backplane cover, loosen and remove the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly (Figure 15-12).

Figure 15-12 ONS 15454 Rear View (with Sheet Metal Covers Attached)



Step 2 Loosen and remove the six perimeter screws that hold the sheet metal cover and UBIC-V in place (Figure 15-13).

Figure 15-13 UBIC-V EIA Screw Locations

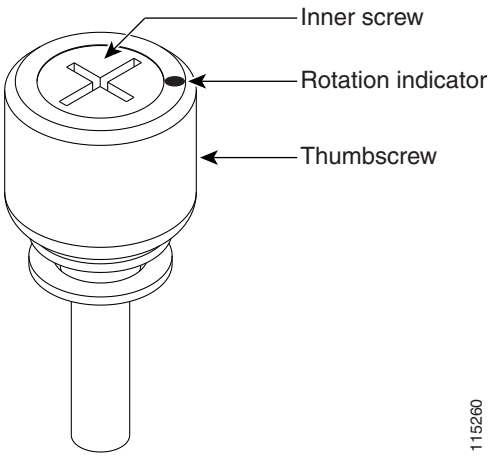


1 Jack screws (3)
2 Perimeter screws, 6-32 x 0.375-inch Phillips head (6)

Step 3 Use a Phillips screwdriver to loosen each jack screw a maximum of two turns. Rotate each jack screw two turns at a time (per the rotation indicator) until all jack screws are fully disengaged (Figure 15-14).

Caution Loosening the jack screws unevenly could cause damage to the UBIC-V connectors.

Figure 15-14 UBIC-V EIA Jack Screw



Step 4 Grip two of the jack screws and use them to carefully pull the UBIC-V away from the shelf.

Note Attach backplane sheet metal covers whenever EIAs are not installed.

Step 5 Perform the "DLP-A190 Install a UBIC-V EIA" task on page 18-59 to install the new UBIC-V EIA.

Stop. You have completed this procedure.

NTP-A336 Edit Network Element Defaults

Purpose	This procedure edits the NE defaults using the NE Defaults editor. The new defaults can either be applied only to the node on which they are edited or exported to a file and imported for use on other nodes.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note For a list of card and node default settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*. To change card settings individually (that is, without changing the defaults), see Chapter 10, "Change Card Settings." To change node settings, see Chapter 11, "Change Node Settings."

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to edit NE defaults.

Step 2 Click the **Provisioning > Defaults** tabs.

Step 3 Under Defaults Selector, choose a card type (if editing card-level defaults), **CTC** (if editing CTC defaults), or **NODE** (if editing node-level defaults). Clicking on the node name (at the top of the Defaults Selector column) lists all available NE defaults in the Default Name column. To selectively display just the defaults for a given card type, for node-level, or for CTC-level, you can drill down the Defaults Selector menu structure.

Step 4 Locate a default you want to change under Default Name.

Step 5 Click in the **Default Value** column for the default property you are changing and either choose a value from the drop-down menu (when available), or type in the desired new value.

Note If you click **Reset** before you click **Apply**, all values will return to their original settings.

Step 6 Click **Apply** (click in the **Default Name** column to activate the Apply button if it is unavailable). You can modify multiple default values before applying the changes.

A pencil icon will appear next to any default value that will be changed as a result of editing the defaults file.

Step 7 If you are modifying node-level defaults, a dialog box appears telling you that applying defaults for node level attributes overrides current provisioning and asks if you want to continue. Click **Yes**.

If you are modifying the IIOP Listener Port setting, a dialog box appears warning you that the node will reboot and asks if you want to continue. Click **Yes**.

Note Changes to most node defaults reprovision the node when you click Apply. Changes made to card settings using the Defaults Editor do not change the settings for cards that are already installed or slots that are preprovisioned for cards, but rather, change only cards that are installed or preprovisioned thereafter. To change settings for installed cards or preprovisioned slots, see Chapter 10, “Change Card Settings.”

Note Changing some NE defaults can cause CTC disconnection or a reboot of the node in order for the default to take effect. Before you change a default, view the Side Effects column of the Defaults editor (right-click a column header and select **Show Column > Side Effects**) and be prepared for the occurrence of any side effects listed for that default.

Stop. You have completed this procedure.

NTP-A337 Import Network Element Defaults

Purpose	This procedure imports the NE defaults using the NE Defaults editor. The defaults can either be imported from the CTC software CD (factory defaults) or from a customized file exported and saved from a node.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note For a list of card and node default settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to import NE defaults.

Step 2 Click the **Provisioning > Defaults** tabs.

Step 3 Click **Import**.

Step 4 If the correct file name and location of the desired file do not appear in the Import Defaults from File dialog box, click **Browse** and browse to the file you are importing.

Step 5 When the correct file name and location appear in the dialog box (the correct file name is 15454-defaults.txt if you are importing the factory defaults), click **OK**.

A pencil icon will appear next to any default value that will be changed as a result of importing the new defaults file.

Step 6 Click **Apply**.

Step 7 If the imported file fails to pass all edits, the problem field shows the first encountered problem default value that must be fixed. Change the problem default value and click **Apply**. Repeat until the imported file passes all edits successfully.

Step 8 If you are modifying node-level defaults, a dialog box appears telling you that applying defaults for node level attributes overrides current provisioning and asks if you want to continue. Click **Yes**.

If you are modifying the IIOP Listener Port setting, a dialog box appears warning you that the node will reboot and asks if you want to continue. Click **Yes**.

Note Changes to most node defaults reprovision the node when you click Apply. Changes made to card settings using the Defaults Editor do not change the settings for cards that are already installed or slots that are preprovisioned for cards, but rather, change only cards that are installed or preprovisioned thereafter. To change settings for installed cards or preprovisioned slots, see Chapter 10, "Change Card Settings."

Note Changing some NE defaults can cause CTC disconnection or a reboot of the node in order for the default to take effect. Before you change a default, view the Side Effects column of the Defaults editor (right-click a column header and select **Show Column > Side Effects**) and be prepared for the occurrence of any side effects listed for that default.

Stop. You have completed this procedure.

NTP-A338 Export Network Element Defaults

Purpose	This procedure exports the NE defaults using the NE Defaults Editor. The exported defaults can be imported to other nodes.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note The defaults currently displayed are exported whether or not they have been applied to the current node.

Note The NE defaults can also be exported from the File > Export menu. These exported defaults are for reference only and cannot be imported.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to export NE defaults.

Step 2 Click the **Provisioning > Defaults** tabs.

Step 3 Click **Export**.

Step 4 If the desired file to export to does not appear in the Export Defaults to File dialog box (or does not yet exist) click **Browse** and browse to the directory where you want to export the data; then either choose or type in (to create) the file to export to [the defaults will be exported as a text file delimited by equals (=) signs].

Step 5 Click **OK**.

Stop. You have completed this procedure.

NTP-A356 Test DS1/E1-56 and DS3XM-12 Electrical Card Ports

Purpose	This procedure tests DS1/E1-56 and DS3XM-12 electrical IO card ports.
Tools/Equipment	None
Prerequisite Procedures	"DLP-A60 Log into CTC" task on page 17-60 and "DLP-A230 Change a Circuit Service State" task on page 19-19.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to perform Bit Error Rate Testing (BERT).

Note The ports must be in OOS-MT state before enabling BERT. For more information on setting the service state of the circuit, see "DLP-A230 Change a Circuit Service State" task on page 19-19.

Step 2 Go to the card view for the card you want to test.

Step 3 Click the **Maintenance > BERT** tabs.

Step 4 To enable BERT on the DS1/E1-56 cards, choose one of the following options from the TPGM-Selection drop-down list:

- TPGM-L—Enables the test pattern generation and monitoring on the line side.
- TPGM-B—Enables the test pattern generation and monitoring on the backplane side. You can enable TPGM-B on a port only if that port has a bidirectional circuit.
- None—Disables the BERT mode.

Go to Step 7.

Step 5 To change the test pattern from Test Pattern Generator and Monitor-Line (TPGM-L) to Test Pattern Generator and Monitor-Backplane (TPGM-B) or vice versa, choose the following options from the TPGM-Selection drop-down list in a sequence:

- None—Stops the previous test pattern that is executed.
- TPGM-L or TPGM-B—Enables the test pattern generation and monitoring on the line side or the backplane side.

Go to Step 7.

Step 6 To enable BERT on the DS3XM-12 cards, select the **DS1** or **DS3** tab. From the TPGM-Selection drop-down list, choose the required option:

- (Only DS1) TPGM-B—Enables test pattern generation and monitoring on the backplane side. You can enable TPGM-B on a port only if that port has a bidirectional circuit.
- (Only DS3) TPGM-L—Enables test pattern generation and monitoring on the line side.
- None—Disables the BERT mode.

Go to Step 7.

Note While reverting CTC to a version lower than Release 8.5, disable BERT on the DS3XM-12 cards.

Step 7 Choose a test pattern from the drop-down list. The available test patterns are PRBS15, PRBS20, PRBS23, QRSS, and ALT1s0s (alternating ones and zeroes).

Note When testing with PRBS15 or PRBS23 BERT signals on the DS3XM-12 card, you need to set the PRBS pattern to inverted mode on test equipment that follow the ITU-T standard 0.150.

Step 8 Click **Apply**.

Step 9 Click the **Test Mode** subtab. In the test mode you can inject error bits and monitor the error count on the traffic running on a port.

Note You can inject errors only if the Synchronization Status is True.

The Synchronization Status column displays the connection status between the test pattern generator (TPG) and test pattern monitor (TPM). If the status is True, then synchronization between TPG and TPM conforms to the test pattern that is configured.

Step 10 Click **Inject Bit Errors**.

The Error Injection dialog appears.

Step 11 Select **Single Bit Error Injection** (single-error-injection mode) or errors at pre-defined error rates, such as, 1.0E-3, 1.0E-4, 1.0E-5, and 1.0E-6 (multirate-error-injection mode). To stop injecting errors in multirate-error-injection mode, click **Stop** in the Error Injection dialog box.

Stop. You have completed this procedure.

CHAPTER 16

Power Down the Node

This chapter explains how to power down a node and stop all node activity on the Cisco ONS 15454.

NTP-A114 Power Down the Node

Purpose	This procedure stops all node activity.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	For software steps, a provisioning level or higher is required. For hardware steps, any level is allowed.

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Caution The following procedure is designed to minimize traffic outages when powering down nodes, but traffic will be lost if you delete and recreate circuits that passed through a working node.

Caution Always use the supplied ESD wristband when working with the ONS 15454. Plug the wristband into the ESD jack located on the fan-tray assembly or on the lower right outside edge of the shelf on the NEBS 3 shelf assembly. To access the ESD plug on the NEBS 3 shelf assembly, open the front door of the ONS 15454. The front door is grounded to prevent electrical shock. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Step 1 Identify the node that you want to power down. If no cards are installed, go to Step 14. If cards are installed, log into the node. See the "DLP-A60 Log into CTC" task on page 17-60 for instructions.

Step 2 In node view, choose **Go to Network View** from the View menu.

Step 3 Verify that the node is not connected to a network.

a. If the node is part of a working network, log out of the node and complete the "NTP-A313 Remove an In-Service Node from a Linear ADM" procedure on page 14-18, the "NTP-A240 Remove a BLSR Node" procedure on page 14-7, or the "NTP-A294 Remove a Path Protection Node" procedure on page 14-13. If the node is part of a dense wavelength division multiplexing (DWDM) configuration, refer to the *Cisco ONS 15454 DWDM Procedure Guide*. Continue with Step 4.

b. If the node is not connected to a working network and the current configurations are no longer required, proceed to Step 4.

Note Current configurations will be saved if Steps 4 to 11 are skipped.

Step 4 In node view, click the **Circuits** tab and verify that no circuits appear, then proceed to Step 5. If circuits appear, complete the "NTP-A151 Modify and Delete Circuits" procedure on page 7-4 to delete all the circuits that originate or terminate in the node. Repeat until no circuits appear.

Step 5 Complete the "NTP-A203 Modify or Delete Card Protection Settings" procedure on page 11-5 to delete any optical protection group. Repeat until no optical protection groups remain.

Step 6 Complete the "DLP-A156 Delete a Section DCC Termination" task on page 18-24 or the "DLP-A359 Delete a Line DCC Termination" task on page 20-45 for all ports. Repeat until no SDCC or LDCC terminations remain.

Step 7 Complete the "DLP-A214 Change the Service State for a Port" task on page 19-9 to change all ports to the Out-of-Service and Management,Disabled (OOS-MA,DSBLD) service state.

Note Refer to the *Cisco ONS 15454 DWDM Procedure Guide* for information regarding DWDM cards.

Step 8 Remove all fiber connections to the cards.

Step 9 Complete the "DLP-A470 Remove GBIC or SFP/XFP Devices" task on page 21-62 if there are any devices installed.

Warning **Class 1 laser product.** Statement 1008

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 1051

Step 10 In node view, right-click an installed card and choose **Delete Card**.

Step 11 Click **Yes**.

Step 12 After you have deleted the cards, open the card ejectors for each card and remove each card from the node.

Note You cannot delete a TCC2 or TCC2P card in Cisco Transport Controller (CTC). Physically remove it after all the other cards have been deleted and removed.

Step 13 Store all the cards you removed and update inventory records according to local site practice.

Step 14 Shut off the power from the power supply that feeds the node.

Step 15 Disconnect the node from its external fuse source.

Stop. You have completed this procedure.

CHAPTER 17

DLPs A1 to A99

Note The terms “Unidirectional Path Switched Ring” and “UPSR” may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as “Path Protected Mesh Network” and “PPMN,” refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

DLP-A1 Unpack and Verify the Shelf Assembly

Purpose	This task removes the shelf assembly from the package.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 When you receive the ONS 15454 system equipment at the installation site, open the top of the box. The Cisco Systems logo designates the top of the box.

Step 2 Remove the foam inserts from the box. The box contains the 15454 shelf (wrapped in plastic) and a smaller box of items needed for installation.

Step 3 To remove the shelf, grasp both rings of the shelf removal strap and slowly lift the shelf out of the box.

Step 4 Open the smaller box of installation materials, and verify that you have all items listed in the “Cisco-Supplied Materials” section on page 1-2.

Note The fan-tray assembly is shipped separately.

Step 5 Return to your originating procedure (NTP).

DLP-A2 Inspect the Shelf Assembly

Purpose	This task verifies that all parts of the shelf assembly are in good condition.
Tools/Equipment	Pinned hex (Allen) key for front door
Prerequisite Procedures	DLP-A1 Unpack and Verify the Shelf Assembly, page 17-1
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Open the shelf using the pinned hex key. For more information, see the "DLP-A8 Open the Front Door" task on page 17-8.

Step 2 Verify the following:

- The pins are not bent or broken.
- The frame is not bent.

Step 3 If the pins are bent or broken or the frame is bent, call your Cisco sales engineer for a replacement.

Step 4 Close the front door before installing.

Step 5 Return to your originating procedure (NTP).

DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack

Purpose	This task installs the mounting bracket to convert a 23-inch (584.2 mm) rack to a 19-inch (482.6 mm) rack.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution Use only the fastening hardware provided with the ONS 15454 to prevent loosening, deterioration, and electromechanical corrosion of the hardware and joined material.

Caution When mounting the ONS 15454 in a frame with a nonconductive coating (such as paint, lacquer, or enamel) either use the thread-forming screws provided with the ONS 15454 shipping kit, or remove the coating from the threads to ensure electrical continuity.

Step 1 Remove the screws that attach the mounting bracket to the side of the shelf assembly.

Step 2 Flip the detached mounting bracket upside down.

Text imprinted on the mounting bracket will now also be upside down.

Step 3 Place the widest side of the mounting bracket flush against the shelf assembly (see Figure 17-1).

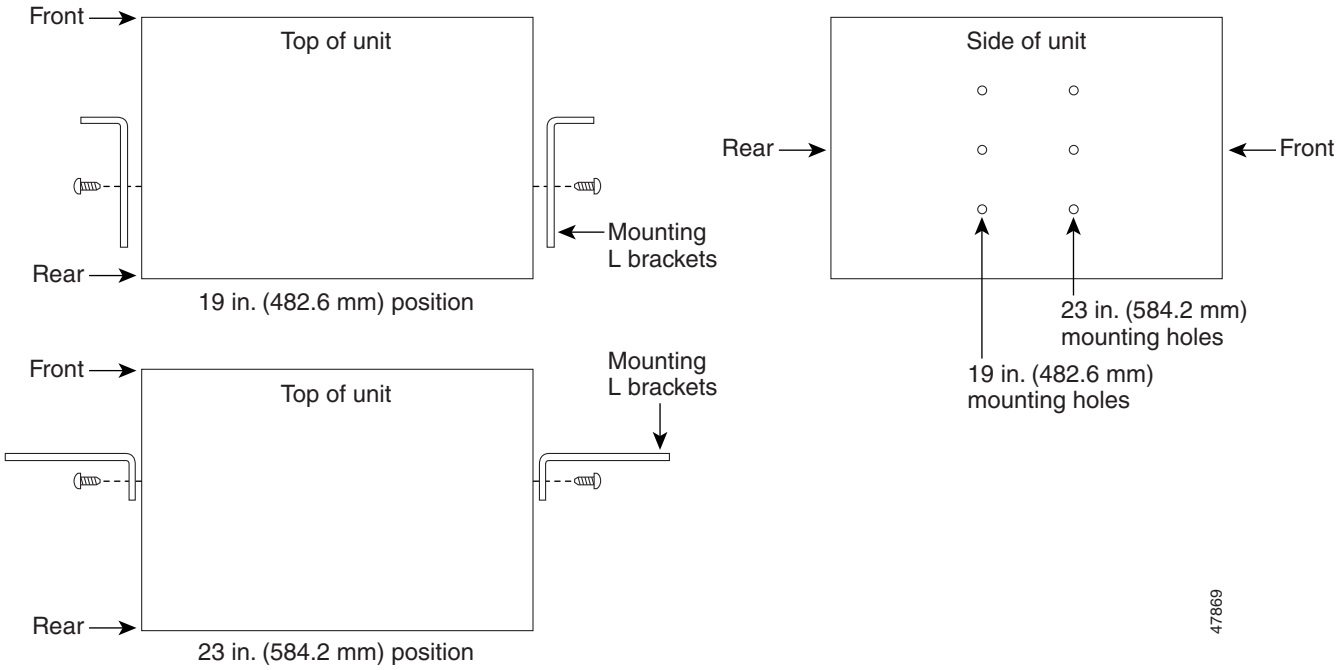
The narrow side of the mounting bracket should be towards the front of the shelf assembly. Text imprinted on the mounting bracket should be visible and upside down.

Step 4 Align the mounting bracket screw holes against the shelf assembly screw holes.

Step 5 Insert the screws that were removed in Step 1 and tighten them.

Step 6 Repeat the task for the mounting bracket on the opposite side.

Figure 17-1 Reversing the Mounting Brackets (23-inch [584.2-mm] Position to 19-inch [482.6-mm] Position



Step 7 Return to your originating procedure (NTP).

DLP-A4 Install the External Brackets and Air Filter

Purpose	This task installs the external brackets and air filter on the bottom of the shelf rather than below the fan-tray assembly. Installing the external brackets and air filter on the bottom of the shelf enables access to the air filter without removing the fan-tray assembly.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack, page 17-2, if applicable
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note If you choose not to install the brackets, install the air filter by sliding it into the compartment at the bottom of the shelf assembly. Each time you remove and reinstall the air filter in the future, you must first remove the fan-tray assembly. Do not install an air filter in both filter locations on any shelf assembly.

Note To install the air filter inside the air ramp unit (15454E-AIR-RAMP or 15454-AIR-RAMP), use the ETSI version of the air filter (15454-FTF2 or 15454E-FTF4).

Step 1 With the fan-tray assembly removed, place the ONS 15454 facedown on a flat surface.

Note Although the filter will work if it is installed with either side facing up, Cisco recommends that you install it with the metal bracing facing up to preserve the surface of the filter.

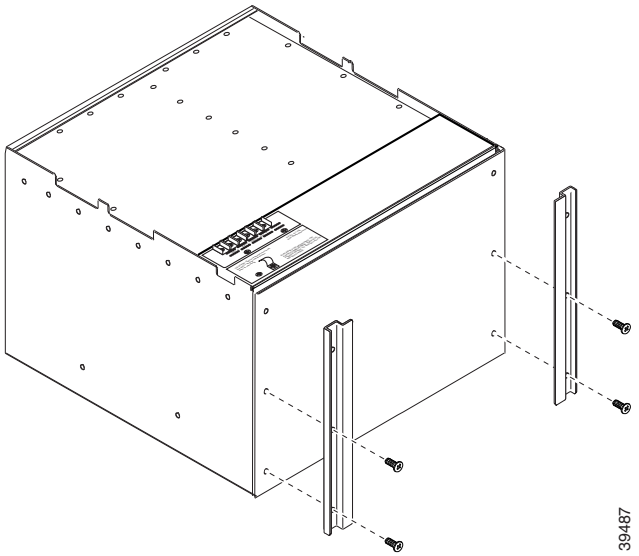
Step 2 Locate the three screw holes that run along the left and right sides of the bottom of the shelf assembly.

Step 3 Secure each bracket to the bottom of the shelf assembly using the screws (48-0003) provided in the backplane standoff kit (53-0795-XX).

Each bracket has a filter stopper and a flange on one end. Make sure to attach the brackets with the stoppers and flanges facing the rear of the shelf assembly (the top, if the ONS 15454 is facedown during installation).

Figure 17-2 illustrates bottom bracket installation. If you do not use the brackets, in the future you must remove the fan-tray assembly before removing the air filter. The brackets enable you to clean and replace the air filter without removing the fan-tray assembly.

Figure 17-2 Installing the External Brackets



Step 4 Slide the air filter into the shelf assembly.

Step 5 Return to your originating procedure (NTP).

DLP-A5 Mount the Shelf Assembly in a Rack (One Person)

Purpose	This task allows one person to mount the shelf assembly in a rack.
Tools/Equipment	Pinned hex tool Two set screws (48-1003-XX) Eight pan-head Phillips mounting screws (48-1004-XX, 48-1007-XX) #2 Phillips screwdriver
Prerequisite Procedures	DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack, page 17-2, if applicable DLP-A4 Install the External Brackets and Air Filter, page 17-4, if applicable
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify that the proper fuse and alarm panel has been installed in the top mounting space. If a fuse and alarm panel has not been installed, you must install one according to manufacturer's instructions.

- If installing the 15454-SA-ANSI or 15454-SA-HD shelf assembly, a 100-A fuse panel (30-A fuse per shelf minimum) is required.
- If installing the 15454-SA-NEBS3 shelf assembly, a standard 80-A fuse panel (20-A fuse per shelf minimum) is required.

Step 2 Ensure that the shelf assembly is set for the desired rack size (either 23 inches [584.2 mm] or 19 inches [482.6 mm]).

Step 3 Using the hex tool that shipped with the assembly, install the two set screws into the screw holes that will not be used to mount the shelf. Let the screws protrude sufficiently to hold the mounting bracket.

Step 4 Lift the shelf assembly to the desired rack position and set it on the set screws.

Step 5 Align the screw holes on the mounting bracket with the mounting holes in the rack.

Step 6 Using the Phillips screwdriver, install one mounting screw in each side of the assembly.

Step 7 When the shelf assembly is secured to the rack, install the remaining mounting screws.

Note Use at least one set of the horizontal screw slots on the ONS 15454 to prevent slippage.

Step 8 Using the hex tool, remove the temporary set screws.

Step 9 Return to your originating procedure (NTP).

DLP-A6 Mount the Shelf Assembly in a Rack (Two People)

Purpose	This task allows two people to mount the shelf assembly in a rack.
Tools/Equipment	Pinned hex tool Two set screws (48-1003-XX) Eight pan-head Phillips mounting screws (48-1004-XX, 48-1007-XX) #2 Phillips screwdriver
Prerequisite Procedures	DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack, page 17-2, if applicable DLP-A4 Install the External Brackets and Air Filter, page 17-4, if applicable
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify that the proper fuse and alarm panel has been installed in the top mounting space. If a fuse and alarm panel is not present, you must install one according to manufacturer's instructions.

- If installing the 15454-SA-ANSI or 15454-SA-HD shelf assembly, a 100-A fuse panel (30-A fuse per shelf minimum) is required.
- If installing the 15454-SA-NEBS3 shelf assembly, a standard 80-A fuse panel (20-A fuse per shelf minimum) is required.

Step 2 Ensure that the shelf assembly is set for the desired rack size (either 23 inches [584.2 mm] or 19 inches [482.6 mm]).

Step 3 Using the hex tool that shipped with the shelf assembly, install the two set screws (48-1003-XX) into the screw holes that will not be used to mount the shelf. Let the set screws protrude sufficiently to hold the mounting brackets.

Step 4 Lift the shelf assembly to the desired position in the rack.

Step 5 Align the screw holes on the mounting brackets with the mounting holes in the rack.

Step 6 While one person holds the shelf assembly in place, the other person can install one mounting screw in each side of the assembly using the Phillips screwdriver.

Step 7 When the shelf assembly is secured to the rack, install the remaining mounting screws.

Note Use at least one set of the horizontal screw slots on the ONS 15454 to prevent slippage.

Step 8 Using the hex tool, remove the temporary set screws.

Step 9 Return to your originating procedure (NTP).

DLP-A7 Mount Multiple Shelf Assemblies in a Rack

Purpose	This task allows multiple shelves to be assembled in a rack.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack, page 17-2, if applicable DLP-A4 Install the External Brackets and Air Filter, page 17-4, if applicable
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note The ONS 15454 must have one inch (25.4 mm) of airspace below the installed shelf assembly to allow air flow to the fan intake. If a second ONS 15454 is installed underneath a shelf assembly, the air ramp on top of the bottom shelf assembly provides the desired space. However, if the ONS 15454 is installed above third-party equipment, you must provide a minimum spacing of one inch (25.4 mm) between the third-party shelf assembly and the bottom of the ONS 15454. The third-party equipment must not vent heat upward into the ONS 15454.

Step 1 Verify that the proper fuse and alarm panel has been installed in the top mounting space. If a fuse and alarm panel is not present, you must install one according to manufacturer's instructions.

- If installing the 15454-SA-ANSI or 15454-SA-HD shelf assembly, a 100-A fuse panel (30-A fuse per shelf minimum) is required.
- If installing the 15454-SA-NEBS3 shelf assembly, a standard 80-A fuse panel (20-A fuse per shelf minimum) is required.

Step 2 Mount the first ONS 15454 directly below the fuse and alarm panel using the "DLP-A5 Mount the Shelf Assembly in a Rack (One Person)" task on page 17-5 or the "DLP-A6 Mount the Shelf Assembly in a Rack (Two People)" task on page 17-6.

Step 3 Repeat the task with the remaining shelves.

Step 4 Return to your originating procedure (NTP).

DLP-A8 Open the Front Door

Purpose	This task describes how to open the front cabinet compartment door.
Tools/Equipment	Pinned hex key
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Caution The ONS 15454 has an ESD plug input and is shipped with an ESD wrist strap. The ESD plug input is located on the outside edge of the shelf assembly on the right-hand side. It is labeled “ESD” on the top and bottom. Always wear an ESD wrist strap and connect the strap to the ESD plug when working on the ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

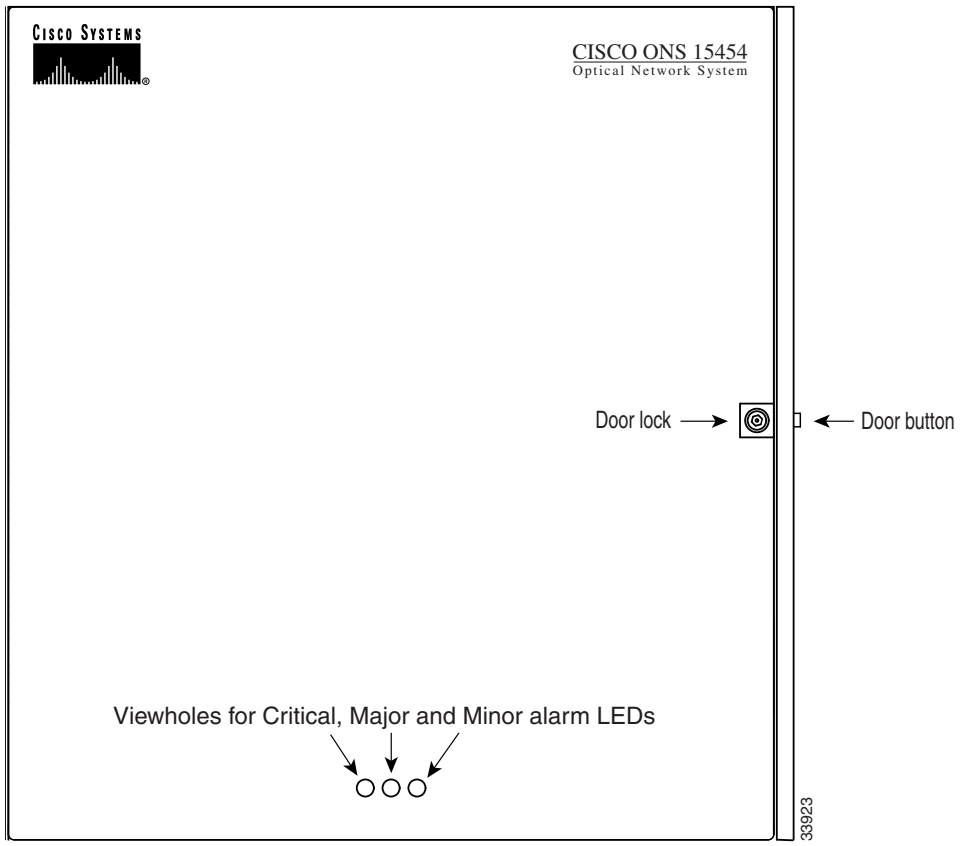
Step 1 Open the front door lock (Figure 17-3).

The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.

Step 2 Press the door button to release the latch.

Step 3 Swing the door open.

Figure 17-3 Cisco ONS 15454 Front Door



Step 4 Return to your originating procedure (NTP).

DLP-A9 Remove the Front Door

Purpose	This task removes the front cabinet compartment door.
Tools/Equipment	Open-end wrench
Prerequisite Procedures	DLP-A8 Open the Front Door, page 17-8
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

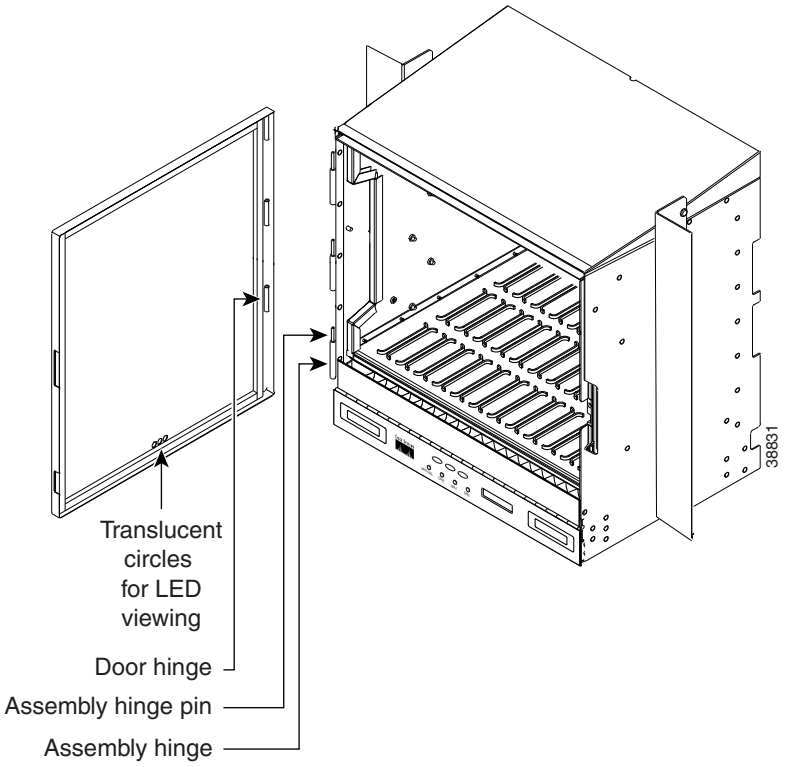
Step 1 To remove the door ground strap (available in Release 3.3 and later), perform the following:

a. To detach the ground strap from the front door, loosen the #6kepnut (49-0600-01) using the open-end wrench. Detach the end of the ground strap terminal lug (72-3622-01) from the male stud on the inside of the door.

b. To detach the other end of the ground strap from the longer screw on the fiber guide, loosen the #4 kepnut (49-0337-01) on the terminal lug using the open-end wrench. Remove the terminal lug and lock washer.

Step 2 Lift the door from its hinges at the top left corner of the door (Figure 17-4).

Figure 17-4 Removing the ONS 15454 Front Door



Step 3 Return to your originating procedure (NTP).

DLP-A10 Remove the Lower Backplane Cover

Purpose	This task removes the lower backplane cover.
Tools/Equipment	#2 Phillips screwdriver
	Medium slot-head screwdriver
	Small slot-head screwdriver
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Unscrew the five retaining screws that hold the cover in place.

Step 2 Grasp the cover on each side.

Step 3 Gently pull the cover away from the backplane.

Step 4 Return to your originating procedure (NTP).

DLP-A11 Remove the Backplane Sheet Metal Cover

Purpose	This task removes the backplane sheet metal cover that is installed on the backplane when EIAs are not installed.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	DLP-A10 Remove the Lower Backplane Cover, page 17-10
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 To remove the backplane sheet metal cover, loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.

Step 2 Loosen the nine perimeter screws that hold the backplane sheet metal cover(s) in place.

Step 3 Lift the panel by the bottom to remove it from the shelf assembly.

Step 4 Store the panel for later use. Attach the backplane cover(s) whenever EIA(s) are not installed.

Step 5 Return to your originating procedure (NTP).

DLP-A12 Install a BNC or High-Density BNC EIA

Purpose	This task installs a BNC or high-density BNC EIA. Use this task if you are using DS3-12, DS3XM-6, or EC-1 cards and prefer a BNC interface to an SMB interface.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Perimeter screws (9) Inner screws (12) Backplane cover screws (5) BNC or high-density BNC card
Prerequisite Procedures	NTP-A4 Remove the Backplane Covers, page 1-7
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Remove the BNC or high-density BNC card from the packaging. Line up the connectors on the card with the mating connectors on the backplane. Gently push the card until both sets of connectors fit together snugly.

Step 2 Place the metal EIA panel over the card.

Step 3 Insert and tighten the nine perimeter screws (P/N 48-0358) at 8 to 10 lb (3.6 to 4.5 kg) to secure the cover panel to the backplane.

Step 4 Insert and tighten the twelve (BNC) or nine (high-density BNC) inner screws (P/N 48-0004) at 8 to 10 lb (3.6 to 4.5 kg) to secure the cover panel to the card and backplane.

Figure 17-5 shows a BNC EIA installation.

Figure 17-5 Installing the BNC EIA

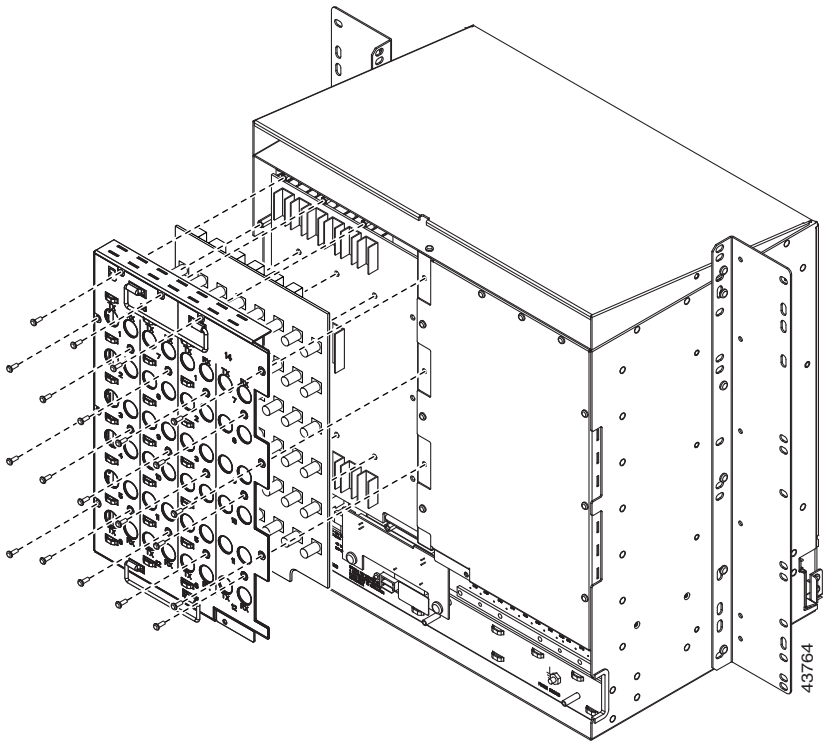
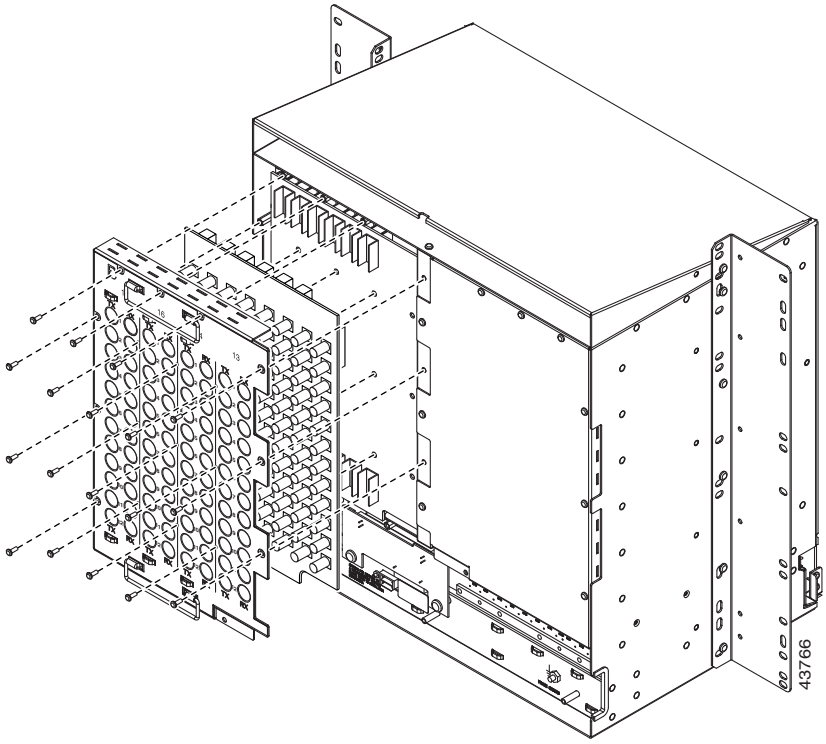


Figure 17-6 shows high-density BNC EIA installation.

Figure 17-6 Installing the High-Density BNC EIA



Step 5 Return to your originating procedure (NTP).

DLP-A13 Install an SMB EIA

Purpose	This task installs an SMB EIA. Use the SMB EIA if you are using DS1-14 cards and prefer an SMB interface to an AMP interface, or if you are using DS3-12, DS3XM-6, or EC-1 cards and prefer an SMB interface to a BNC interface.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver 9 perimeter screws 12 inner screws 5 backplane cover screws SMB card Foil EMI gasket (might already be installed on some SMB EIA assemblies) Metal SMB cover panel
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Remove the SMB card from the packaging. Line up the connectors on the card with the mating connectors on the backplane. Gently push the card until both sets of connectors fit together snugly.

Step 2 Place the foil EMI gasket over the SMB card so that the holes in the foil EMI gasket line up with the SMB connectors.

Caution The foil EMI gasket might ship already installed on the SMB EIA assembly. If it is not, you must install it to meet electromagnetic interference (EMI) guidelines.

Step 3 Place the metal SMB cover panel over the card.

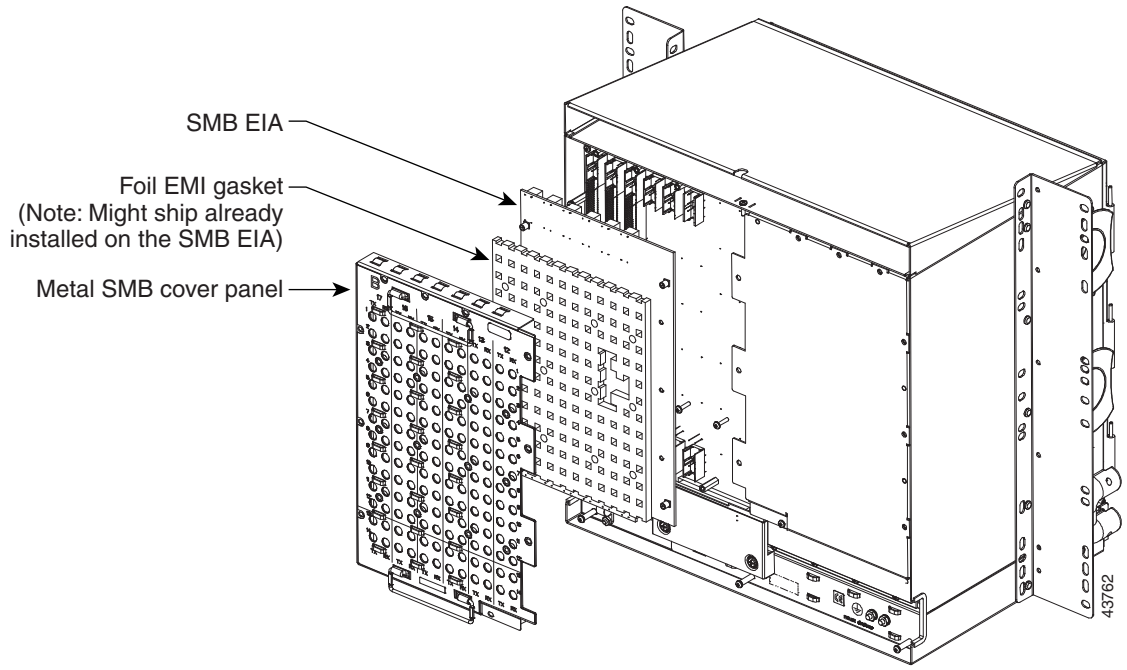
Step 4 Insert and tighten the twelve inner screws (P/N 48-0004) at 8 to 10 lb (3.6 to 4.5 kg) to secure the cover panel to the card and backplane.

Step 5 Insert and tighten the nine perimeter screws (P/N 48-0358) at 8 to 10 lb (3.6 to 4.5 kg) to secure the cover panel to the backplane.

If you are using SMB EIAs to make DS-1 connections, you need the DS-1 electrical interface adapter, commonly referred to as a balun (P/N 15454-WW-14=).

Figure 17-7 shows an SMB EIA installation.

Figure 17-7 Installing the SMB EIA (Use a Balun for DS-1 Connections)



Step 6 Return to your originating procedure (NTP).

DLP-A14 Install the AMP Champ EIA

Purpose	This task installs an AMP Champ EIA. Use an AMP Champ EIA if you are using DS1-14 cards and prefer an AMP interface to an SMB interface.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver 9 perimeter screws 12 inner screws 5 backplane cover screws 6 AMP Champ cards EIA panel
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Align the AMP Champ panel with the backplane and insert and tighten the nine perimeter screws (P/N 48-0358) at 8 to 10 lb (3.6 to 4.5 kg).

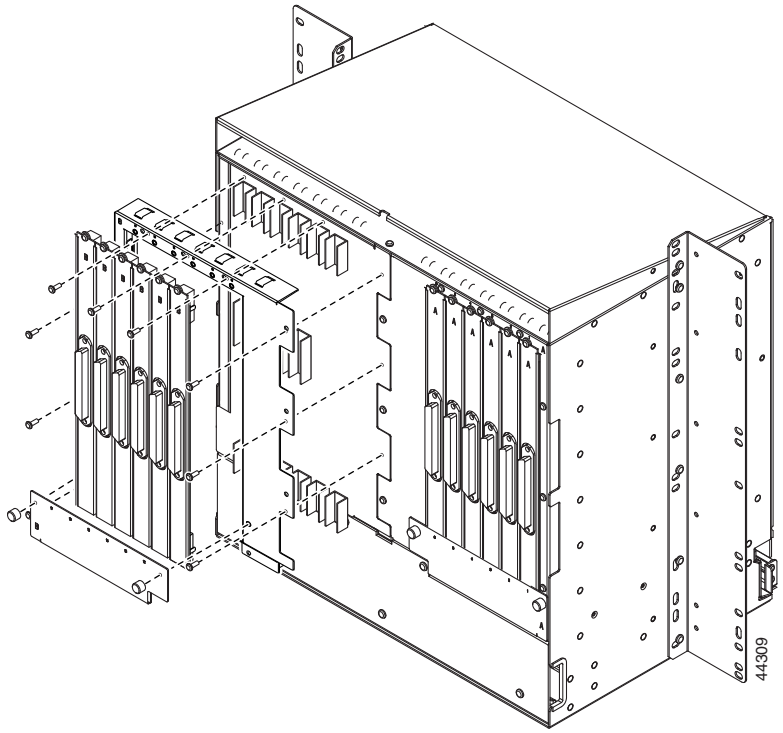
Step 2 Align an AMP Champ card with the backplane connector and push until it fits snugly. Repeat until you have installed all six AMP Champ cards.

Step 3 To secure each AMP Champ card to the cover panel, insert and tighten a screw (P/N 48-0003) at the top of each card at 8 to 10 lb (3.6 to 4.5 kg).

Step 4 Place the AMP Champ fastening plate along the bottom of the cover panel, and hand-tighten the two thumbscrews.

Figure 17-8 shows an AMP Champ EIA installation.

Figure 17-8 Installing the AMP Champ EIA



Step 5 Return to your originating procedure (NTP).

DLP-A17 Connect Office Power to the ONS 15454 Shelf

Purpose	This task connects power to the ONS 15454 shelf.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Wire cutters Wire strippers Crimp tool Fuse panel Power cable (from fuse and alarm panel to assembly), #10 AWG, copper conductors, 194 degrees F [90 degrees C]) Ground cable #6 AWG stranded
Prerequisite Procedures	Connect the chassis to the office ground. For detailed instructions on grounding the chassis, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **When installing or replacing the unit, the ground connection must always be made first and disconnected last.** Statement 202

Note The battery return connection is treated as DC-I, as defined in Telcordia GR-1089-CORE Issue 4 and 5.

Note If the system loses power or both TCC2/TCC2P cards are reset and the system is not provisioned to get the time from a Network Time Protocol/Simple Network Time Protocol (NTP/SNTP) server, you must reset the ONS 15454 clock. After powering down, the date defaults to January 1, 1970, 00:04:15. To reset the clock, see the "NTP-A25 Set Up Name, Date, Time, and Contact Information" procedure on page 4-5. If you are using the TCC2/TCC2P cards, the system clock will be kept running for up to three hours. In this case, no action would be required.

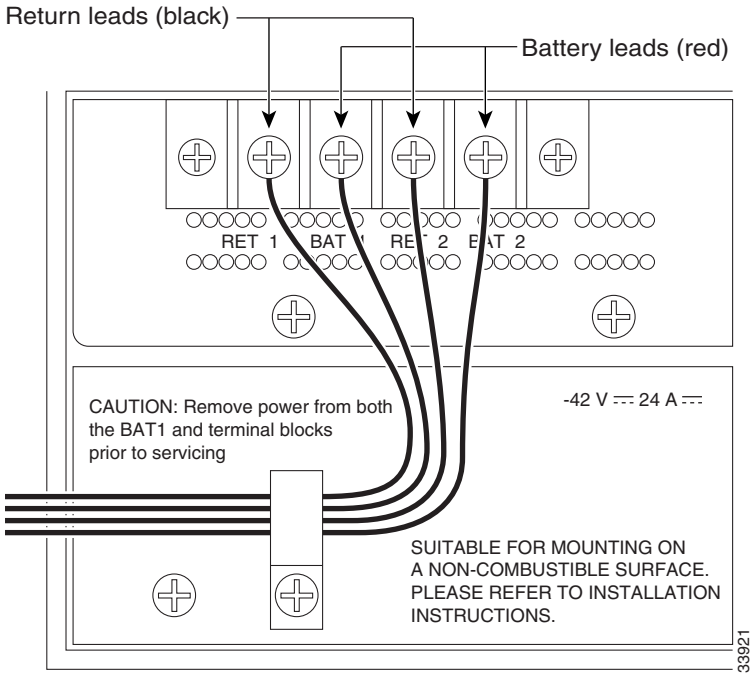
Note If you encounter problems with the power supply, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 1 Connect the office power according to the fuse panel engineering specifications.

Step 2 Measure and cut the cables as needed to reach the ONS 15454 from the fuse panel. Figure 17-9 shows the ONS 15454 power terminals.

Step 3 Dress the power cabling according to local site practice.

Figure 17-9 Cisco ONS 15454 Power Terminals



Step 4 Remove or loosen the #8 power terminal screws on the ONS 15454. To avoid confusion, label the cables connected to the BAT1/RET1 (A) power terminals as 1, and the cables connected to the BAT2/RET2 (B) power terminals as 2.

Note Use only pressure terminal connectors, including ring, fork, and dual-lug types, when terminating the battery, battery return, and frame ground conductors.

Caution Before you make any crimp connections, coat all bare conductors (battery, battery return, and frame ground) with an appropriate antioxidant compound. Bring all unplated connectors, braided strap, and bus bars to a bright finish, then coat with an antioxidant before you connect them. You do not need to prepare tinned, solder-plated, or silver-plated connectors and other plated connection surfaces, but always keep them clean and free of contaminants.

Caution When terminating power, return, and frame ground, do not use soldering lug, screwless (push-in) connectors, quick-connect, or other friction-fit connectors.

Step 5 Strip 1/2 inch (12.7 mm) of insulation from all power cables that you will use.

Step 6 Crimp the lugs onto the ends of all power leads.

Note When terminating battery and battery return connections as shown in Figure 17-9, follow a torque specification of 10 in-lb.

Step 7 Terminate the return 1 lead to the RET1 backplane terminal. Use oxidation-prevention grease to keep connections noncorrosive.

Step 8 Terminate the negative 1 lead to the negative BAT1 backplane power terminal. Use oxidation prevention grease to keep connections noncorrosive.

Step 9 If you use redundant power leads, terminate the return 2 lead to the positive RET2 terminal on the ONS 15454. Terminate the negative 2 lead to the negative BAT2 terminal on the ONS 15454. Use oxidation-preventative grease to keep connections noncorrosive.

Note The configured ONS 15454 shelf can work with a single power line since the ONS 15454 power configuration offers redundancy. When using the 15454-FTA3 fan tray, if the ONS15454 shelf is powered by a single power line, the BAT-FAIL alarm appears, the fans run at a maximum speed, and the system does not comply with NEBS GR-63 Issue 3 and GR-1089 Issue 4 and 5 requirements. In order to meet the above mentioned NEBS requirements, the ONS 15454 shelf must be powered by both the DC power lines.

Step 10 Route the cables out below the power terminals using the plastic cable clamp, as shown in Figure 17-9 on page 17-19.

Step 11 Connect the return cables to earth ground at power supply side.

Step 12 Return to your originating procedure (NTP).

DLP-A18 Turn On and Verify Office Power

Purpose	This task measures the power to verify correct power and returns.
Tools/Equipment	Voltmeter
Prerequisite Procedures	Connect the chassis to the office ground. For detailed instructions on grounding the chassis, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide. DLP-A17 Connect Office Power to the ONS 15454 Shelf, page 17-18
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Using a voltmeter, verify the office battery and ground at the following points on the fuse and alarm panel:

a. To verify the power, place the black test lead of the voltmeter to the frame ground. Place the red test lead on the A-side connection and verify that it is between –40.5 VDC and –57 VDC. Place the red test lead on the B-side connection and verify that it is between –40.5 VDC and –57 VDC.

Note The minimum and maximum voltages required to power the chassis are –40.5 VDC and –57 VDC respectively. The nominal voltage value is -48.0V.

b. To verify the ground, place the black test lead of the voltmeter to the frame ground. Place the red test lead on the A-side return ground and verify that no voltage is present. The voltmeter must read 0 VDC. Place the red test lead on the B-side return ground and verify that no voltage is present. The voltmeter must read 0 VDC.

Step 2 Complete one of the following to power up the node:

- If you are using a 80-A fuse panel, insert a 20-A fuse into the fuse position according to site practice.
- If you are using a 100-A fuse panel, insert a 30-A fuse into the fuse position according to site practice.

Step 3 Return to your originating procedure (NTP).

DLP-A19 Install Alarm Wires on the Backplane

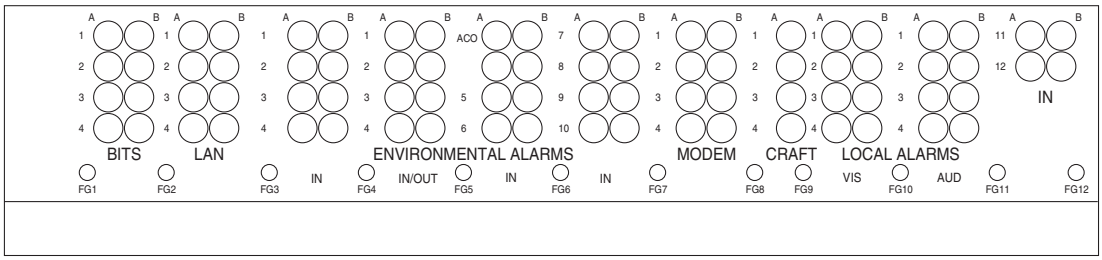
Purpose	This task installs alarm wires on the backplane so that you can provision external (environmental) alarms and controls with the Alarm Interface Controller–International (AIC-I) card. If you are using the alarm extension panel (AEP), do not perform this task.
Tools/Equipment	Wire wrapper #22 or #24 AWG (0.51 mm² or 0.64 mm²) wires 100-ohm shielded building integrated timing supply (BITS) clock cable pair #22 or #24 AWG (0.51 mm² or 0.64 mm²), twisted-pair T1-type
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Using 100-ohm shielded BITS clock cable pair #22 or #24 AWG (0.51 mm² or 0.64 mm²) twisted-pair T1-type wires, wrap the alarm wires on the appropriate wire-wrap pins according to local site practice. Ground the shield of the BITS Input cable at the BITS end. For BITS Output, wrap the ground shield of the BITS cable to the frame ground pin (FG1) located below the column of BITS pins.

Figure 17-10 shows alarm pin assignments for the AIC-I in the Release 3.4 or higher ONS 15454 backplane.

Note The AIC-I requires a shelf assembly running Software Release 3.4.0 or later. The backplane of the ANSI shelf contains a wire-wrap field with pin assignment according to the layout in Figure 17-10. The shelf assembly might be an existing shelf that has been upgraded to R3.4 or later. In this case, the backplane pin labeling will appear as indicated in Figure 17-12 on page 17-23, but you must use the pin assignments provided by the AIC-I as shown in Figure 17-10.

Figure 17-10 Cisco ONS 15454 Backplane Pinouts (Release 3.4 or Later)



Field	Pin	Function
BITS	A1	BITS Output 2 negative (–)
	B1	BITS Output 2 positive (+)
	A2	BITS Input 2 negative (–)
	B2	BITS Input 2 positive (+)
	A3	BITS Output 1 negative (–)
	B3	BITS Output 1 positive (+)
	A4	BITS Input 1 negative (–)
	B4	BITS Input 1 positive (+)
LAN	Connecting to a hub, or switch	
	A1	RJ-45 pin 6 RX–
	B1	RJ-45 pin 3 RX+
	A2	RJ-45 pin 2 TX–
	B2	RJ-45 pin 1 TX+
	Connecting to a PC/Workstation or router	
	A1	RJ-45 pin 2 RX–
	B1	RJ-45 pin 1 RX+
	A2	RJ-45 pin 6 TX–
	B2	RJ-45 pin 3 TX+
ENVIR ALARMS IN	A1	Alarm input pair number 1: Reports closure on connected wires.
	B1	
	A2	Alarm input pair number 2: Reports closure on connected wires.
	B2	
	A3	Alarm input pair number 3: Reports closure on connected wires.
	B3	
	A4	Alarm input pair number 4: Reports closure on connected wires.
	B4	
	A5	Alarm input pair number 5: Reports closure on connected wires.
	B5	
	A6	Alarm input pair number 6: Reports closure on connected wires.
	B6	
	A7	Alarm input pair number 7: Reports closure on connected wires.
	B7	
	A8	Alarm input pair number 8: Reports closure on connected wires.
	B8	
	A9	Alarm input pair number 9: Reports closure on connected wires.
	B9	
	A10	Alarm input pair number 10: Reports closure on connected wires.
	B10	
	A11	Alarm input pair number 11: Reports closure on connected wires.
	B11	
	A12	Alarm input pair number 12: Reports closure on connected wires.
	B12	

Field	Pin	Function
ENVIR ALARMS IN/OUT N/O	A1/A13	Normally open output pair number 1
	B1/B13	
	A2/A14	Normally open output pair number 2
	B2/B14	
	A3/A15	Normally open output pair number 3
	B3/B15	
	A4/A16	Normally open output pair number 4
	B4/B16	
ACO	A1	Normally open ACO pair
	B1	
CRAFT	A1	Receive (PC pin #2)
	A2	Transmit (PC pin #3)
	A3	Ground (PC pin #5)
	A4	DTR (PC pin #4)
LOCAL ALARMS AUD (Audible) N/O	A1	Alarm output pair number 1: Remote audible alarm.
	B1	
	A2	Alarm output pair number 2: Critical audible alarm.
	B2	
	A3	Alarm output pair number 3: Major audible alarm.
	B3	
	A4	Alarm output pair number 4: Minor audible alarm.
	B4	
LOCAL ALARMS VIS (Visual) N/O	A1	Alarm output pair number 1: Remote visual alarm.
	B1	
	A2	Alarm output pair number 2: Critical visual alarm.
	B2	
	A3	Alarm output pair number 3: Major visual alarm.
	B3	
	A4	Alarm output pair number 4: Minor visual alarm.
	B4	

If you are using an AIC-I card, contacts provisioned as OUT are 1-4. Contacts provisioned as IN are 13-16.

83020

Figure 17-11 describes the environmental alarm pins on the backplane for Release 3.4 or later.

Figure 17-11 Highlighted Environmental Alarms

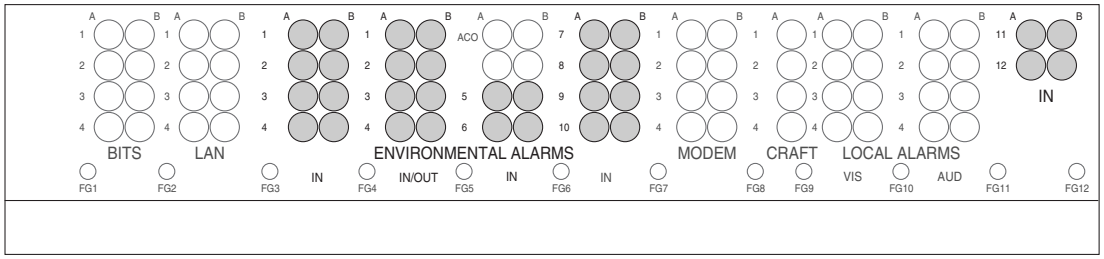
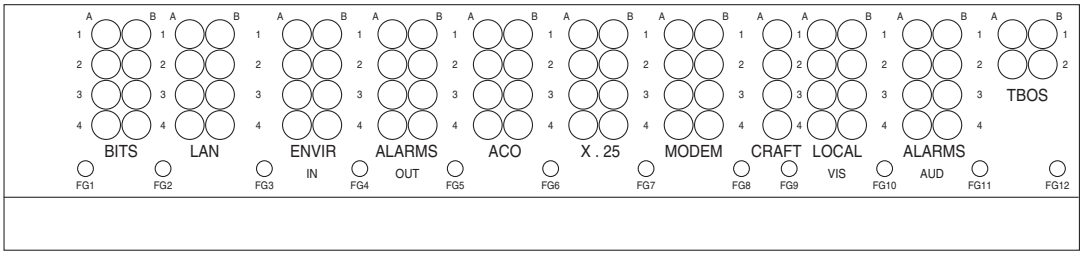


Figure 17-12 shows alarm pin assignments in a shelf for Release 3.3 and earlier. The AIC-I is incompatible with shelves Release 3.3 or earlier.

Figure 17-12 Cisco ONS 15454 Backplane Pinouts (Release 3.3 or Earlier)



Field	Pin	Function
BITS	A1	BITS Output 2 negative (-)
	B1	BITS Output 2 positive (+)
	A2	BITS Input 2 negative (-)
	B2	BITS Input 2 positive (+)
	A3	BITS Output 1 negative (-)
	B3	BITS Output 1 positive (+)
	A4	BITS Input 1 negative (-)
	B4	BITS Input 1 positive (+)
LAN	Connecting to a hub, or switch	
	A1	RJ-45 pin 6 RX-
	B1	RJ-45 pin 3 RX+
	A2	RJ-45 pin 2 TX-
	B2	RJ-45 pin 1 TX+
	Connecting to a PC/Workstation or router	
	A1	RJ-45 pin 2 RX-
	B1	RJ-45 pin 1 RX+
	A2	RJ-45 pin 6 TX-
	B2	RJ-45 pin 3 TX+
ENVIR ALARMS IN	A1	Alarm input pair number 1: Reports closure on connected wires.
	B1	
	A2	Alarm input pair number 2: Reports closure on connected wires.
	B2	
	A3	Alarm input pair number 3: Reports closure on connected wires.
	B3	
	A4	Alarm input pair number 4: Reports closure on connected wires.
	B4	

Field	Pin	Function
ENVIR ALARMS OUT N/O	A1	Normally open output pair number 1
	B1	
	A2	Normally open output pair number 2
	B2	
	A3	Normally open output pair number 3
	B3	
	A4	Normally open output pair number 4
	B4	
ACO	A1	Normally open ACO pair
	B1	
CRAFT	A1	Receive (PC pin #2)
	A2	Transmit (PC pin #3)
	A3	Ground (PC pin #5)
	A4	DTR (PC pin #4)
LOCAL ALARMS AUD (Audible) N/O	A1	Alarm output pair number 1: Remote audible alarm.
	B1	
	A2	Alarm output pair number 2: Critical audible alarm.
	B2	
	A3	Alarm output pair number 3: Major audible alarm.
	B3	
	A4	Alarm output pair number 4: Minor audible alarm.
	B4	
LOCAL ALARMS VIS (Visual) N/O	A1	Alarm output pair number 1: Remote visual alarm.
	B1	
	A2	Alarm output pair number 2: Critical visual alarm.
	B2	
	A3	Alarm output pair number 3: Major visual alarm.
	B3	
	A4	Alarm output pair number 4: Minor visual alarm.
	B4	

38533

Note The X.25, Modem, and TBOS pin fields are not active.

Step 2 Return to your originating procedure (NTP).

DLP-A20 Install Timing Wires on the Backplane

Purpose	This task installs the BITS timing wires on the backplane.
Tools/Equipment	Wire wrapper 100-ohm shielded BITS clock cable pair #22 or #24 AWG (0.51 mm² or 0.64 mm²), twisted-pair T1-type
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Using 100-ohm shielded BITS clock cable pair #22 or #24 AWG (0.51 mm² or 0.64 mm²), twisted-pair T1-type, wrap the clock wires on the appropriate wire-wrap pins according to local site practice.

Ground the shield of the BITS input cable at the BITS end. For BITS output, wrap the ground shield of the BITS cable to the frame ground pin (FG1) located beneath the column of BITS Pins. Table 17-1 lists the pin assignments for the BITS timing pin fields.

Table 17-1 External Timing Pin Assignments for BITS

BITS Pin	Tip/Ring	CTC/TL1 Name	Function
A4	ring	BITS-1	Input from BITS device 1
B4	tip	BITS-1	Input from BITS device 1
A3	ring	BITS-1	Output to external device 1
B3	tip	BITS-1	Output to external device 1
A2	ring	BITS-2	Input from BITS device 2
B2	tip	BITS-2	Input from BITS device 2
A1	ring	BITS-2	Output to external device 2
B1	tip	BITS-2	Output to external device 2

Note For more detailed information about timing, refer to the "Timing" chapter of the *Cisco ONS 15454 Reference Manual*. To set up system timing, see the "NTP-A28 Set Up Timing" procedure on page 4-13.

Step 2 Return to your originating procedure (NTP).

DLP-A21 Install LAN Wires on the Backplane

Purpose	This task installs the LAN wires on the backplane.
Tools/Equipment	Wire wrapper #22 or #24 AWG (0.51 mm² or 0.64 mm²) wire, preferably CAT-5 UTP
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Rather than using the LAN wires, you can use the LAN connection port on the TCC2/TCC2P if preferred. Use either the backplane connection or the TCC2/TCC2P front connection. You cannot use the LAN backplane pins and the LAN connection port on the TCC2/TCC2P simultaneously; however, it is possible for you to make a direct connection from a computer to the LAN connection port on the TCC2/TCC2P while the LAN backplane pins are in use, as long as the computer that is connected directly to the TCC2/TCC2P is not connected to the same LAN.
The LAN ports of the ONS15454 are suitable for connection only to shielded intra-building cabling grounded at both ends (STP cables).

Step 1 Using #22 or #24 AWG (0.51 mm² or 0.64 mm²) wire or CAT-5 STP Ethernet cable, wrap the wires on the appropriate wire-wrap pins according to local site practice.

Caution Crosstalk might result if both receive (Rx) and transmit (Tx) pins connect on the same twisted pair of wires from the CAT-5 cable. The two Tx pins need to be on one twisted pair, and the two Rx pins need to be on another twisted pair.

A frame ground pin is located beneath each pin field (FG2 for the LAN pin field). Wrap the ground shield of the LAN interface cable to the frame ground pin. Table 17-2 shows the LAN pin assignments.

Table 17-2 LAN Pin Assignments

Pin Field	Backplane Pins	RJ-45 Pins	Function/Color
LAN 1 Connecting to data circuit-terminating equipment (DCE*) (a hub or switch); the ONS 15454 is a DCE	B2	1	TX+ white/green
	A2	2	TX– green
	B1	3	RX+ white/orange
	A1	6	RX– orange
LAN 1 Connecting to data terminal equipment (DTE) (a PC/workstation or router)	B1	1	RX+ white/green
	A1	2	RX– green
	B2	3	TX+ white/orange
	A2	6	TX– orange

Note The TCC2/TCC2P does not support Ethernet polarity detection. If your Ethernet connection has incorrect polarity (this can only occur with cables that have the receive wire pairs flipped), a "Lan Connection Polarity Reversed" condition is raised. This condition usually occurs during an upgrade or initial node deployment. To correct the situation, ensure that your Ethernet cable has the correct mapping of the wire-wrap pins.

Step 2 Return to your originating procedure (NTP).

DLP-A22 Install the TL1 Craft Interface

Purpose	This task installs the TL1 craft interface using the craft backplane pins. You can also use a LAN cable connected to the EIA/TIA-232 port on the TCC2/TCC2P card to access a TL1 craft interface.
Tools/Equipment	Wire wrapper #22 or #24 AWG (0.51 mm² or 0.64 mm²) alarm wires
Prerequisite Procedures	NTP-A4 Remove the Backplane Covers, page 1-7
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Rather than using the craft pins, you can use a LAN cable connected to the EIA/TIA-232 port on the TCC2/TCC2P card to access a TL1 craft interface.

Step 1 Using #22 or #24 AWG (0.51 mm² or 0.64 mm²) wire, wrap the craft interface wires on the appropriate wire-wrap pins according to local site practice.

Step 2 Wrap the ground shield of the craft interface cable to the frame-ground pin.

Wrap the ground wire of your computer cable to Pin A3 on the craft pin field. Table 17-3 shows the pin assignments for the CRAFT pin field.

Note You cannot use the craft backplane pins and the EIA/TIA-232 port on the TCC2/TCC2P card simultaneously. Using a combination prevents access to the node or causes a loss in connectivity.

Table 17-3 Craft Interface Pin Assignments

Pin Field	Contact	Function
Craft	A1	Receive
	A2	Transmit
	A3	Ground
	A4	DTR

Step 3 Return to your originating procedure (NTP).

DLP-A23 Install DS-1 Cables Using Electrical Interface Adapters (Balun)

Purpose	This task installs the DS-1 cables on an SMB EIA using the electrical interface adapters.
Tools/Equipment	Wire wrapper Twisted-pair cables
Prerequisite Procedures	DLP-A13 Install an SMB EIA, page 17-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note All DS-1 cables connected to the ONS 15454 DS-1 ports must terminate with twisted-pair cables to connect to the DS-1 electrical interface adapter. The DS-1 electrical interface adapters project 1.72 inches (43.7 mm) beyond the SMB EIA. Refer to the "Shelf and Backplane Hardware" chapter in the *Cisco ONS 15454 Reference Manual* for more information.

Step 1 Attach the SMB connector on an adapter to the SMB connector for the port's transmit pair on the backplane.

Step 2 Attach the SMB connector on an adapter to the SMB connector for the port's receive pair on the backplane.

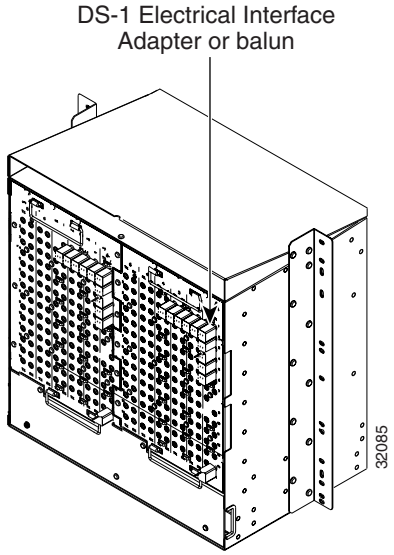
Step 3 Terminate the DS-1 transmit and receive cables for the port to the wire-wrap posts on the adapter:

- **a.** Using a wire-wrap tool, connect the receive cables to the receive adapter pins on the backplane connector for the desired port.
- **b.** Connect the transmit cables to the transmit adapter pins on the backplane connector for the desired port.
- **c.** Terminate the shield ground wire on the DS-1 cable to ground according to local site practice.

Note If you put DS1N-14 cards in Slots 3 and 15 to form 1:N protection groups, do not wire Slots 3 and 15 for DS-1 electrical interface adapters.

Figure 17-13 shows a ONS 15454 backplane with an SMB EIA. DS-1 electrical interface adapters are attached on both sides of the shelf assembly to create DS-1 twisted-pair termination points.

Figure 17-13 Backplane with an SMB EIA for DS-1 Cables



Step 4 Return to your originating procedure (NTP).

DLP-A24 Install DS-1 AMP Champ Cables on the AMP Champ EIA

Purpose	This task installs the DS-1 AMP Champ cables on the AMP Champ EIA.
Tools/Equipment	Wire wrapper Twisted-pair cables
Prerequisite Procedures	DLP-A14 Install the AMP Champ EIA, page 17-16
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Prepare a 56-wire cable for each DS1-14/DS1N-14 card you will install in the shelf assembly.

Step 2 Connect the male AMP Champ connector on the cable to the female AMP Champ connector on the ONS 15454 backplane.

Step 3 Use the clips on the male AMP Champ connector to secure the connection.

The female connector has grooves on the outside edge for snapping the clips into place.

Table 17-4 shows the pin assignments for the AMP Champ connectors on the ONS 15454 AMP Champ EIA.

Note In Table 17-4, the shaded area corresponds to the white/orange binder group. A binder group is a set of 25 pairs of wires coded with an industry-standard color scheme.

Table 17-4 Pin Assignments for AMP Champ Connectors

Signal/Wire	Pin	Pin	Signal/Wire	Signal/Wire	Pin	Pin	Signal/Wire
Tx Tip 1 white/blue	1	33	Tx Ring 1 blue/white	Rx Tip 1 yellow/orange	17	49	Rx Ring 1 orange/yellow
Tx Tip 2 white/orange	2	34	Tx Ring 2 orange/white	Rx Tip 2 yellow/green	18	50	Rx Ring 2 green/yellow
Tx Tip 3 white/green	3	35	Tx Ring 3 green/white	Rx Tip 3 yellow/brown	19	51	Rx Ring 3 brown/yellow
Tx Tip 4 white/brown	4	36	Tx Ring 4 brown/white	Rx Tip 4 yellow/slate	20	52	Rx Ring 4 slate/yellow
Tx Tip 5 white/slate	5	37	Tx Ring 5 slate/white	Rx Tip 5 violet/blue	21	53	Rx Ring 5 blue/violet
Tx Tip 6 red/blue	6	38	Tx Ring 6 blue/red	Rx Tip 6 violet/orange	22	54	Rx Ring 6 orange/violet
Tx Tip 7 red/orange	7	39	Tx Ring 7 orange/red	Rx Tip 7 violet/green	23	55	Rx Ring 7 green/violet
Tx Tip 8 red/green	8	40	Tx Ring 8 green/red	Rx Tip 8 violet/brown	24	56	Rx Ring 8 brown/violet
Tx Tip 9 red/brown	9	41	Tx Ring 9 brown/red	Rx Tip 9 violet/slate	25	57	Rx Ring 9 slate/violet
Tx Tip 10 red/slate	10	42	Tx Ring 10 slate/red	Rx Tip 10 [1] white/blue	26	58	Rx Ring 10 blue/white
Tx Tip 11 black/blue	11	43	Tx Ring 11 blue/black	Rx Tip 11 white/orange	27	59	Rx Ring 11 orange/white
Tx Tip 12 black/orange	12	44	Tx Ring 12 orange/black	Rx Tip 12 white/green	28	60	Rx Ring 12 green/white
Tx Tip 13 black/green	13	45	Tx Ring 13 green/black	Rx Tip 13 white/brown	29	61	Rx Ring 13 brown/white
Tx Tip 14 black/brown	14	46	Tx Ring 14 brown/black	Rx Tip 14 white/slate	30	62	Rx Ring 14 slate/white
Tx Spare0+ Not applicable	15	47	Tx Spare0– Not applicable	Rx Spare0+ Not applicable	31	63	Rx Spare0– Not applicable
Tx Spare1+ Not applicable	16	48	Tx Spare1– Not applicable	Rx Spare1+ Not applicable	32	64	Rx Spare1– Not applicable

1. Pins 26, 27, 28, 29, 30, 58, 59, 60, 61, and 62 correspond to the white/orange binder group. A binder group is a set of 25 pairs of wires coded with an industry-standard color scheme.

Table 17-5 shows the pin assignments for the AMP Champ connectors on the ONS 15454 AMP Champ EIA for a shielded DS-1 cable.

Table 17-5 Pin Assignments for AMP Champ Connectors (Shielded DS1 Cable)

64-Pin Blue Bundle				64-Pin Orange Bundle			
Signal/Wire	**Pin**	**Pin**	**Signal/Wire**	**Signal/Wire**	**Pin**	**Pin**	**Signal/Wire**
Tx Tip 1 white/blue	1	33	Tx Ring 1 blue/white	Rx Tip 1 white/blue	17	49	Rx Ring 1 blue/white
Tx Tip 2 white/orange	2	34	Tx Ring 2 orange/white	Rx Tip 2 white/orange	18	50	Rx Ring 2 orange/white
Tx Tip 3 white/green	3	35	Tx Ring 3 green/white	Rx Tip 3 white/green	19	51	Rx Ring 3 green/white
Tx Tip 4 white/brown	4	36	Tx Ring 4 brown/white	Rx Tip 4 white/brown	20	52	Rx Ring 4 brown/white
Tx Tip 5 white/slate	5	37	Tx Ring 5 slate/white	Rx Tip 5 white/slate	21	53	Rx Ring 5 slate/white
Tx Tip 6 red/blue	6	38	Tx Ring 6 blue/red	Rx Tip 6 red/blue	22	54	Rx Ring 6 blue/red
Tx Tip 7 red/orange	7	39	Tx Ring 7 orange/red	Rx Tip 7 red/orange	23	55	Rx Ring 7 orange/red
Tx Tip 8 red/green	8	40	Tx Ring 8 green/red	Rx Tip 8 red/green	24	56	Rx Ring 8 green/red
Tx Tip 9 red/brown	9	41	Tx Ring 9 brown/red	Rx Tip 9 red/brown	25	57	Rx Ring 9 brown/red
Tx Tip 10 red/slate	10	42	Tx Ring 10 slate/red	Rx Tip 10 red/slate	26	58	Rx Ring 10 slate/red
Tx Tip 11 black/blue	11	43	Tx Ring 11 blue/black	Rx Tip 11 black/blue	27	59	Rx Ring 11 blue/black
Tx Tip 12 black/orange	12	44	Tx Ring 12 orange/black	Rx Tip 12 black/orange	28	60	Rx Ring 12 orange/black
Tx Tip 13 black/green	13	45	Tx Ring 13 green/black	Rx Tip 13 black/green	29	61	Rx Ring 13 green/black
Tx Tip 14 black/brown	14	46	Tx Ring 14 brown/black	Rx Tip 14 black/brown	30	62	Rx Ring 14 brown/black
Tx Tip 15 black/slate	15	47	Tx Tip 15 slate/black	Rx Tip 15 black/slate	31	63	Rx Tip 15 slate/black
Tx Tip 16 yellow/blue	16	48	Tx Tip 16 blue/yellow	Rx Tip 16 yellow/blue	32	64	Rx Tip 16 blue/yellow

Step 4 Return to your originating procedure (NTP).

DLP-A25 Install Coaxial Cable With BNC Connectors

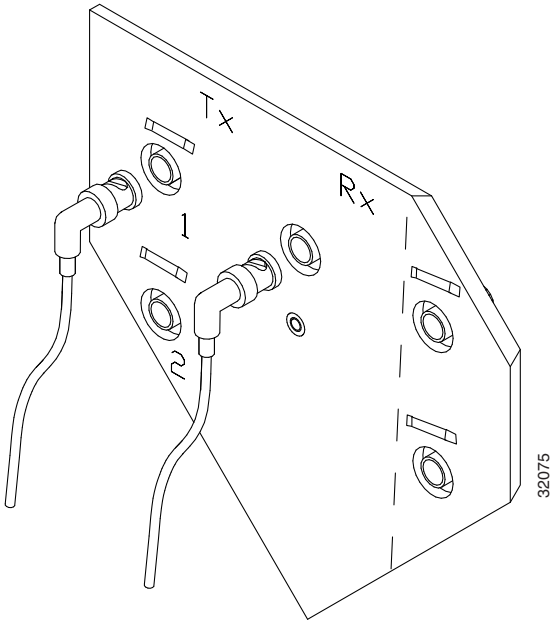
Purpose	This task installs the coaxial cable with BNC connectors.
Tools/Equipment	None
Prerequisite Procedures	DLP-A12 Install a BNC or High-Density BNC EIA, page 17-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **Metallic interfaces for connection to outside plant lines (such as T1/E1/T3/E3 etc.) must be connected through a registered or approved device such as CSU/DSU or NT1.** Statement 290

Step 1 Place the BNC cable connector over the desired connection point on the backplane.

Figure 17-14 shows how to connect a coaxial cable to the BNC EIA using a right-angle BNC cable connector.

Figure 17-14 Using a Right-Angle Connector to Install Coaxial Cable with BNC Connectors



Step 2 Position the cable connector so that the slot in the connector is over the corresponding notch at the backplane connection point.

Step 3 Gently push the connector down until the notch backplane connector slides into the slot on the cable connector.

Step 4 Turn the cable connector clockwise to lock it into place.

Step 5 Tie wrap or lace the cables to the EIA according to Telcordia standards (GR-1275-CORE) or local site practice.

Step 6 Route the cables to the nearest side of the shelf assembly through the side cutouts according to local site practice. The rubber-coated edges of the side cutouts prevent the cables from chafing.

Step 7 Label all cables at each end of the connection to avoid confusion with cables that are similar in appearance.

Step 8 Return to your originating procedure (NTP).

DLP-A26 Install Coaxial Cable With High-Density BNC Connectors

Purpose	This task installs the coaxial cable with high-density BNC connectors.
Tools/Equipment	BNC insertion tool
Prerequisite Procedures	DLP-A12 Install a BNC or High-Density BNC EIA, page 17-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Place the cable connector over the desired connection point on the backplane.

Step 2 Using the BNC insertion tool, position the cable connector so that the slot in the connector is over the corresponding notch at the backplane connection point.

Step 3 Gently push the connector down until the notch backplane connector slides into the slot on the cable connector.

Step 4 Turn the cable connector clockwise to lock it into place.

Step 5 Tie wrap or lace the cables to the EIA according to Telcordia standards (GR-1275-CORE) or local site practice.

Step 6 Route the cables to the nearest side of the shelf assembly through the side cutouts according to local site practice.

The rubber-coated edges of the side cutouts prevent the cables from chafing.

Step 7 Return to your originating procedure (NTP).

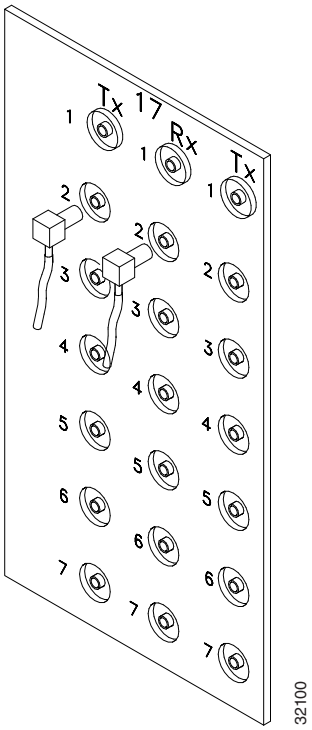
DLP-A27 Install Coaxial Cable with SMB Connectors

Purpose	This task installs the coaxial cable with SMB connectors.
Tools/Equipment	SMB cable connector
Prerequisite Procedures	DLP-A13 Install an SMB EIA, page 17-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **Metallic interfaces for connection to outside plant lines (such as T1/E1/T3/E3 etc.) must be connected through a registered or approved device such as CSU/DSU or NT1.** Statement 290

Step 1 Place the SMB cable connector over the desired connection point on the backplane (Figure 17-15).

Figure 17-15 Installing Coaxial Cable with SMB Connectors



Step 2 Gently push the connector until it clicks into place.

Step 3 Tie wrap or lace the cables to the EIA according to Telcordia standards (GR-1275-CORE) or local site practice.

Step 4 Route the cables to the nearest side of the shelf assembly into rack runs according to local site practice.

Step 5 Label the transmit, receive, working, and protect cables at each end of the connection to avoid confusion with cables that are similar in appearance.

Step 6 Return to your originating procedure (NTP).

DLP-A28 Route Coaxial Cables

Purpose	This task routes the coaxial cables.
Tools/Equipment	RG179, RG59 (735A) #26 AWG cable, or RG59 (734A) #20 AWG cable
Prerequisite Procedures	One or more of the following tasks, as needed: • DLP-A25 Install Coaxial Cable With BNC Connectors, page 17-31 • DLP-A26 Install Coaxial Cable With High-Density BNC Connectors, page 17-32 • DLP-A27 Install Coaxial Cable with SMB Connectors, page 17-32
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Tie wrap or lace the coaxial cables according to local site practice and route the cables through the side cutouts on either side of the ONS 15454. The rubber coated edges of the side cutouts prevent the cables from chafing.

Step 2 Use short lengths of pigtail RG179 to terminate the shelf assembly.

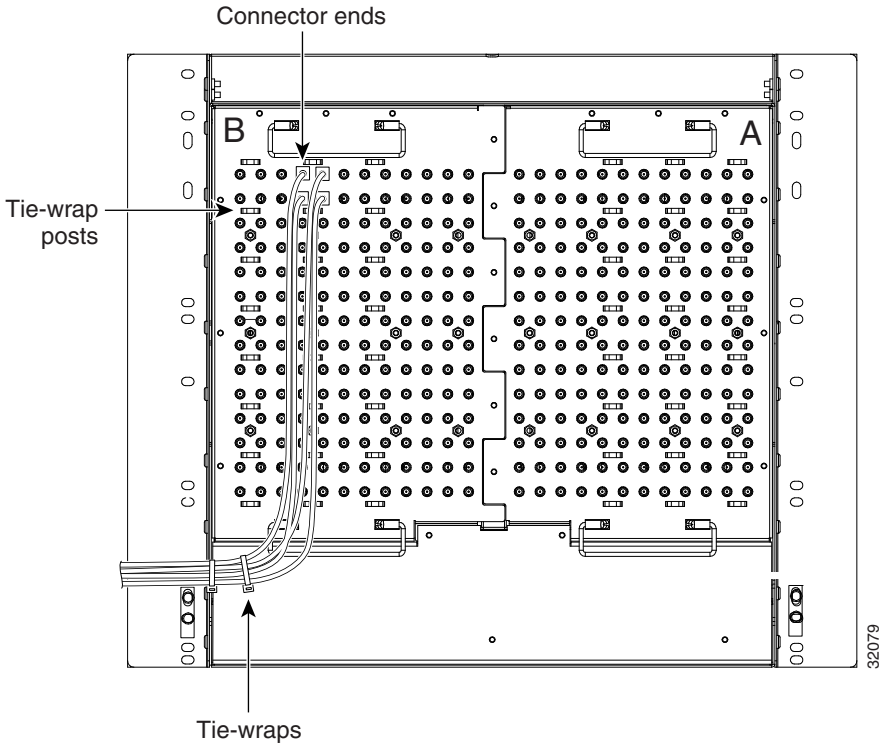
Step 3 Use standard RG59 (735A) cable connected to the RG179 for the remainder of the cable run. When using a 10-foot (3.05-m) section of the RG179, you can attach a maximum length of 437 feet (133 m) of RG59 (735A). When using a 30-foot (9.1-m) section of RG179, you can attach a maximum length of 311 feet (94.8 m) of RG59 (735A).

When using the RG179 cable, the maximum distance available (122 feet, 37.2 m) is less than the maximum distance available with standard RG59 (735A) cable (306 feet, 93.3 m). The maximum distance when using the RG59 (734A) cable is 450 feet (137.2 m). The shorter maximum distance available with the RG179 is due to a higher attenuation rate for the thinner cable. Attenuation rates are calculated using a DS-3 signal:

- For RG179, the attenuation rate is 59 dB/kft (dB per kilo-foot) at 22 MHz.
- For RG59 (735A), the attenuation rate is 23 dB/kft at 22 MHz.

Use a figure of 5.0 for total cable loss when making calculations. Figure 17-16 shows an example of proper coaxial cable routing.

Figure 17-16 Routing Coaxial Cable (SMB EIA Backplane)



Step 4 Return to your originating procedure (NTP).

DLP-A29 Route DS-1 Twisted-Pair Cables

Purpose	This task routes the DS-1 twisted-pair cables.
Tools/Equipment	None
Prerequisite Procedures	DLP-A23 Install DS-1 Cables Using Electrical Interface Adapters (Balun), page 17-27
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify the following:

- DS-1 electrical interface adapters are installed on every transmit and receive connector for DS-1 ports.
- Wire-wrap posts on the DS-1 electrical interface adapters are used to connect the terminated incoming cables.

Step 2 Tie-wrap or lace the twisted-pair cables according to local site practice and route the cables into the side cutouts on either side of the ONS 15454.

Note SMB EIAs feature cable-management eyelets for tie wrapping or lacing cables to the cover panel.

Step 3 Return to your originating procedure (NTP).

DLP-A32 Inspect the Shelf Installation and Connections

Purpose	Use this task to inspect the shelf installation and connections and to verify that everything is installed and connected properly.
Tools/Equipment	None
Prerequisite Procedures	Complete Table 1-5 on page 1-32
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Check each wire and cable connection to make sure all cables are locked securely. If a wire or cable is loose, return to the applicable installation procedure to correct it.

Step 2 To check that the backplane is seated correctly, verify that the screw holes and the backplane interface card holes align properly and that the A and B connectors interlock.

Step 3 Return to your originating procedure (NTP).

DLP-A33 Measure Voltage

Purpose	This task measures the power to verify correct power and returns.
Tools/Equipment	Voltmeter
Prerequisite Procedures	Complete Table 1-5 on page 1-32.
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Using a voltmeter, verify the office ground and power. Figure 17-9 on page 17-19 shows the power terminals.

a. Place the black lead (positive) on the frame ground on the bay. Hold it there while completing Step b.

b. Place the red lead (negative) on the fuse power points and alarm panel to verify that they read between –40.5 VDC and –57 VDC (power) or 0 (return ground).

Step 2 Using a voltmeter, verify the shelf ground and power wiring:

a. Place the black lead (positive) on the RET1 and the red lead on the BAT1 point. Verify a reading between –40.5 VDC and –57 VDC. If there is no voltage, check the following and correct if necessary:

- Battery and ground are reversed to the shelf.
- Battery is open or missing.
- Return is open or missing.

b. Repeat Step 2 for the RET2 and BAT2 if the B power feed is provided.

Step 3 Return to your originating procedure (NTP).

DLP-A36 Install the TCC2/TCC2P Cards

Purpose	This task installs redundant TCC2/TCC2P cards. The first card you install in the ONS 15454 must be a TCC2/TCC2P card, and it must initialize before you install any cross-connect or traffic cards.
Tools/Equipment	Two TCC2/TCC2P cards
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note When installing cards, allow each card to boot completely before installing the next card.

Step 1 Open the latches/ejectors of the TCC2/TCC2P card that you will install.

Step 2 Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 7 or 11).

Step 3 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

If you insert a card into a slot provisioned for a different card, all LEDs turn off.

Step 4 Go to Step a to verify the LED activity on the TCC2 card. For the TCC2P card, go to Step b.

a. For the TCC2 card:

- All LEDs turn on briefly. The red FAIL LED and the yellow ACT/STBY LED turn on for about 15 seconds.
- The red FAIL LED and the green ACT/STBY LED turn on for about 40 seconds.
- The red FAIL LED blinks for about 15 seconds.
- The red FAIL LED turns on for about 15 seconds. All LEDs turn on for about 3 seconds before turning off for about 3 seconds.

- Both green PWR LEDs turn on for 10 seconds. The PWR LEDs then turn red for 2 to 3 minutes before going to steady green.
- While the PWR LEDs are red for two to three minutes, the ACT/STBY, MJ, and MN LEDs turn on, followed by the SNYC LED.
- The boot up process is complete when the PWR LEDs turn green and the ACT/STBY remains on. (The ACT/STBY LED will be green if this is the first TCC2 card installed, and amber if this is the second TCC2 card installed.)

Note It might take up to 4 minutes for the A and B power alarms to clear.

Note Alarm LEDs might be on; disregard alarm LEDs until you are logged into Cisco Transport Controller (CTC) and can view the Alarms tab.

Note If you are logged into CTC, the SFTWDOWN alarm might appear as many as two times while the TCC2 card initializes. The alarm should clear after the card completely boots.

Note If the FAIL LED is on continuously, see the tip in Step 8 about the TCC2 card automatic upload.

b. For the TCC2P card:

- All LEDs turn on briefly. The red FAIL LED, the yellow ACT/STBY LED, the green SYNC LED, and the green ACO LED turn on for about 15 seconds.
- The red FAIL LED and the green ACT/STBY LED turn on for about 30 seconds.
- The red FAIL LED blinks for about 3 seconds.
- The red FAIL LED turns on for about 15 seconds.
- The red FAIL LED blinks for about 10 seconds and then becomes solid.
- All LEDs (including the CRIT, MAJ, MIN, REM, SYNC, and ACO LEDs) blink once and turn off for about 5 seconds.
- Both green PWR LEDs turn on for 10 seconds. The PWR LEDs then turn red for 2 to 3 minutes before going to steady green. During this time, the ACT/STBY, MJ, and MN LEDs might turn on, followed by the SNYC LED briefly.
- The boot up process is complete when the PWR LEDs turn green and the yellow ACT/STBY remains on. (The ACT/STBY LED will be green if this is the first TCC2 card installed, and yellow if this is the second TCC2 card installed.)

Note It might take up to 3 minutes for the A and B power alarms to clear.

Note Alarm LEDs might be on; disregard alarm LEDs until you are logged into CTC and can view the Alarms tab.

Note If you are logged into CTC, the SFTWDOWN alarm might appear as many as two times while the TCC2P card initializes. The alarm should clear after the card completely boots.

Note If the FAIL LED is on continuously, see the tip in Step 8 about the TCC2P card automatic upload.

Step 5 Verify that the ACT/STBY LED is green if this is the first powered-up TCC2/TCC2P card being installed, or yellow for standby if this is the second powered-up TCC2/TCC2P. The IP address, temperature of the node, and time of day appear on the LCD. The default time and date is 12:00 AM, January 1, 1970.

Step 6 The LCD cycles through the IP address (the default is 192.1.0.2), node name, and software version. Verify that the correct software version displays on the LCD. The software text string indicates the node type (SDH or SONET) and software release.(For example: SDH 08.50-05L-20.10 indicates it is an SDH software load, Release 8.50. The numbers following the release number do not have any significance.)

Step 7 If the LCD shows the correct software version, continue with Step 8. If the LCD does not show the correct software version, upgrade the software or remove the TCC2/TCC2P card and install a replacement card.

Refer to the release-specific software upgrade document to replace the software. To exchange the TCC2/TCC2P card, see the *Cisco ONS 15454 Troubleshooting Guide*.

Step 8 Repeat Steps 1 through 7 for the redundant TCC2/TCC2P card.

Tip If you install a standby TCC2/TCC2P card that has a different software version than the active card, the newly installed standby TCC2/TCC2P card automatically copies the software version from the active TCC2/TCC2P card. You do not need to do anything in this situation, but the loading TCC2/TCC2P card does not boot up in the normal manner. When the standby card is first inserted, the LEDs follow most of the sequence listed in Step 4. However, after the red FAIL LED turns on for about 5 seconds, the FAIL LED and the ACT/STBY LED begin to flash alternately for up to 30 minutes while the new software loads onto the active TCC2/TCC2P card. After loading the new software, the upgraded TCC2/TCC2P card's LEDs repeat the sequence from Step 4, and the amber ACT/STBY LED turns on.

Note If you insert a card into a slot provisioned for a different card, all LEDs turn off.

Note Alarm LEDs might be on; disregard alarm LEDs until you are logged into CTC and can view the Alarms tab.

Step 9 Verify that the ACT/STBY LED is amber for standby.

Step 10 Return to your originating procedure (NTP).

DLP-A37 Install the XCVT, XC10G, or XC-VXC-10G Cards

Purpose	This task installs the cross-connect (XCVT/XC10G/XC-VXC-10G) cards.
Tools/Equipment	XCVT/XC10G/XC-VXC-10G (cross-connect) cards
Prerequisite Procedures	DLP-A36 Install the TCC2/TCC2P Cards, page 17-37
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note Do not use this procedure to upgrade cross-connect cards. If you are upgrading an XCVT card to an XC10G card, or an XC10G card to an XC-VXC-10G card, see Chapter 12, "Upgrade Cards and Spans."

Note When installing cards, let each card boot completely before installing the next card.

Step 1 Open the latches/ejectors of the first XCVT, XC10G, or XC-VXC-10G card that you will install.

Step 2 Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 8 or 10).

Step 3 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 4 Verify the LED activity:

- The red FAIL LED turns on for 20 to 30 seconds.
- The red FAIL LED blinks for 35 to 45 seconds.
- The red FAIL LED turns on for 5 to 10 seconds.
- All LEDs blink once and turn on.
- The ACT/STBY LED turns on.

Note If you insert a card into a slot provisioned for a different card, all LEDs turn off.

Note If the red FAIL LED does not turn on, check the power.

Note If the red FAIL LED is on continuously or the LEDs act erratically, the card is not installed properly. Remove the card and repeat Steps 1 to 4.

Step 5 Verify that the ACT/STBY LED is green for active.

Step 6 Use the latches/ejectors to firmly slide the second cross-connect card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 8 or 10).

Step 7 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 8 Verify the LED activity:

- The red FAIL LED turns on for 20 to 30 seconds.
- The red FAIL LED blinks for 35 to 45 seconds.
- The red FAIL LED turns on for 5 to 10 seconds.
- All LEDs blink once and turn on.
- The ACT/STBY LED turns on.

Note If you insert a card into a slot provisioned for a different card, all LEDs turn off.

Note If the red FAIL LED does not turn on, check the power.

Note If the red FAIL LED is turned on continuously or the LEDs act erratically, the card is not installed properly. Remove the card and repeat Steps 6 through 8.

Step 9 Verify that the ACT/STBY LED is amber for standby.

Step 10 Return to your originating procedure (NTP).

DLP-A39 Install Ethernet Cards

Purpose	This task installs the Ethernet cards (E100T-12, E100T-G, E1000-2, E1000-2-G, G1K-4, ML100T-12, ML1000-2, ML100X-8, ML-MR-10, CE-100T-8, CE-1000-4, and CE-MR-10).
Tools/Equipment	Ethernet cards
Prerequisite Procedures	NTP-A15 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Open the card latches/ejectors.

Step 2 Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot.

Step 3 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 4 Verify the LED activity:

- The red FAIL LED turns on for 20 to 30 seconds.
- The red FAIL LED blinks for 35 to 45 seconds.
- All LEDs blink once and turn off for 1 to 5 seconds.
- The ACT or ACT/STBY LED turns on. The SF LED can persist until all card ports connect to their far end counterparts and a signal is present.

Note If the red FAIL LED does not turn on, check the power.

Note If you insert a card into a slot provisioned for a different card, all LEDs turn off.

Step 5 Return to your originating procedure (NTP).

DLP-A41 Install the Alarm Interface Controller–International Card

Purpose	This task installs the Alarm Interface Controller–International (AIC-I) card. The AIC-I card provides connections for external alarms and controls (environmental alarms).
Tools/Equipment	AIC-I card
Prerequisite Procedures	DLP-A36 Install the TCC2/TCC2P Cards, page 17-37 DLP-A37 Install the XCVT, XC10G, or XC-VXC-10G Cards, page 17-40
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note When installing cards, allow each card to boot completely before installing the next card.

Step 1 Open the latches/ejectors on the card.

Step 2 Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 9).

Step 3 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 4 Verify the following:

- The red FAIL LED turns on for 1 second, then blinks for 1 to 5 seconds.
- The PWR A and PWR B LEDs become red and the two INPUT/OUTPUT LEDs become green for approximately 3 seconds.
- The PWR A LED turns green, the INPUT/OUTPUT LEDs turn off, and the ACT LED turns on. If the red FAIL LED does not turn on, check the power.

Note It might take up to 3 minutes for the PWR A and PWR B LEDs to update.

Note If you insert a card into a slot provisioned for a different card, no LEDs turn on.

Note If the red FAIL LED is on continuously or the LEDs act erratically, the card is not installed properly. Remove the card and repeat Steps 1 to 4.

Step 5 Return to your originating procedure (NTP).

DLP-A43 Install Fiber-Optic Cables for Path Protection Configurations

Purpose	This task connects the fiber-optic cables to the east and west path protection ports at each node. See Chapter 5, "Turn Up a Network" to provision and test path protection configurations.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors, page 15-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note To avoid error, connect fiber-optic cable so that the farthest slot to the right represents the east port, and the farthest slot to the left represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.

Caution Do not provision the path protection east and west ports on the same OC-N card.

Step 1 Plan your fiber connections. Use the same plan for all path protection nodes.

Step 2 Plug the fiber into the Tx connector of an OC-N card at one node and plug the other end of the fiber into the Rx connector of an OC-N card at the adjacent node. The card displays an SF LED if the transmit and receive fibers are mismatched (one fiber connects a receive port on one card to a receive port on another card, or the same situation with transmit ports).

Step 3 Repeat Step 2 until you have configured the ring.

Figure 17-17 shows fiber connections for a four-node path protection configuration with trunk (span) cards in Slot 5 (west) and Slot 12 (east).

Figure 17-17 Connecting Fiber to a Four-Node Path Protection Configuration

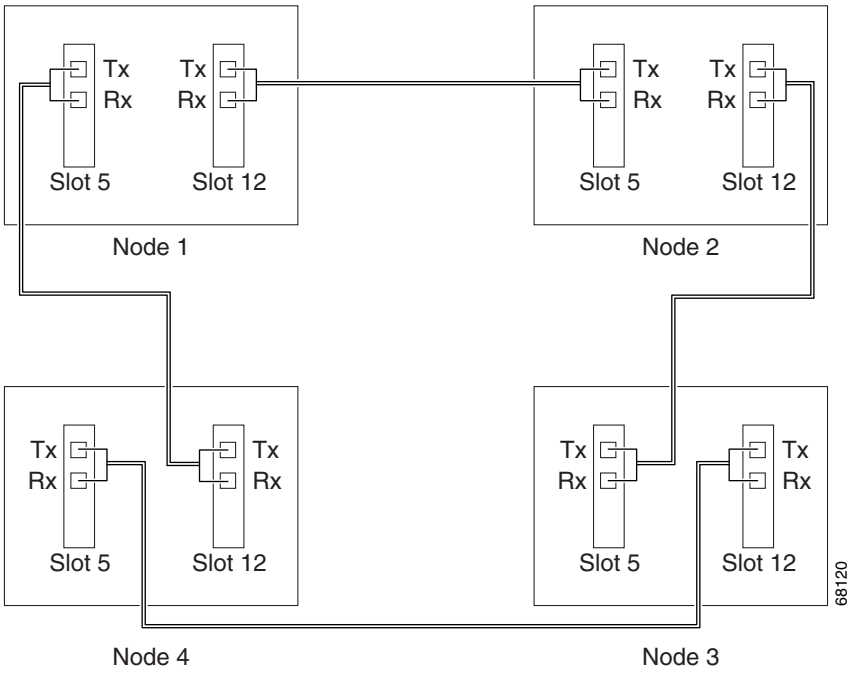


Figure 17-18 shows a traditional path protection dual-ring interconnect (DRI) example.

Figure 17-18 Connecting Fiber to an Eight-Node Traditional Path Protection Dual-Ring Interconnect

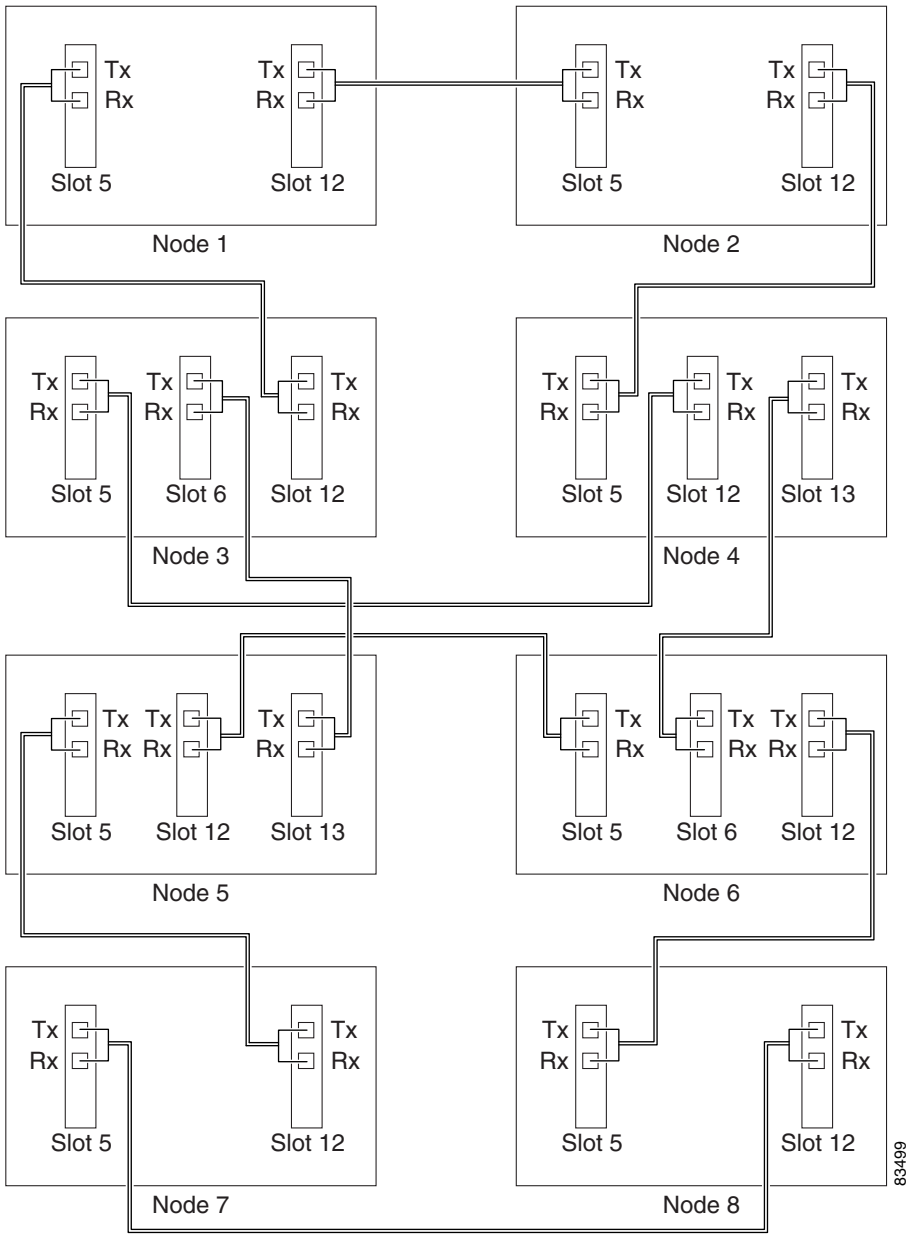
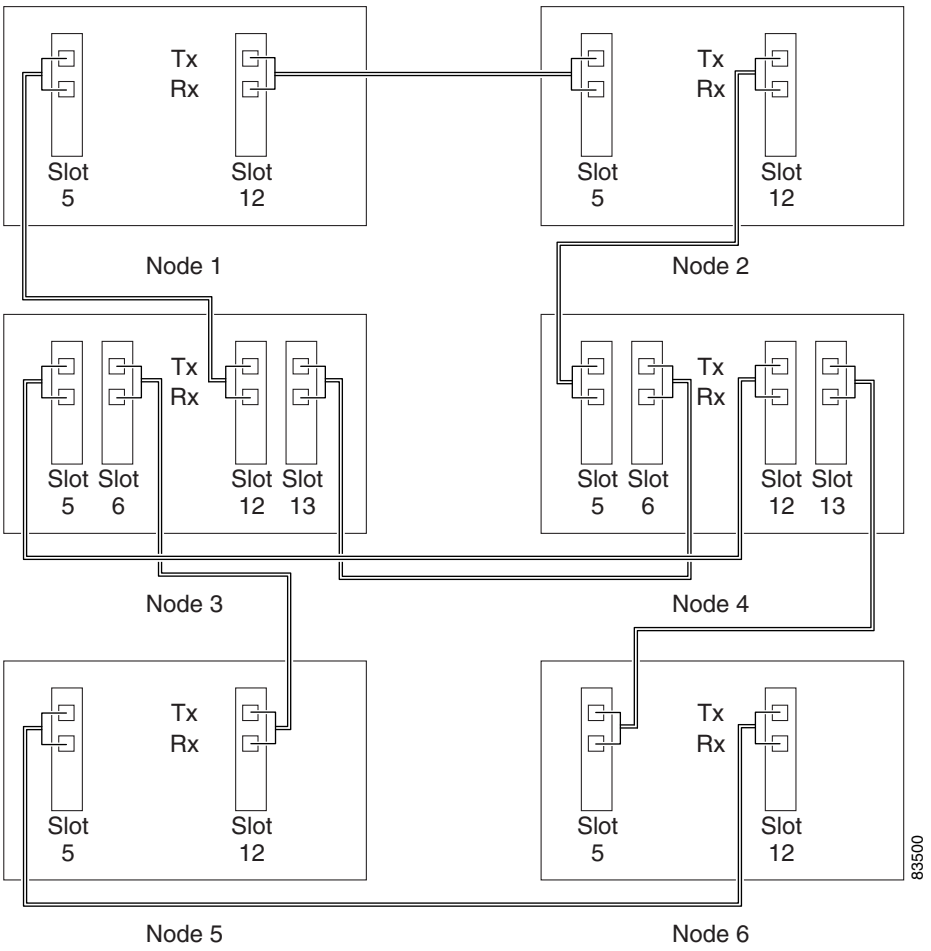


Figure 17-19 shows an integrated dual-ring interconnect (DRI) example.

Figure 17-19 Connecting Fiber to a Six-Node Integrated Path Protection Dual-Ring Interconnect



Step 4 Return to your originating procedure (NTP).

DLP-A44 Install Fiber-Optic Cables for BLSR Configurations

Purpose	This task installs the fiber-optic cables to the east and west bidirectional line switched ring (BLSR) ports at each node. See Chapter 5, "Turn Up a Network" to provision and test BLSR configurations.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors, page 15-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note To avoid error, connect fiber-optic cable so that the farthest slot to the right represents the east port, and the farthest slot to the left represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.

Caution Do not provision the BLSR east and west ports on the same OC-N card.

Step 1 Plan your fiber connections. Use the same plan for all BLSR nodes.

Step 2 Plug the fiber into the Tx connector of an OC-N card at one node and plug the other end into the Rx connector of an OC-N card at the adjacent node. The card displays an SF LED if the transmit and receive fibers are mismatched.

Note Do not mix working and protect card connections when connecting a four-fiber BLSR. The BLSR does not function if working and protect cards are interconnected. See Figure 17-21 on page 17-48 for an example of correct four-fiber BLSR cabling.

Step 3 Repeat Step 2 until you have configured the ring.

Figure 17-20 shows fiber connections for a two-fiber BLSR with trunk (span) cards in Slot 5 (west) and Slot 12 (east).

Figure 17-20 Connecting Fiber to a Four-Node, Two-Fiber BLSR

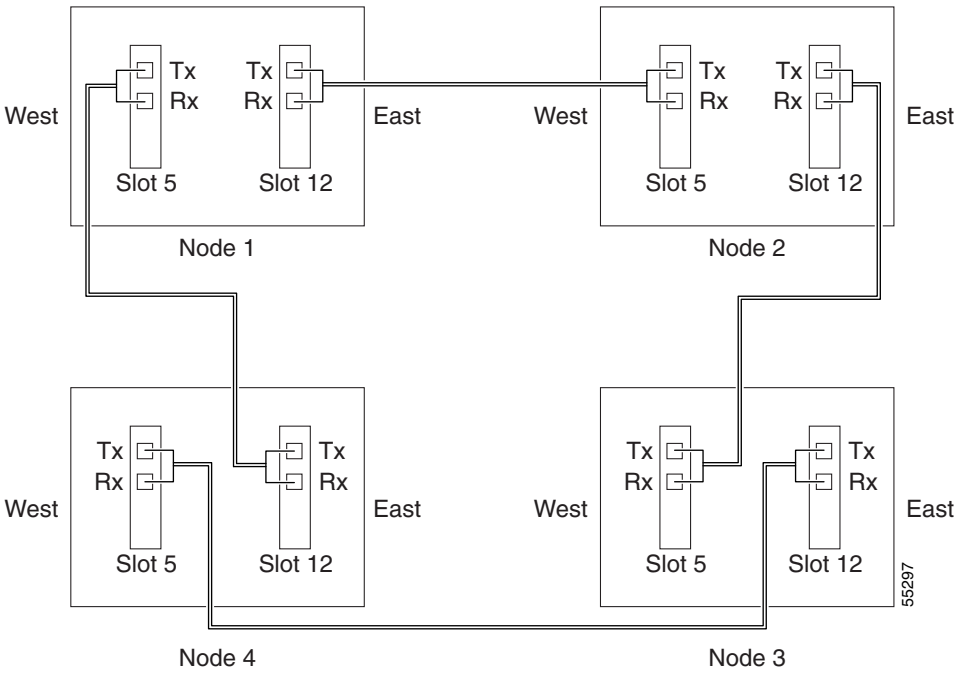
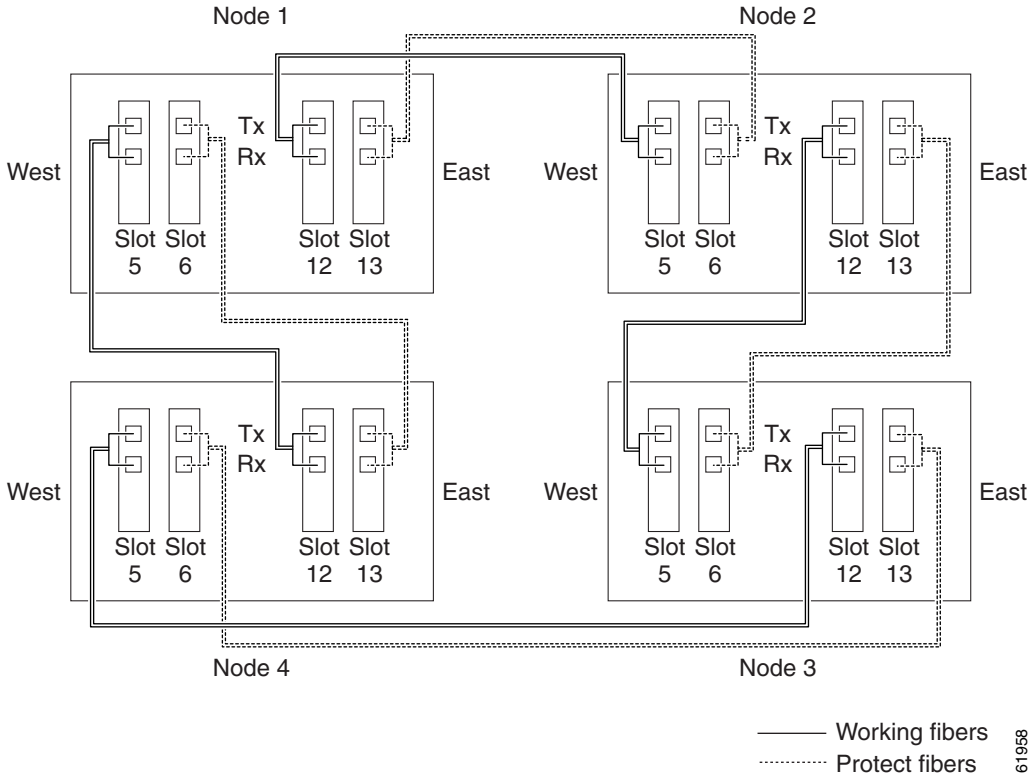


Figure 17-21 shows fiber connections for a four-fiber BLSR. Slot 5 (west) and Slot 12 (east) carry the working traffic. Slot 6 (west) and Slot 13 (east) carry the protect traffic.

Figure 17-21 Connecting Fiber to a Four-Node, Four-Fiber BLSR



Step 4 Return to your originating procedure (NTP).

DLP-A45 Install the Fiber Boot

Purpose	This task installs the fiber boot, which protects fiber from excessive bending. Fiber boots are required for all OC-N cards except the OC-192, OC192-XFP, and OC-48 AS cards. The boots are not necessary for these cards because of the angled SC connectors on the cards.
Tools/Equipment	Fiber boot
Prerequisite Procedures	NTP-A16 Install Optical Cards and Connectors, page 2-8
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

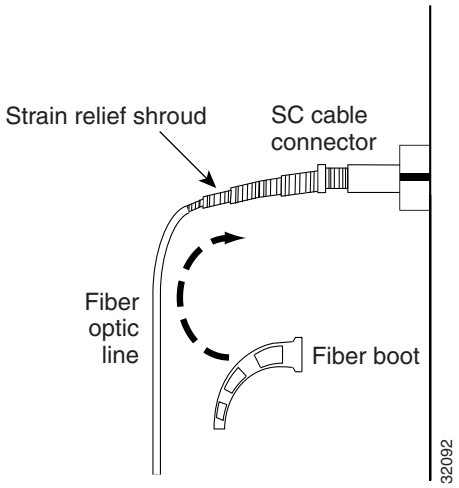
Note You can install the fiber boots on the fiber-optic cables before or after the cables are attached to the OC-N card.

Note On the OC3IR/STM1SH 1310-8 card, you must use a fiber clip instead of a fiber boot on the Port 8 Rx fiber connector.

Step 1 Position the open slot of the fiber boot underneath the fiber cable.

Step 2 Push the fiber cable down into the fiber boot. Figure 17-22 shows the fiber boot attachment.

Figure 17-22 Attaching a Fiber Boot



Step 3 Twist the fiber boot to lock the fiber cable into the tail end of the fiber boot.

Step 4 Slide the fiber boot forward along the fiber-optic cable until the fiber boot fits snugly onto the end of the SC cable connector.

Step 5 Return to your originating procedure (NTP).

DLP-A50 Set Up a Windows PC for Craft Connection to an ONS 15454 on the Same Subnet Using Static IP Addresses

Purpose	This task sets up your computer for a local craft connection to the ONS 15454 when: • You will access nodes running software releases earlier than Software Release 3.3. • You will connect to one ONS 15454; if you will connect to multiple ONS 15454s, you might need to reconfigure your computer's IP settings each time you connect to an ONS 15454. • You need to use non-ONS 15454 applications such as ping and tracert (trace route).
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify the operating system that is installed on your computer:

a. From the Windows Start menu, choose **Settings > Control Panel**.

b. In the Control Panel window, double-click the **System** icon.

c. On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows NT 4.0, Windows 2000, or Windows XP.

Step 2 According to the Windows operating system installed on your computer, perform one of the following steps:

- For Windows 98, complete Step 3.
- For Windows NT 4.0, complete Step 4.
- For Windows 2000, complete Step 5.
- For Windows XP, complete Step 6.

Step 3 If you have Windows 98 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings > Control Panel**.

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, choose **TCP/IP** for your NIC card, then click **Properties**.

d. In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.

e. Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.

f. Click the **IP Address** tab.

g. In the IP Address window, click **Specify an IP address**.

h. In the IP Address field, enter an IP address that is identical to the ONS 15454 IP address except for the last octet. The last octet must be 1 or 3 through 254. This IP address appears on the LCD unless its display is suppressed during node provisioning.

i. In the Subnet Mask field, type the same subnet mask as the ONS 15454. The default is **255.255.255.0** (24 bit).

j. Click **OK**.

k. In the TCP/IP dialog box, click the **Gateway** tab.

l. In the New Gateway field, type the ONS 15454 IP address. Click **Add**.

m. Verify that the IP address appears in the Installed Gateways field, then click **OK**.

n. When the prompt to restart your PC appears, click **Yes**.

Step 4 If you have Windows NT 4.0 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings > Control Panel**.

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, click the **Protocols** tab, choose **TCP/IP Protocol**, then click **Properties**.

d. Click the **IP Address** tab.

e. In the IP Address window, click **Specify an IP address**.

f. In the IP Address field, enter an IP address that is identical to the ONS 15454 IP address except for the last octet. The last octet must be 1 or 3 through 254. This IP address appears on the LCD unless its display is suppressed during node provisioning.

g. In the Subnet Mask field, type **255.255.255.0**.

h. Click **Advanced**.

i. In the Gateways List, click **Add**. The TCP/IP Gateway Address dialog box appears.

j. Type the ONS 15454 IP address in the Gateway Address field.

k. Click **Add**.

l. Click **OK**.

m. Click **Apply**.

n. In some cases, Windows NT 4.0 prompts you to reboot your PC. If you receive this prompt, click **Yes**.

Step 5 If you have Windows 2000 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings > Network and Dial-up Connections > Local Area Connection**.

b. In the Local Area Connection Status dialog box, click **Properties**.

c. On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. Click **Use the following IP address**.

e. In the IP Address field, enter an IP address that is identical to the ONS 15454 IP address except for the last octet. The last octet must be 1 or 3 through 254. This IP address appears on the LCD unless its display is suppressed during node provisioning.

f. In the Subnet Mask field, type **255.255.255.0**.

g. In the Default Gateway field, type the ONS 15454 IP address.

h. Click **OK**.

i. In the Local Area Connection Properties dialog box, click **OK**.

j. In the Local Area Connection Status dialog box, click **Close**.

Step 6 If you have Windows XP installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Control Panel > Network Connections**.

Note If the Network Connections menu is not available, click **Switch to Classic View**.

b. From the Network Connections dialog box, click the **Local Area Connection** icon.

c. From the Local Area Connection Properties dialog box, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. In the IP Address field, enter an IP address that is identical to the ONS 15454 IP address except for the last octet. The last octet must be 1 or 3 through 254. This IP address appears on the LCD unless its display is suppressed during node provisioning.

e. In the Subnet Mask field, type **255.255.255.0**.

f. In the Default Gateway field, type the ONS 15454 IP address.

g. Click **OK**.

h. In the Local Area Connection Properties dialog box, click **OK**.

i. In the Local Area Connection Status dialog box, click **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-A51 Set Up a Windows PC for Craft Connection to an ONS 15454 Using Dynamic Host Configuration Protocol

Purpose	This task sets up your computer for craft connection to the ONS 15454 using Dynamic Host Configuration Protocol (DHCP).
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1 NTP-A169 Set Up CTC Network Access, page 4-8
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Do not use this task for initial node turn-up. Use the task only if DHCP forwarding is enabled on the ONS 15454. By default, DHCP is not enabled. To enable it, see the "NTP-A169 Set Up CTC Network Access" procedure on page 4-8.

Note The ONS 15454 does not provide the IP addresses. If DHCP forwarding is enabled, it passes DCHP requests to an external DHCP server.

Step 1 Verify the operating system that is installed on your computer:

a. From the Windows Start menu, choose **Settings > Control Panel**.

b. In the Control Panel window, double-click the **System** icon.

c. On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows NT 4.0, Windows 2000, or Windows XP.

Step 2 According to the Windows operating system installed on your computer, perform one of the following steps:

- For Windows 98, complete Step 3.
- For Windows NT 4.0, complete Step 4.
- For Windows 2000, complete Step 5.
- For Windows XP, complete Step 6.

Step 3 If you have Windows 98 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings > Control Panel**.

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, select **TCP/IP** for your NIC, then click **Properties**.

d. In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.

e. Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.

f. Click the **IP Address** tab.

g. In the IP Address window, click **Obtain an IP address automatically**.

h. Click **OK**.

i. When the prompt to restart your PC appears, click **Yes**.

Step 4 If you have Windows NT 4.0 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings > Control Panel**.

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, click the **Protocols** tab, choose **TCP/IP Protocol**, then click **Properties**.

d. Click the **IP Address** tab.

e. In the IP Address window, click **Obtain an IP address from a DHCP server**.

f. Click **OK**.

g. Click **Apply**.

h. If Windows prompts you to restart your PC, click **Yes**.

Step 5 If you have Windows 2000 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings > Network and Dial-up Connections > Local Area Connection**.

b. In the Local Area Connection Status dialog box, click **Properties**.

c. On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. Click **Obtain an IP address from a DHCP server**.

e. Click **OK**.

f. In the Local Area Connection Properties dialog box, click **OK**.

g. In the Local Area Connection Status dialog box, click **Close**.

Step 6 If you have Windows XP installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Control Panel > Network Connections.**

Note If the Network Connections menu is not available, click **Switch to Classic View**.

b. In the Network Connections dialog box, click **Local Area Connection**.

c. In the Local Area Connection Status dialog box, click **Properties**.

d. On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

e. Click **Obtain an IP address from a DHCP server**.

f. Click **OK**.

g. In the Local Area Connection Properties dialog box, click **OK**.

h. In the Local Area Connection Status dialog box, click **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-A52 Set Up a Windows PC for Craft Connection to an ONS 15454 Using Automatic Host Detection

Purpose	This task sets up your computer for local craft connection to the ONS 15454 when: • You will connect to the ONS 15454 Ethernet port or backplane LAN pins either directly or through a hub. • All nodes that you will access are running Software Release 3.3 or later. • You will connect to multiple ONS 15454s and do not want to reconfigure your IP address each time. • You do not need to access non-ONS 15454 applications such as ping and tracert (trace route).
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify the operating system that is installed on your computer:

a. From the Windows Start menu, choose **Settings > Control Panel**.

Note In Windows XP, you can select Control Panel directly from the Windows Start menu. Make sure you are in Classic View before continuing with this procedure.

b. In the Control Panel window, double-click the **System** icon.

c. On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows NT 4.0, Windows 2000, or Windows XP.

Step 2 According to the Windows operating system installed on your computer, perform one of the following steps:

- For Windows 98, complete Step 3.
- For Windows NT 4.0, complete Step 4.
- For Windows 2000, complete Step 5.
- For Windows XP, complete Step 6.

Step 3 If you have Windows 98 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings > Control Panel**.

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, select **TCP/IP** for your NIC, then click **Properties**.

d. In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.

e. Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.

f. Click the **IP Address** tab.

g. In the IP Address window, click **Specify an IP address**.

h. In the IP Address field, enter any legitimate IP address other than the node IP address.

i. In the Subnet Mask field, type the same subnet mask as the ONS 15454. The default is **255.255.255.0** (24 bit).

j. Click **OK**.

k. In the TCP/IP dialog box, click the **Gateway** tab.

l. In the New Gateway field, type the address entered in Step h. Click **Add**.

m. Verify that the IP address appears in the Installed Gateways field, then click **OK**.

n. When the prompt to restart your PC appears, click **Yes**.

Step 4 If you have Windows NT 4.0 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings > Control Panel**.

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, click the **Protocols** tab, choose **TCP/IP Protocol**, then click **Properties**.

d. Click the **IP Address** tab.

e. In the IP Address window, click **Specify an IP address**.

f. In the IP Address field, enter any legitimate IP address other than the node IP address.

g. In the Subnet Mask field, type the same subnet mask as the ONS 15454. The default is **255.255.255.0** (24 bit).

h. Click **Advanced**.

i. In the Gateways List, click **Add**. The TCP/IP Gateway Address dialog box appears.

j. Type the IP address entered in Step f in the Gateway Address field.

k. Click **Add**.

l. Click **OK**.

m. Click **Apply**.

n. Reboot your PC.

Step 5 If you have Windows 2000 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings > Network and Dial-up Connections > Local Area Connection**.

b. In the Local Area Connection Status dialog box, click **Properties**.

c. On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. Click **Use the following IP address**.

e. In the IP Address field, enter any legitimate IP address other than the node IP address.

f. In the Subnet Mask field, type the same subnet mask as the ONS 15454. The default is **255.255.255.0** (24 bit).

g. Type the IP address entered in Step e in the Gateway Address field.

h. Click **OK**.

i. In the Local Area Connection Properties dialog box, click **OK**.

j. In the Local Area Connection Status dialog box, click **Close**.

Step 6 If you have Windows XP installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Control Panel > Network Connections**.

Note If the Network Connections menu is not available, click **Switch to Classic View**.

b. From the Network Connections dialog box, click the **Local Area Connection** icon to select it. Right-click and select **Properties**.

c. From the Local Area Connection Properties dialog box, click on **Internet Protocol (TCP/IP)** to select it, then click **Properties**.

d. In the IP Address field, enter any legitimate IP address other than the node IP address as indicated on the LCD of the ONS 15454. The default IP address is 192.1.0.2.

e. In the Subnet Mask field, type the same subnet mask as the ONS 15454. The default is **255.255.255.0** (24 bit).

f. Type the IP address entered in Step d in the Gateway Address field.

g. Click **OK**.

h. In the Local Area Connection Properties dialog box, click **OK**.

i. In the Local Area Connection Status dialog box, click **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-A54 Hard-Reset a CE-100T-8 Card Using CTC

Purpose	This task hard-resets the CE-100T-8 Ethernet card without requiring physical removal.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution A hard reset causes a traffic hit.

Note The hard-reset option is enabled only when the card is in the OOS-MA, MT service state.

Step 1 In node view click the **Inventory** tab. Locate the appropriate card in the inventory pane.

Step 2 Click the **Admin State** drop-down menu and select **OOS-MT,MA**. Click **Apply**.

Step 3 Click **Yes** in the "Action may be service affecting. Are you sure?" dialog box.

Step 4 The service state of the card becomes Locked enabled, loopback & maintenance. The card's faceplate appears blue in CTC and the SRV LED turns amber.

Step 5 Right-click the card to reveal a pop-up menu.

Step 6 Click **Hard-reset Card**.

Step 7 Click **Yes** in the "Are you sure you want to hard-reset this card?" dialog box.

Step 8 Return to your originating procedure (NTP).

DLP-A56 Disable Proxy Service Using Internet Explorer (Windows)

Purpose	This task disables proxy service for PCs running Internet Explorer.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	Required if your computer is connected to a network computer proxy server and your browser is Internet Explorer.
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 From the Windows Start menu, select **Settings > Control Panel**.

Note If your computer is running Windows XP, you can select Control Panel directly from the Windows Start menu. Make sure that you are in Classic View before continuing with this procedure.

Step 2 In the Control Panel window, choose **Internet Options**.

Step 3 In the Internet Properties dialog box, click **Connections > LAN Settings**.

Step 4 In the LAN Settings dialog box, complete one of the following tasks:

- Uncheck **Use a proxy server** to disable the service.
- Leave **Use a proxy server** selected and click **Advanced**. In the Proxy Setting dialog box under Exceptions, enter the IP addresses of ONS 15454 nodes that you will access. Separate each address with a semicolon. You can insert an asterisk (*) for the host number to include all the ONS 15454s on your network. Click **OK** to close each open dialog box.

Note For ONS 15454 nodes that have TCC2P cards installed with the TCC2P secure mode option enabled, enter the backplane LAN port IP addresses. If the node is in secure mode and the configuration has been locked, you will not be able to change the IP address unless the lock is disabled by Cisco Technical Support. See the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual* for more information about secure mode.

Step 5 Return to your originating procedure (NTP).

DLP-A57 Disable Proxy Service Using Netscape (Windows and UNIX)

Purpose	This task disables proxy service for PCs and UNIX workstations running Netscape. You must perform this task if your computer is connected to a network computer proxy server and your browser is Netscape.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Open Netscape.

Step 2 From the Edit menu, choose **Preferences**.

Step 3 In the Preferences dialog box under Category, choose **Advanced > Proxies**.

Step 4 On the right side of the Preferences dialog box under Proxies, perform one of the following options:

- Choose **Direct connection to the Internet** to bypass the proxy server.

- Choose **Manual proxy configuration** to add exceptions to the proxy server, then click **View**. In the Manual Proxy Configuration dialog box under Exceptions, enter the IP addresses of the ONS 15454 nodes that you will access. Separate each address with a comma. Click **OK** to close each open dialog box.

Note For ONS 15454 nodes that have TCC2P cards installed with the TCC2P secure mode option enabled, enter the backplane LAN port IP addresses. If the node is in secure mode and the configuration has been locked, you will not be able to change the IP address unless the lock is disabled by Cisco Technical Support. See the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual* for more information about secure mode.

Step 5 Return to your originating procedure (NTP).

DLP-A598 Disable Proxy Service Using Mozilla Firefox (Windows and UNIX)

Purpose	This task disables proxy service for PCs and UNIX workstations running Mozilla Firefox.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As Needed
Onsite/Remote	Onsite or remote
Security Level	None

Note You must perform this task if your computer is connected to a network computer proxy server and your browser is Mozilla Firefox.

Step 1 Open Mozilla Firefox.

Step 2 From the Tools menu, choose **Options**.

Step 3 In the Options dialog box under the Network tab, click **Settings**.

Step 4 In the Connection Settings dialog box, perform one of the following options, as applicable:

- Choose the **No Proxy** radio button to disable the proxy service.
- Choose **Manual proxy configuration** to add exceptions to the proxy server. In the **No Proxy for** option under the Manual Proxy Configuration, enter the IP addresses of the ONS 15454 nodes that you access. Separate each address with a comma. Click **OK** to close each open dialog box.

Note For ONS 15454 nodes that have TCC2P cards installed with the TCC2P secure mode option enabled, enter the backplane LAN port IP addresses. If the node is in secure mode and the configuration has been locked, you will not be able to change the IP address unless the lock is disabled by Cisco Technical Support. See the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual* for additional information about secure mode.

Step 5 Return to your originating procedure (NTP).

DLP-A60 Log into CTC

Purpose	This task logs a user into Cisco Transport Controller (CTC).
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1 One of the following procedures: • NTP-A234 Set Up CTC Computer for Local Craft Connection to the ONS 15454, page 3-3 • NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454, page 3-5 • NTP-A236 Set Up a Remote Access Connection to the ONS 15454, page 3-6
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note For information about CTC views and navigation, see Appendix A, "CTC Information and Shortcuts."

Step 1 From the computer connected to the ONS 15454, start Netscape (PC or UNIX) or Mozilla Firefox (PC only):

- If you are using a PC, launch Netscape or Mozilla Firefox from the Windows Start menu or a shortcut icon.
- If you are using UNIX, launch Netscape from the command line by typing:
  - To install Netscape colors for Netscape use, type:

    ```
    # netscape -install
    ```

  - To limit Netscape to 32 colors so that if the requested color is not available, Netscape chooses the closest color option, type:

    ```
    netscape -ncols 32
    ```

Note Netscape or Internet Explorer can be used for IPv4 address and Mozilla Firefox or Netscape can be used for IPv6 address.

Note CTC requires a full 24-color palette to run properly. When using color-intensive applications such as Netscape in UNIX, it is possible that UNIX might run out of colors to use for CTC. The -install or the -ncols 32 command line options limit the number of colors that Netscape uses.

Step 2 In the Netscape or Mozilla Firefox web address (URL) field, enter the ONS 15454 IPv4/v6 address. For initial setup, the default IP address is 192.1.0.2. (This IP address can appear on the LCD. You can suppress the LCD IP address display using CTC. For more information, see the "DLP-A266 Change IP Settings" task on page 19-50.) Press **Enter**.

To log into CTC using an IPv6 address, you must first log into CTC using an IPv4 address and assign an IPv6 address for the node. Use the IPv6 address that you assigned to the node to log into CTC. For more information about configuring IPv6 address, see "DLP-A249 Provision IP Settings" section on page 19-30. You need to enter the IPv6 address in the format [*IPv6 address*] in the address bar of the browser.

Note If you are logging into ONS 15454 nodes running different releases of CTC software, log into the node running the most recent release. If you log into a node running an older release, you will receive an INCOMPATIBLE-SW alarm for each node in the network running a new release, and CTC will not be able to manage these nodes. To check the software version of a node, select About CTC from the CTC Help menu. This will display the ONS 15454 software version for each node visible on the network view. If the node is not visible, the software version can be read from the LCD display. To resolve an alarm, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

If a Java Plug-in Security Warning dialog box appears, complete the "DLP-A418 Install Public-Key Security Certificate" task on page 21-5 to install the public-key security certificate required by Software Release 4.1 and later.

After you complete the security certificate dialog box (or if the certificate is already installed), a Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments. If this is the first login, CTC caching messages appear while CTC files are downloaded to your computer. The first time you connect to an ONS 15454, this process can take several minutes. After the download, a warning message window appears (Figure 17-23).

Figure 17-23 Warning Message Window

Step 3 Click **OK** to consent to the message. The CTC Login dialog box appears (Figure 17-24).

Figure 17-24 Logging into CTC

Step 4 In the Login dialog box, type a user name and password (both are case sensitive). For initial setup, type the user name **CISCO15** and the password **otbu+1**.

Note The CISCO15 user is provided with every ONS 15454. CISCO15 has superuser privileges, so you can create other users. You must create another superuser before you can delete the CISCO15 user. CISCO15 is delivered with the otbu+1 password. To change the password for CISCO15, click the Provisioning > Security tabs after you log in and change the password. To set up ONS 15454 users and assign security, go to the "NTP-A30 Create Users and Assign Security" procedure on page 4-4. Additional information about security is provided in the "Security" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 5 Each time you log into an ONS 15454, you can make selections on the following login options:

- Additional Nodes—Displays a list of current login node groups. To create a login node group or add additional groups, see the "DLP-A61 Create Login Node Groups" task on page 17-63.
- Disable Network Discovery—Check this box to view only the ONS 15454 (and login node group members, if any) entered in the Node Name field. Nodes linked to this node through DCCs are not discovered and will not appear in CTC network view. Using this option can decrease the CTC startup time in networks with many DCC-connected nodes, and reduce memory consumption.
- Disable Circuit Management—Check this box to disable discovery of existing circuits. Using this option can decrease the CTC initialization time in networks with many existing circuits and reduce memory consumption. This option does not prevent the creation and management of new circuits.

Step 6 If you keep Disable Network Discovery unchecked, CTC attempts to upgrade the CTC software by downloading more recent versions of the JAR files it finds during the network discovery. Click **Yes** to allow CTC to download the newer JAR files, or **No** to prevent CTC from downloading the JAR files.

Note Upgrading the CTC software will overwrite your existing software. You must restart CTC after the upgrade is complete.

Step 7 Click **Login**.

If the login is successful, the CTC window appears. From here, you can navigate to other CTC views to provision and manage the ONS 15454. If you need to turn up the shelf for the first time, see Chapter 4, "Turn Up a Node." If login problems occur, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 8 Return to your originating procedure (NTP).

DLP-A61 Create Login Node Groups

Purpose	This task creates a login node group to display ONS 15454s that have an IP connection but not a DCC connection to the login node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu in node view, choose **Preferences**.

Step 2 Click **Login Node Group** and **Create Group**.

Step 3 Enter a name for the group in the Create Login Group Name dialog box. Click **OK**.

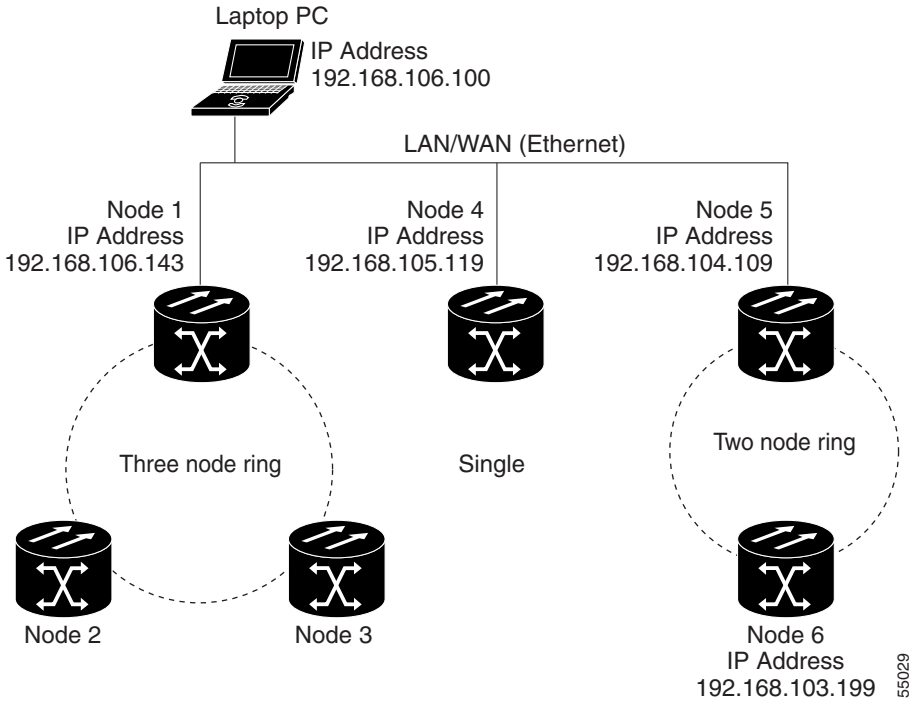
Step 4 In the Members area, type the IP address (or node name) of a node you want to add to the group. Click **Add**. Repeat this step for each node that you want to add to the group.

Note If the ONS 15454 that you want to add to the login node group has TCC2P cards installed and the TCC2P secure mode option is enabled, enter the backplane LAN port IP address. If the node is in secure mode and the configuration has been locked, you will not be able to change the IP address unless the lock is disabled by Cisco Technical Support. See the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual* for more information about secure mode.

Step 5 Click **OK**.

The next time you log into an ONS 15454, the login node group will be available in the Additional Nodes list of the Login dialog box. For example, in Figure 17-25, a login node group is created that contains the IP addresses for Nodes 1, 4, and 5. During login, if you choose this group from the Additional Nodes list and Disable Network Discovery is not selected, all nodes in the figure appear. If the login group and Disable Network Discovery are both selected, Nodes 1, 4, and 5 appear. You can create as many login groups as you need. The groups are stored in the CTC preferences file and are not visible to other users.

Figure 17-25 Login Node Group



Step 6 Return to your originating procedure (NTP).

DLP-A62 Add a Node to the Current Session or Login Group

Purpose	This task adds a node to the current CTC session or login node group.
Tools	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the CTC File menu, click **Add Node**.

Step 2 In the Add Node dialog box, enter the node name (or IP address).

If the ONS 15454 that you want to add has TCC2P cards installed and the TCC2P secure mode option is enabled, enter the backplane LAN port IP address.

Note If the node is in secure mode, the backplane IP address display might be disabled. A Superuser can reenable the IP address display. If the node is in secure mode and the configuration has been locked, you will not be able to change the IP address unless the lock is disabled by Cisco Technical Support. See the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual* for more information about secure mode.

Step 3 If you want to add the node to the current login group, check **Add to current login node group**. Otherwise, leave it unchecked.This check box is active only if you selected a login group when you logged into CTC.

Step 4 Click **OK**.

After a few seconds, the new node appears on the network view map.

Step 5 Return to your originating procedure (NTP).

DLP-A64 Set the IP Address, Default Router, and Network Mask Using the LCD

Purpose	This task changes the ONS 15454 IPv4 address, default router, and network mask using the LCD on the fan-tray assembly. Use this task if you cannot log into CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A36 Install the TCC2/TCC2P Cards, page 17-37
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note You cannot perform this task if the LCD IP Display on the node view Provisioning > Network tab is set to Display Only or Suppress Display. See "DLP-A249 Provision IP Settings" task on page 19-30 to view or change the LCD IP Display field. If the node is locked in secure mode with the LCD display disabled, you will not be able to change this provisioning unless the lock is disabled by Cisco Technical Support. Refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual* for more information about secure mode.

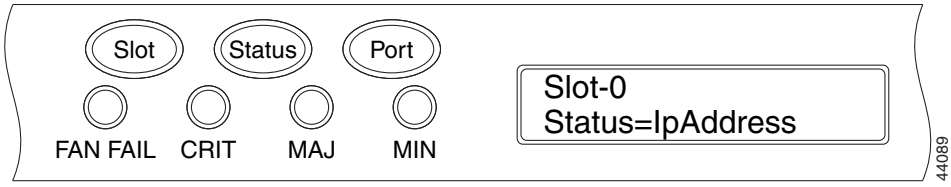
Note The LCD reverts to normal display mode after 5 seconds of button inactivity. IPv6 cannot be configured using the LCD push buttons.

Step 1 On the ONS 15454 front panel, repeatedly press the **Slot** button until Node appears on the LCD.

Step 2 Repeatedly press the **Port** button until the following displays:

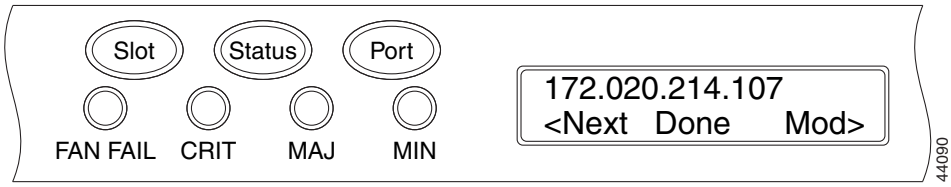
- To change the node IP address, Status=IpAddress (Figure 17-26)
- To change the node network mask, Status=Net Mask
- To change the default router IP address, Status=Default Rtr

Figure 17-26 Selecting the IP Address Option



Step 3 Press the **Status** button to display the node IP address (Figure 17-27), the node subnet mask length, or the default router IP address.

Figure 17-27 Changing the IP Address



Step 4 Push the **Slot** button to move to the IP address or subnet mask digit you need to change. The selected digit flashes.

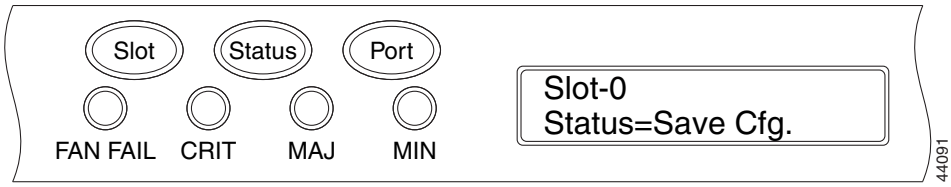
Tip The Slot, Status, and Port button positions correspond to the command position on the LCD. For example, in Figure 17-27, you press the Slot button to invoke the Next command and the Port button to invoke the Done command.

Step 5 Press the **Port** button to cycle the IP address or subnet mask to the correct digit.

Step 6 When the change is complete, press the **Status** button to return to the Node menu.

Step 7 Repeatedly press the **Port** button until the Save Configuration option appears (Figure 17-28).

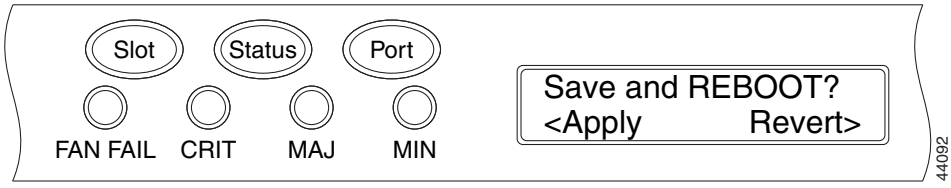
Figure 17-28 Selecting the Save Configuration Option



Step 8 Press the **Status** button to choose the Save Configuration option.

A Save and REBOOT message appears (Figure 17-29).

Figure 17-29 Saving and Rebooting the TCC2/TCC2P



Step 9 Press the **Slot** button to apply the new IP address configuration or press **Port** to cancel the configuration.

Saving the new configuration causes the TCC2/TCC2P cards to reboot. During the reboot, a "Saving Changes - TCC Reset" message displays on the LCD. The LCD returns to the normal alternating display after the TCC2/TCC2P reboot is complete.

Note The IP address and default router must be on the same subnet. If not, you cannot apply the configuration.

Step 10 Return to your originating procedure (NTP).

DLP-A65 Create a Static Route

Purpose	This task creates a static route to establish CTC connectivity to a computer on another network.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	Required if either of the following conditions is true: • CTC computers on one subnet need to connect to ONS 15454s that are connected by a router to ONS 15454s residing on another subnet. OSPF is not enabled and the ENE gateway setting is not checked. • You need to enable multiple CTC sessions among ONS 15454s residing on the same subnet and the ENE gateway setting is not enabled.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Network** tabs.

Step 2 Click the **Static Routing** tab. Click **Create**.

Step 3 In the Create Static Route dialog box, enter the following:

- Destination—Enter the IP address of the computer running CTC. To limit access to one computer, enter the full IP address and a subnet mask of 255.255.255.255. To allow access to all computers on the 192.168.1.0 subnet, enter 192.168.1.0 and a subnet mask of 255.255.255.0. You can enter a destination of 0.0.0.0 to allow access to all CTC computers that connect to the router.
- Mask—Enter a subnet mask. If the destination is a host route (that is, one CTC computer), enter a 32-bit subnet mask (255.255.255.255). If the destination is a subnet, adjust the subnet mask accordingly, for example, 255.255.255.0. If the destination is 0.0.0.0, CTC automatically enters a subnet mask of 0.0.0.0 to provide access to all CTC computers. You cannot change this value.
- Next Hop—Enter the IP address of the router port or the node IP address if the CTC computer is connected to the node directly.
- Cost—Enter the number of hops between the ONS 15454 and the computer.

Step 4 Click **OK**. Verify that the static route appears in the Static Route window.

Note Static route networking examples are provided in the "Management Network Connectivity" chapter of the *Cisco ONS 15454 Reference Manual*.

Step 5 Return to your originating procedure (NTP).

DLP-A67 Provision the IIOP Listener Port on the ONS 15454

Purpose	This task sets the Internet Inter-ORB Protocol (IIOP) listener port on the ONS 15454, which enables you to access ONS 15454s that reside behind a firewall.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If the Enable SOCKS Proxy Server on port 1080 check box is checked, CTC will use port 1080 and ignore the configured IIOP port setting. If Enable SOCKS Proxy Server is subsequently unchecked, the configured IIOP listener port will be used.

Step 1 In node view, click the **Provisioning** > **Security** > **Access** tabs.

Step 2 In the TCC CORBA (IIOP) Listener Port area, choose a listener port option:

- Default - TCC Fixed—Select this option if the ONS 15454s are on the same side of the firewall as the CTC computer or if no firewall is used (default). This option sets the ONS 15454 listener port to Port 57790. It can be used for access through a firewall if Port 57790 is open.
- Standard Constant—Select this option to use Port 683, the CORBA default port number, as the ONS 15454 listener port.
- Other Constant—If port 683 is not used, type the IIOP port specified by your firewall administrator.

Step 3 Click **Apply**.

Step 4 When the Change Network Configuration message appears, click **Yes**.

Both ONS 15454 TCC2/TCC2P cards reboot, one at a time. The reboot takes approximately 15 minutes.

Step 5 Return to your originating procedure (NTP).

DLP-A68 Provision the IIOP Listener Port on the CTC Computer

Purpose	This task selects the IIOP listener port on CTC. You must perform this task if the computer running CTC resides behind a firewall.
Tools/Equipment	IIOP listener port number from LAN or firewall administrator.
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **Firewall** tab.

Step 3 In the CTC CORBA (IIOP) Listener Port area, choose a listener port option:

- Default - Variable—Select this option if the ONS 15454s are on the same side of the firewall as the CTC computer or if no firewall is used (default). This option sets the CTC listener port to Port 57790. It can be used for access through a firewall if Port 57790 is open.
- Standard Constant—Select this option to use Port 683, the CORBA default port number, as the CTC computer listener port.
- Other Constant—If Port 683 is not used, enter the IIOP port defined by your administrator.

Step 4 Click **Apply**. A warning appears telling you that the port change will apply during the next CTC login.

Step 5 Click **OK**.

Step 6 In the Preferences dialog box, click **OK**.

Step 7 To access the ONS 15454 using the IIOP port, log out of CTC then log back in. (To log out, choose **Exit** from the File menu).

Step 8 Return to your originating procedure (NTP).

DLP-A69 Set Up SONET External or Line Timing

Purpose	This task defines the SONET timing source (external or line) for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 In the Timing Standard area, make sure that the Current Timing Standard is SONET. If it is not, continue with Step 3. If the Current Timing Standard is SONET, skip to Step 4.

Step 3 Click **Change** to switch the timing from SDH to SONET.

Note Changing the timing standard reinitializes the node and might affect traffic.

Step 4 In the General Timing area, complete the following information:

- Timing Mode—Choose **External** if the ONS 15454 derives its timing from a BITS source wired to the backplane pins; choose **Line** if timing is derived from an OC-N card that is optically connected to the timing node. A third option, Mixed, allows you to set both external and line timing references.

Note Because Mixed timing might cause timing loops, Cisco does not recommend its use. Use this mode with care.

- SSM Message Set—Choose a synchronization status messaging (SSM) message set. All ONS 15454s can translate Generation 2 message sets, so choose Generation 2 if the ONS 15454 is connected to other ONS 15454s. Choose Generation 1 only when the ONS 15454 is connected to equipment that does not support Generation 2. If a node that has its SSM message set to Generation 1 receives a Generation 2 message, it maps the message down to the next available Generation 1 message. The transit node clock (TNC) and ST3E (Stratum 3E) will become an ST3 (Stratum 3) clock.
- Quality of RES—If your timing source supports the reserved S1 byte, set the timing quality here. (Most timing sources do not use RES.) Qualities are displayed in descending quality order as ranges. For example, ST3<RES<ST2 means the timing reference is higher than a Stratum 3 and lower than a Stratum 2. Refer to the "Timing" chapter of the *Cisco ONS 15454 Reference Manual* for more information about SSM, including definitions of the SONET timing levels.
- Revertive—Select this check box if you want the ONS 15454 to revert to a primary reference source after the conditions that caused it to switch to a secondary timing reference are corrected.
- Revertive Time—If Revertive is checked, choose the amount of time the ONS 15454 will wait before reverting to its primary timing source. Five minutes is the default.

Step 5 In the Reference Lists area, complete the following information:

Note You can define up to three timing references for the node and up to six BITS Out references. BITS Out references define the timing references used by equipment that can be attached to the node's BITS Out pins on the backplane. If you attach equipment to BITS Out pins, you normally attach it to a node with Line mode because equipment near the external timing reference can be directly wired to the reference.

- NE Reference—Allows you to define three timing references (Ref 1, Ref 2, Ref 3). The node uses Reference 1 unless a failure occurs to that reference, in which case the node uses Reference 2. If Reference 2 fails, the node uses Reference 3, which is typically set to Internal Clock. The internal clock is the Stratum 3 clock provided on the TCC/TCC2P. The options displayed depend on the Timing Mode setting.
- If the Timing Mode is set to External, your options are BITS1, BITS2, and Internal Clock.

- If the Timing Mode is set to Line, your options are the node's working OC-N cards and Internal Clock. Choose the cards/ports that are directly or indirectly connected to the node wired to the BITS source, that is, the node's trunk (span) cards. Set Reference 1 to the trunk card that is closest to the BITS source. For example, if Slot 5 is connected to the node wired to the BITS source, choose Slot 5 as Reference 1.
- If the Timing Mode is set to Mixed, both BITS and OC-N cards are available, allowing you to set a mixture of external BITS and OC-N trunk (span) cards as timing references.
- BITS-1 Out/BITS-2 Out—Define the timing references for equipment wired to the BITS Out pins on the backplane. BITS-1 Out and BITS-2 Out are enabled when BITS-1 and BITS-2 facilities are put in service. If Timing Mode is set to External, choose the OC-N card used to set the timing. If Timing Mode is set to Line, you can choose an OC-N card or choose NE Reference to have the BITS-1 Out and/or BITS-2 Out follow the same timing references as the NE.

Step 6 Click the **BITS Facilities** subtab.

The BITS Facilities section sets the parameters for your BITS1 and BITS2 timing references. Many of these settings are determined by the timing source manufacturer. If equipment is timed through BITS Out, you can set timing parameters to meet the requirements of the equipment.

Step 7 In the BITS In area, complete the following information:

- Facility Type—(TCC2P card only) Choose the BITS signal type supported by your BITS clock, either DS1 or 64Khz+8Khz.
- BITS In State—If Timing Mode is set to External or Mixed, set the BITS In State for BITS-1 and/or BITS-2 to **IS** (in service) depending whether one or both BITS input pin pairs on the MIC are connected to the external timing source. If Timing Mode is set to Line, set the BITS In State to **OOS** (out of service).

Step 8 If BITS In State is set to OOS, continue with Step 9. If the BITS In State is set to IS, complete the following information:

- Coding—Choose the coding used by your BITS reference, either B8ZS (binary 8-zero substitution) or AMI (alternate mark inversion).
- Framing—Choose the framing used by your BITS reference, either ESF (Extended Super Frame) or SF (D4) (Super Frame).
- Sync Messaging—Check this check box to enable SSM. SSM is not available if Framing is set to Super Frame.
- Admin SSM—If the Sync Messaging check box is not checked, you can choose the SSM Generation 2 type from the drop-down list.

Step 9 In the BITS Out area, complete the following information, as needed:

- Facility Type—Choose the BITS Out signal type, either DS1 or 64 Khz.
- BITS Out State—If equipment is connected to the node's BITS output pins on the backplane and you want to time the equipment from a node reference, set the BITS Out State for BITS-1 and/or BITS-2 to **IS**, depending on which BITS Out pins are used for the external equipment. If equipment is not attached to the BITS output pins, set the BITS Out State to **OOS**.

Step 10 If the BITS Out State is set to OOS, continue with Step 11. If BITS Out State is set to IS, complete the following information:

- Coding—Choose the coding used by your BITS reference, either B8ZS or AMI.
- Framing—Choose the framing used by your BITS reference, either ESF or SF (D4).

- AIS Threshold—If SSM is disabled or Super Frame is used, choose the quality level where a node sends an alarm indication signal (AIS) from the BITS 1 Out and BITS 2 Out backplane pins. An AIS alarm is raised when the optical source for the BITS reference falls to or below the SSM quality level defined in this field.
- LBO—If you are timing an external device connected to the BITS Out pins, choose the distance between the device and the ONS 15454. Options are: 0-133 ft. (default), 124-266 ft., 267-399 ft., 400-533 ft., and 534-655 ft. Line build out (LBO) relates to the BITS cable length.

Step 11 Click **Apply**.

Note Refer to the *Cisco ONS 15454 Troubleshooting Guide* for timing-related alarms.

Step 12 Return to your originating procedure (NTP).

Note When provisioning a line timing reference for the node, you cannot select the protect port of a 1+1 protection group. If a traffic switch occurs on the working port of the 1+1 protection group, the timing reference of the node automatically switches to the protect port of the 1+1 protection group.

DLP-A70 Set Up Internal Timing

Purpose	This task sets up internal timing (Stratum 3) for an ONS 15454. Use only if a BITS source is not available.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Internal timing is Stratum 3 and not intended for permanent use. All ONS 15454 nodes should be timed to a Stratum 2 or better primary reference source.

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 In the General Timing area, enter the following:

- Timing Mode—Set to **External**.
- SSM Message Set—Set to **Generation 1**.
- Quality of RES—Does not apply to internal timing.
- Revertive—Does not apply to internal timing.
- Revertive Time—Does not apply to internal timing.

Step 3 In the Reference Lists area, enter the following information:

- NE Reference

  - Ref 1—Set to **Internal Clock**.
  - Ref 2—Set to **Internal Clock**.
  - Ref 3—Set to **Internal Clock**.
- BITS-1 Out/BITS-2 Out—Set to **None**.

Step 4 Click the **Provisioning > Timing > BITS Facilities** tabs.

Step 5 In the BITS Facilities area, change the BITS In State and BITS Out State to **OOS**. Disregard the other BITS Facilities settings; they are not relevant to internal timing.

Step 6 Click **Apply**.

Step 7 Return to your originating procedure (NTP).

DLP-A71 Create a 1:1 Protection Group

Purpose	This task creates a 1:1 electrical card protection group.
Tools/Equipment	Redundant DS-1, DS-3, EC-1, or DS3XM cards should be installed in the shelf, or the ONS 15454 slots must be provisioned for two of these cards.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that the cards required for 1:1 protection are installed according to requirements specified in Table 4-1 on page 4-14.

Step 2 In node view, click the **Provisioning > Protection** tabs.

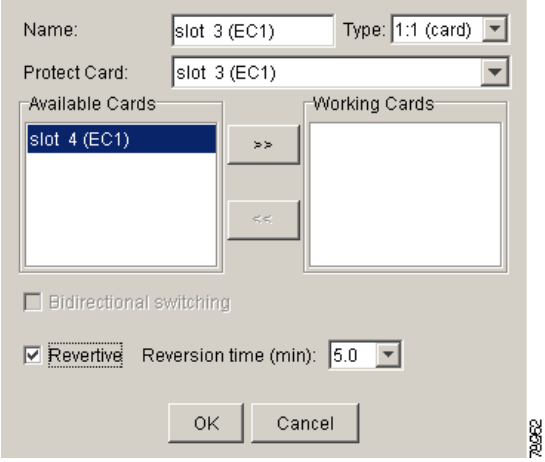
Step 3 Click **Create**.

Step 4 In the Create Protection Group dialog box, enter the following:

- Name—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (“) characters.
- Type—Choose **1:1** from the drop-down list.
- Protect Card—Choose the protect card from the drop-down list. The list displays cards available for 1:1 protection. If no cards are available, no cards appear in the list.

After you choose the protect card, the card available for protection appear in the Available Cards list, as shown in Figure 17-30. If no cards are available, no cards appear. If this occurs, you can not complete this task until you install the physical cards or preprovision the ONS 15454 slots using the “DLP-A330 Preprovision a Card Slot” task on page 20-20.

Figure 17-30 Creating a 1:1 Protection Group



Step 5 From the Available Cards list, choose the card that will be protected by the card selected in the Protect Card drop-down list. Click the top arrow button to move each card to the Working Cards list.

Step 6 Complete the remaining fields:

- Bidirectional switching—Not available for 1:1 protection.
- Revertive—Check this check box if you want traffic to revert to the working card after failure conditions remain corrected for the amount of time entered in the Reversion Time field.

Note When you perform a protection switch, do not change the protection group mode from nonrevertive to revertive or from revertive to nonrevertive.

- Reversion time—If Revertive is checked, choose the reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card after conditions causing the switch are cleared. The reversion timer starts after conditions causing the switch are cleared.

Step 7 Click **OK**, then click **Yes** in the confirmation dialog box.

Step 8 Return to your originating procedure (NTP).

DLP-A72 Create a 1:N Protection Group

Purpose	This task creates a DS-1, DS-3, or SVC-RAN 1:N protection group.
Tools/Equipment	DS1N-14, DS3N-12, DS3N-12E, DS3/EC1-48, or DS1/E1-56 (protect cards); DS1-14, DS3-12, or DS3-12E (working cards). **Note** The DS1N-14, DS3N-12, DS3N-12E, DS3/EC1-48, or DS1/E1-56 protect cards must be installed in Slot 3 or Slot 15, and the cards they protect (DS1-14, DS3-12, DS3-12E) must be on the same side of the shelf.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that the cards are installed according to the 1:N requirements specified in Table 4-1 on page 4-14.

Step 2 Click the **Provisioning** > **Protection** tabs.

Step 3 In the Protection Groups area, click **Create**.

Step 4 In the Create Protection Group dialog box, enter the following:

- Name—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (“) characters.
- Type—Choose **1:N** from the drop-down list.
- Protect Card—Choose the protect card from the drop-down list. The list displays DS1N-14, DS3N-12, DS3/EC1-48, DS3N-12E, or DS1/E1-56 cards (installed in Slots 3 or 15). If these cards are not installed, no cards appear in the drop-down list.

After you choose the protect card, a list of cards available for protection appear in the Available Cards list. If no cards are available, no cards appear. If this occurs, you can not complete this task until you install the physical cards or preprovision the ONS 15454 slots using the “DLP-A330 Preprovision a Card Slot” task on page 20-20.

Step 5 From the Available Cards list, choose the cards that will be protected by the card selected in the Protect Card drop-down list. Click the top arrow button to move each card to the Working Cards list.

Step 6 Complete the remaining fields:

- Bidirectional switching—Not available for 1:N protection.
- Revertive—Always enabled for 1:N protection groups.

Note When you perform a protection switch, do not change the protection group mode from nonrevertive to revertive or from revertive to nonrevertive.

- Reversion time—Click **Reversion time** and select a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card after conditions causing the switch are cleared. The reversion timer starts after conditions causing the switch are cleared.

Step 7 Click **OK**, then click **Yes** in the confirmation dialog box.

Step 8 Return to your originating procedure (NTP).

DLP-A73 Create a 1+1 Protection Group

Purpose	This task creates a 1+1 protection group for any OC-N card/port (OC-3, OC3-8, OC-12, OC12-4, OC-48, OC-48 AS, OC-192, MRC-12, MRC-2.5G-4, OC192SR1/STM64IO Short Reach, and OC192/STM64 Any Reach cards).
Tools/Equipment	Installed OC-N cards or preprovisioned slots
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that the cards are installed according to 1+1 requirements specified in Table 4-1 on page 4-14.

Step 2 In node view, click the **Provisioning** > **Protection** tabs.

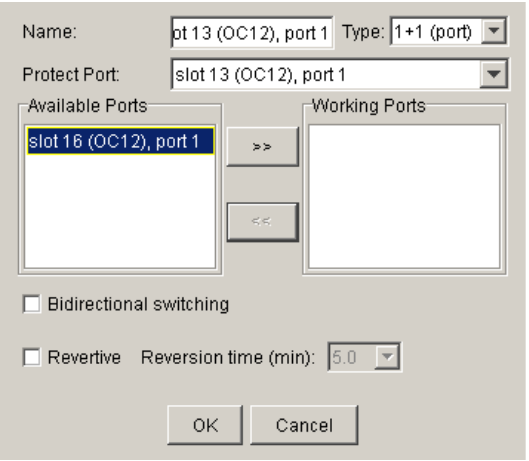
Step 3 In the Protection Groups area, click **Create**.

Step 4 In the Create Protection Group dialog box, enter the following:

- Name—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (“) characters.
- Type—Choose **1+1** from the drop-down list.
- Protect Port—Choose the protect port from the drop-down list. The list displays the available OC-N ports, as shown in Figure 17-31 on page 17-77. If OC-N cards are not installed, no ports appear in the drop-down list.

After you choose the protect port, a list of ports available for protection appear in the Available Ports list, as shown in Figure 17-31. If no cards are available, no ports appear. If this occurs, you can not complete this task until you install the physical cards or preprovision the ONS 15454 slots using the “DLP-A330 Preprovision a Card Slot” task on page 20-20.

Figure 17-31 Creating a 1+1 Protection Group



Step 5 From the Available Ports list, choose the port that will be protected by the port you selected in the Protect Port field. Click the top arrow button to move each port to the Working Ports list.

Step 6 Complete the remaining fields:

- Bidirectional switching—Check this check box if you want both Tx and Rx signals to switch to the protect port when a failure occurs to one signal. Leave unchecked if you want only the failed signal to switch to the protect port.
- Revertive—Check this check box if you want traffic to revert to the working card after failure conditions remain corrected for the amount of time entered in the Reversion Time field.

Note When you perform a protection switch, do not change the protection group mode from nonrevertive to revertive or from revertive to nonrevertive.

- Reversion time—If Revertive is checked, choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. Reversion time is the amount of time that will elapse before the traffic reverts to the working card after conditions causing the switch are cleared. The reversion timer starts after conditions causing the switch are cleared.

Step 7 Click **OK**.

Step 8 Return to your originating procedure (NTP).

Note When provisioning a line timing reference for the node, you cannot select the protect port of a 1+1 protection group. If a traffic switch occurs on the working port of the 1+1 protection group, the timing reference of the node automatically switches to the protect port of the 1+1 protection group.

DLP-A74 Create a New User on a Single Node

Purpose	This task creates a new user for one ONS 15454 node.
Tools/Equipment	None

Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning > Security > Users** tabs.

Step 2 In the Users window, click **Create**.

Step 3 In the Create User dialog box, enter the following:

- Name—Type the user name. The name must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters. For TL1 compatibility, the user name must be 6 to 10 characters.
- Password—Type the user password. The password length, by default, is set to a minimum of six and a maximum of 20. You can configure the default values in node view through Provisioning > NE Defaults > Node > security > passwordComplexity. The minimum length can be set to eight, ten or twelve characters, and the maximum length to 80 characters. The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters, where at least two characters are nonalphabetic and at least one character is a special character. For TL1 compatibility, the password must be 6 to 10 characters. The password must not contain the user name.
- Confirm Password—Type the password again to confirm it.
- Security Level—Choose a security level for the user: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. Refer to the "Security" chapter in the *Cisco ONS 15454 Reference Manual* for information about the capabilities provided with each level.

Note Each security level has a different idle time. The idle time is the length of time that CTC can remain idle before the password must be reentered. The defaults are: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes. To change the idle times, refer to the "NTP-A205 Modify Users and Change Security" procedure on page 11-7.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-A75 Create a New User on Multiple Nodes

Purpose	This task adds a new user to multiple ONS 15454 nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note All nodes where you want to add users must be accessible in network view.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > Security > Users** tabs.

Step 3 In the Users window, click **Create**.

Step 4 In the Create User dialog box, enter the following:

- Name—Type the user name. The name must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters. For TL1 compatibility, the user name must 6 to 10 characters.
- Password—Type the user password. The password length, by default, is set to a minimum of six and a maximum of 20. You can configure the default values in node view through Provisioning > NE Defaults > Node > security > passwordComplexity. The minimum length can be set to eight, ten or twelve characters, and the maximum length to 80 characters. The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #, %) characters, where at least two characters are nonalphabetic and at least one character is a special character. For TL1 compatibility, the password must be 6 to 10 characters. The password must not contain the user name.
- Confirm Password—Type the password again to confirm it.
- Security Level—Choose a security level for the user: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. Refer to the "Security" chapter in the *Cisco ONS 15454 Reference Manual* for information about the capabilities provided with each level.

Note Each security level has a different idle time. The idle time is the length of time that CTC can remain idle before it locks up and the password must be reentered. The defaults are: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes. To change the idle times, refer to the "NTP-A205 Modify Users and Change Security" procedure on page 11-7.

Step 5 Under "Select applicable nodes," deselect any nodes where you do not want to add the user (all network nodes are selected by default).

Step 6 Click **OK**.

Step 7 In the User Creation Results dialog box, verify that the user was added to all the nodes chosen in Step 5. If not, click **OK** and repeat Steps 2 through 6. If the user was added to all nodes, click **OK** and continue with the next step.

Step 8 Return to your originating procedure (NTP).

DLP-A83 Provision Orderwire

Purpose	This task provisions orderwire on the AIC-I card.
Tools/Equipment	An AIC-I card must be installed in Slot 9. OC-N cards must be installed.

Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the network view, click the **Provisioning > Overhead Circuits** tabs.

Step 2 Click **Create**.

Step 3 In the Overhead Circuit Creation dialog box, complete the following fields in the Circuit Attributes area:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces).
- Circuit Type—Choose either **Local Orderwire** or **Express Orderwire** depending on the orderwire path that you want to create. If regenerators are not used between ONS 15454 nodes, you can use either local or express orderwire channels. If regenerators exist, use the express orderwire channel. You can provision up to four ONS 15454 OC-N ports for each orderwire path.
- PCM—Choose the Pulse Code Modulation voice coding and companding standard, either Mu_Law (North America, Japan) or A_Law (Europe). The provisioning procedures are the same for both types of orderwire.

Caution When provisioning orderwire for ONS 15454 nodes residing in a ring, do not provision a complete orderwire loop. For example, a four-node ring typically has east and west ports provisioned at all four nodes. However, to prevent orderwire loops, provision two orderwire ports (east and west) at all but one of the ring nodes.

Step 4 Click **Next**.

Step 5 In the Circuit Source area, complete the following:

- Node—Choose the source node.
- Slot—Choose the source slot.
- Port—If displayed, choose the source port.

Step 6 Click **Next**.

Step 7 In the Circuit Destination area, complete the following:

- Node—Choose the destination node.
- Slot—Choose the destination slot.
- Port—If displayed, choose the destination port.

Step 8 Click **Finish**.

Step 9 Return to your originating procedure (NTP).

DLP-A88 Optical 1+1 Protection Test

Purpose	This task verifies that a 1+1 protection group will switch traffic properly. You must perform this procedure if you have created a 1+1 protection group.
Tools/Equipment	The test set specified by the acceptance test procedure.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60; a test circuit created as part of the topology acceptance test.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 3 Click the **Conditions** tab. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 4 On the network map, double-click the node containing the 1+1 protection group you are testing to open it in node view.

Step 5 Click the **Maintenance > Protection** tabs.

Step 6 Initiate a Force switch on the working port:

a. In the Protection Groups area, click the 1+1 protection group.

b. Click the working port. Next to Switch Commands, click **Force**.

c. In the Confirm Force Operation dialog box, click **Yes**.

d. In the Selected Group area, verify that the following appears:

- Protect port: Protect/Active [FORCE_SWITCH_TO_PROTECT], [PORT STATE]
- Working port: Working/Standby [FORCE_SWITCH_TO_PROTECT], [PORT STATE]

Step 7 Verify that traffic on the test set connected to the node is still running. Some bit errors are normal, but traffic flow should not be interrupted. If a traffic interruption occurs, complete Step 8, then refer to your next level of support. If a traffic interruption does not occur, complete Steps 8 through 12.

Step 8 Clear the switch on the working port:

a. Next to Switch Commands, click **Clear**.

b. In the Confirm Clear Operation dialog box, click **Yes**.

Step 9 Initiate a Force switch on the protect port:

a. In the Selected Group area, click the protect port. Next to Switch Commands, click **Force**.

b. In the Confirm Force Operation dialog box, click **Yes**.

c. In the Selected Group area, verify that the following appears:

- Protect port: Protect/Active [FORCE_SWITCH_TO_WORKING], [PORT STATE]
- Working port: Working/Standby [FORCE_SWITCH_TO_WORKING], [PORT STATE]

Step 10 Verify that the traffic on the test set connected to the node is still running. If a traffic interruption occurs, complete Step 11 and then refer to your next level of support. If a traffic interruption does not occur, complete Steps 11 and 12.

Step 11 Clear the switch on the protect port:

a. Next to Switch Commands, click **Clear**.

b. In the Confirm Clear Operation dialog box, click **Yes**.

c. In the Selected Group area, verify the following states:

- Protect port: Protect/Standby
- Working port: Working/Active

Step 12 Return to your originating procedure (NTP).

DLP-A89 Remap the K3 Byte

Purpose	This task provisions the K3 byte. Do not remap the K3 byte unless specifically required to run an ONS 15454 BLSR through third-party equipment. This task is unnecessary for most users.
Tools/Equipment	OC48 AS cards must be installed on the BLSR span that you remap.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution If you remap the K3 byte, remap to the same extended byte (Z2, E2, or F1) on both sides of the span.

Step 1 In node view, double-click the OC48 AS card that connects to the third-party equipment.

Step 2 Click the **Provisioning > Line** tabs.

Step 3 Click **BLSR Ext Byte** and choose the alternate byte: Z2, E2, or F1.

Step 4 Click **Apply**.

Step 5 (Four-fiber BLSRs only) Repeat Steps 2 through 4 for each protect card.

Step 6 Repeat this task at the node and card on the other end of the BLSR span.

Note The extension byte chosen in Step 3 should match at both ends of the span.

Step 7 Return to your originating procedure (NTP).

DLP-A91 BLSR Switch Test

Purpose	This task verifies that protection switching is working correctly in a BLSR.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click the row of the BLSR you will switch, then click **Edit**.

Step 4 Initiate a Force Ring switch the west port:

a. Right-click any BLSR node west port and choose **Set West Protection Operation**. Figure 19-2 on page 19-11 shows an example. (To move a graphic icon, click it, then press **Ctrl** while you drag and drop it to a new location.)

Note For two fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. Right-click either working or protect port.

b. In the Set West Protection Operation dialog box, choose **FORCE RING** from the drop-down list.

c. Click **OK**.

d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the BLSR channel where you invoked the Force Ring switch. The BLSR span lines turn purple where the switch was invoked, and all span lines between other BLSR nodes turn green.

Step 5 Verify the conditions:

a. Click the **Conditions** tab.

b. Click **Retrieve**.

c. Verify that the following conditions are reported on the node where you invoked the Force Ring switch on the West port:

- FORCED-REQ-RING—A Force Switch Request On Ring condition is reported against the span's working slot on the west side of the node.
- RING-SW-EAST—A Ring Switch Active on the east side condition is reported against the working span on the east side of the node.

Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

d. Verify that the following conditions are reported on the node that is connected to the West line of the node where you performed the switch:

- FE-FRCDWKSWPR-RING—A Far-End Working Facility Forced to Switch to Protection condition is reported against the working span on the east side of the node.
- RING-SW-WEST—A Ring Switch Active on the west side condition is reported against the working span on the west side of the node.

Step 6 (Optional) If you remapped the K3 byte to run an ONS 15454 BLSR through third-party equipment, check the following condition. Verify a FULLPASSTHR-BI condition reported on other nodes that are not connected to the west side of the node where you invoked the Force Ring switch.

Step 7 Verify the BLSR line status on each node:

a. From the View menu choose **Go to Node View**.

b. Click the **Maintenance > BLSR** tabs.

c. Verify the following:

- The line states are shown as Stby/Stby on the west side of the node and Act/Act on the east side of the node where you invoked the Force Ring switch.
- The line states are shown as Stby/Stby on the east side of the node and Act/Act on the west side of the node that is connected to the west line of the node where you invoked the Force Ring switch.
- The line states are shown as Act/Act on both East and west sides of the remaining nodes in the ring.

Step 8 From the View menu, choose **Go to Network View**.

Step 9 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 10 Display the BLSR window where you invoked the Force Ring switch (the window might be hidden by the CTC window).

Step 11 Clear the switch on the west port:

a. Right-click the west port of the BLSR node where you invoked the Force Ring switch and choose **Set West Protection Operation**.

b. In the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down list.

c. Click **OK**.

d. Click **Yes** in the Confirm BLSR Operation dialog box.

On the network view graphic, the Force Ring switch is removed, the F indicating the switch is removed, and the span lines between BLSR nodes will be purple and green. The span lines might take a few moments to change color.

Step 12 From network view, click the **Conditions** tab. Verify that all conditions raised in this procedure are cleared from the network. If unexplained conditions appear, resolve them before continuing.

Step 13 Verify the BLSR line status on each node:

a. From the View menu, choose **Go to Node View**.

a. Click the **Maintenance > BLSR** tabs.

b. Verify that the line states are shown as Act/Stby on both the east and west sides of each node in the ring.

Step 14 Initiate a Force Ring switch on the east port:

a. Right-click the east port of BLSR node and choose **Set East Protection Operation**.

b. In the Set East Protection Operation dialog box, choose **FORCE RING** from the drop-down list.

c. Click **OK**.

d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the working BLSR channel where you invoked the Force Ring switch. The BLSR span lines are purple where the Force Ring switch was invoked, and all span lines between other BLSR nodes are green. The span lines might take a few moments to change color.

Step 15 Verify the conditions:

a. Click the **Conditions** tab.

b. Click **Retrieve**.

c. Verify that the following conditions are reported on the node where you invoked the Force Ring switch on the East port:

- FORCED-REQ-RING—A Force Switch Request On Ring condition is reported against the span's working slot on the east side of the node.
- RING-SW-WEST—A Ring Switch Active on the west side condition is reported against the working span on the east side of the node.

Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

d. Verify that the following conditions are reported on the node that is connected to the East line of the node where you performed the switch:

- FE-FRCDWKSWPR-RING—A Far-End Working Facility Forced to Switch to Protection condition is reported against the working span on the west side of the node.
- RING-SW-EAST—A Ring Switch Active on the east side condition is reported against the working span on the west side of the node.

Step 16 (Optional) If you remapped the K3 byte to run an ONS 15454 BLSR through third-party equipment, verify a FULLPASSTHR-BI condition reported on other nodes that are not connected to the west side of the node where you invoked the Force Ring switch.

Step 17 Verify the BLSR line status on each node:

a. From the View menu, choose **Go to Node View**.

b. Click the **Maintenance > BLSR** tabs.

- Verify the following:
- The line states are shown as Stby/Stby on the east side of the node and Act/Act on the west side of the node where you invoked the Force Ring switch.
- The line states are shown as Stby/Stby on the west side of the node and Act/Act on the east side of the node that is connected to the east line of the node where you invoked the Force Ring switch.
- The line states are shown as Act/Act on both East and West sides of the remaining nodes in the ring.

Step 18 From the View menu, choose **Go to Network View**.

Step 19 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 20 Display the BLSR window where you invoked the Force Ring switch (the window might be hidden by the CTC window).

Step 21 Clear the switch on the east port:

a. Right-click the east port of the BLSR node where you invoked the Force Ring switch and choose **Set East Protection Operation**.

b. In the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down list.

c. Click **OK**.

d. Click **Yes** in the Confirm BLSR Operation dialog box.

On the network view graphic, the Force Ring switch is removed, the F indicating the switch is removed, and the span lines between BLSR nodes will be purple and green. The span lines might take a few moments to change color.

Step 22 From network view, click the **Conditions** tab. Verify that all conditions raised in this procedure are cleared from the network. If unexplained conditions appear, resolve them before continuing.

Step 23 Verify the BLSR line status on each node:

a. From the View menu, choose **Go to Node View**.

b. Click the **Maintenance > BLSR** tabs.

c. Verify that the line states are shown as Act/Stby on both the East and west sides of each node in the ring.

Step 24 From the File menu, choose **Close** to close the BLSR window.

Step 25 Return to your originating procedure (NTP).

DLP-A92 Four-Fiber BLSR Exercise Span Test

Purpose	This task exercises a four-fiber BLSR span. Ring exercise conditions (including the K-byte pass-through) are reported and cleared within 10 to 15 seconds.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click the BLSR you will exercise, then click **Edit**.

Step 4 Exercise the west span:

a. Right-click the west port of the four-fiber BLSR node that you want to exercise and choose **Set West Protection Operation**. (To move a graphic icon, press **Ctrl** while you drag and drop it to a new location.)

Note The squares on the network map represent ports. Right-click a working port.

b. In the Set West Protection Operation dialog box, choose **EXERCISE SPAN** from the drop-down list.

c. Click **OK**. In the Confirm BLSR Operation dialog box, click **Yes**.

On the network view graphic, an E appears on the BLSR channel where you invoked the exercise. The E will appear for 10 to 15 seconds, then disappear.

Step 5 Verify the conditions:

a. Click the **Conditions** tab, then click **Retrieve**.

b. Verify the following conditions:

- EXERCISING-SPAN—An Exercise Ring Successful condition is reported on the node where the span was exercised.
- FE-EX-SPAN—A Far-End Exercise Span Request condition is reported against the east span of the node connected to the west side of the node where you exercised the span.
- KB-PASSTHR—If applicable, a K Byte Pass Though Active condition is reported.

Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

Step 6 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 7 Exercise the east span:

a. Right-click the east port of the four-fiber BLSR node that you want to exercise and choose **Set East Protection Operation**.

b. In the Set East Protection Operation dialog box, choose **EXERCISE SPAN** from the drop-down list.

c. Click **OK**.

d. In the Confirm BLSR Operation dialog box, click **Yes**.

On the network view graphic, an E appears on the BLSR channel where you invoked the exercise. The E will appear for 10 to 15 seconds, then disappear.

Step 8 From the File menu, choose **Close**.

Step 9 Verify the conditions:

a. Click the **Conditions** tab, then click **Retrieve**.

b. Verify the following conditions:

- EXERCISING-SPAN—An Exercise Ring Successful condition is reported on the node where the span was exercised.
- FE-EX-SPAN—A Far-End Exercise Span Request condition is reported against the east span of the node connected to the west side of the node where you exercised the span.
- KB-PASSTHR—If applicable, a K Byte Pass Though Active condition is reported.

Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

Step 10 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 11 From the File menu, choose **Close** to close the BLSR window.

Step 12 Return to your originating procedure (NTP).

DLP-A93 Four-Fiber BLSR Span Switching Test

Purpose	This task verifies that traffic will switch from working to protect fibers on a four-fiber BLSR span.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click **Edit**. A BLSR window appears containing a graphic of the BLSR.

Note If the node icons are stacked on the BLSR graphic, press Ctrl while you drag and drop each one to a new location so you can see the BLSR port information clearly.

Step 4 Switch the west span:

a. Right-click the west port of the four-fiber BLSR node that you want to exercise and choose **Set West Protection Operation**. Figure 19-2 on page 19-11 shows an example.

Note The squares on the network map represent ports. Right-click a working port.

b. In the Set West Protection Operation dialog box, choose **FORCE SPAN** from the drop-down list.

c. Click **OK**.

d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the BLSR channel where you invoked the protection switch. The BLSR span lines turn purple where the Force Span switch was invoked, and all span lines between other BLSR nodes turn green.

Step 5 Verify the conditions:

a. Click the **Conditions** tab.

b. Click **Retrieve**.

c. Verify that a SPAN-SW-WEST (Span Switch West) condition is reported on the node where you invoked the Force Span switch, and a SPAN-SW-EAST (Span Switch East) condition is reported on the node connected to the west line of the node where you performed the switch. Make sure the Filter button in the lower right corner of window is off. Click the Node column to sort conditions by node.

Step 6 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 7 Display the BLSR window where you invoked the Force Span switch (the window might be hidden by the CTC window).

Step 8 Clear the west switch:

a. Right-click the west port of the BLSR node where you invoked the Force Span switch and choose **Set West Protection Operation**.

b. In the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down list.

c. Click **OK**.

d. Click **Yes** in the Confirm BLSR Operation dialog box.

On the network view graphic, the Force Span switch is removed, the F disappears, and the span lines between BLSR nodes will be purple and green. The span lines might take a few moments to change color.

Step 9 Switch the east span:

a. Right-click the east port of BLSR node and choose **Set East Protection Operation**.

b. In the Set East Protection Operation dialog box, choose **FORCE SPAN** from the drop-down list.

c. Click **OK**.

d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the BLSR channel where you invoked the Force Span switch. The BLSR span lines are purple where the Force Span switch was invoked, and all span lines between other BLSR nodes are green. The span lines might take a few moments to change color.

Step 10 Verify the conditions:

a. Click the **Conditions** tab.

b. Click **Retrieve**.

c. Verify that a SPAN-SW-EAST (Span Switch East) condition is reported on the node where you invoked the Force Span switch, and a SPAN-SW-WEST (Span Switch West) condition is reported on the node connected to the west line of the node where you performed the switch. Make sure the Filter button in the lower right corner of window is off.

Step 11 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 12 Display the BLSR window where you invoked the Force Span switch (the window might be hidden by the CTC window).

Step 13 Clear the east switch:

a. Right-click the east port of the BLSR node where you invoked the Force Span switch and choose **Set East Protection Operation**.

b. In the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down list.

c. Click **OK**.

d. Click **Yes** in the Confirm BLSR Operation dialog box.

On the network view graphic, the Force Span switch is removed, the F indicating the switch is removed, and the span lines between BLSR nodes will be purple and green. The span lines might take a few moments to change color.

Step 14 From the File menu, choose **Close** to close the BLSR window.

Step 15 Return to your originating procedure (NTP).

DLP-A94 Path Protection Configuration Protection Switching Test

Purpose	This task verifies that a path protection span is switching correctly.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Although a service interruption under 60 ms might occur, the test circuit should continue to work before, during, and after the switches. If the circuit stops working, do not continue. Contact your next level of support.

Step 1 From the View menu, choose **Go to the Network View**.

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Initiate a Force switch for all circuits on the span:

a. Click the **Perform Path Protection span switching** field.

b. Choose **FORCE SWITCH AWAY** from the drop-down list.

c. Click **Apply**.

d. In the Confirm Path Protection Switch dialog box, click **Yes**.

e. In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the Switch State for all circuits is FORCE. Unprotected circuits will not switch.

Step 4 Clear the Force switch:

a. Click the **Perform Path Protection span switching** field.

b. Choose **CLEAR** from the drop-down list.

c. Click **Apply**.

d. In the Confirm Path Protection Switch dialog box, click **Yes**.

e. In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the Switch State for all path protection circuits is CLEAR.

Step 5 Return to your originating procedure (NTP).

DLP-A95 Provision a DS-1 Circuit Source and Destination

Purpose	This task provisions an electrical circuit source and destination for a DS-1 circuit.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note After you have selected the circuit properties in the Circuit Source dialog box according to the specific circuit creation procedure, you are ready to provision the circuit source.

Step 1 From the Node drop-down list, choose the node where the source will originate.

Step 2 From the Slot drop-down list, choose the slot containing the DS1-14, DS1N-14, DS1/E1-56, DS3XM-6, or DS3XM-12 card where the circuit will originate.

Note A VT circuit source or destination can be on the STS grooming endpoint of a portless aggregation circuit.

Step 3 If you chose DS3XM-6 or DS3XM-12 as the card, choose the port from the Port drop-down list.

Step 4 From the DS-1 drop-down list, choose the source DS-1.

Step 5 If you need to create a secondary source, for example, a path protection bridge/selector circuit entry point in a multivendor path protection configuration, click **Use Secondary Source** and repeat Steps 1 through 4 to define the secondary source. If you do not need to create a secondary source, continue with Step 6.

Step 6 Click **Next**.

Step 7 From the Node drop-down list, choose the destination (termination) node.

Step 8 From the Slot drop-down list, choose the slot containing the destination card. The destination is typically a DS-1 card. You can also choose an OC-N card to map the DS-1 to a VT1.5 for OC-N transport.

Step 9 Depending on the destination card, choose the destination port, STS, VT, or DS1 from the drop-down lists that appear based on the card selected in Step 8. See Table 6-2 on page 6-3 for a list of valid options. CTC does not display ports, STSs, VTs, or DS1s already used by other circuits. If you and another user who is working on the same network choose the same port, STS, VT, port, or DS1 simultaneously, one of you receives a Path in Use error and is unable to complete the circuit. The user with the partial circuit needs to choose new destination parameters.

Step 10 If you need to create a secondary destination, for example, a path protection bridge/selector circuit exit point in a multivendor path protection configuration, click **Use Secondary Destination** and repeat Steps 7 through 9 to define the secondary destination.

Step 11 Click **Next**.

Step 12 Return to your originating procedure (NTP).

DLP-A96 Provision a DS-1 or DS-3 Circuit Route

Purpose	This task provisions the circuit route for manually routed DS-1 or DS-3 circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
	The Circuit Creation wizard Route Review and Edit page must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the Route Review/Edit area of the Circuit Creation wizard, click the source node icon if it is not already selected.

Step 2 Starting with a span on the source node, click the arrow of the span you want the circuit to travel. The arrow turns yellow. In the Selected Span area, the From and To fields provide span information. The source STS and VT (DS-1 circuit only) appear.

Step 3 If you want to change the source STS, adjust the Source STS field; otherwise, continue with Step 4.

Step 4 If you want to change the source VT for DS-1 circuits, adjust the Source VT field; otherwise, continue with Step 5.

Note VT is gray (unavailable) for DS-3 circuits.

Step 5 Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

Step 6 If the Fully Protect Path check box is checked in the Circuit Routing Preferences panel, you must:

- Add two spans for all path protection or unprotected portions of the circuit route from the source to the destination.
- Add one span for all BLSR or 1+1 portions of route from the source to the destination.
- For circuits routed on path protection DRI topologies, provision the working and protect paths as well as spans between the DRI nodes.

Step 7 Repeat Steps 2 through 6 until the circuit is provisioned from the source to the destination node through all intermediary nodes.

Step 8 Return to your originating procedure (NTP).

DLP-A97 Provision an OC-N Circuit Source and Destination

Purpose	This task provisions an OC-N circuit source and destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note After you have selected the circuit properties in the Circuit Source dialog box according to the specific circuit creation procedure, you are ready to provision the circuit source and destination.

Step 1 From the Node drop-down list, choose the node where the circuit will originate.

Step 2 From the Slot drop-down list, choose the slot containing the OC-N card where the circuit originates. (If card capacity is fully utilized, it does not appear in the list.)

Step 3 Depending on the circuit origination card, choose the source port and/or STS from the Port and STS lists. The Port list is only available if the card has multiple ports. STSs do not appear if they are already in use by other circuits.

Note The STSs that appear depend on the card, circuit size, and protection scheme. For example, if you create an STS-3c circuit on an OC-12 card in a path protection configuration, only four STSs are available. If you create an STS-3c circuit on an OC-12 card in a BLSR, two STSs are available because of the BLSR protection characteristics.

Step 4 If you need to create a secondary source, for example, a path protection bridge/selector circuit entry point in a multivendor path protection configuration, click **Use Secondary Source** and repeat Steps 1 through 3 to define the secondary source.

Step 5 Click **Next**.

Step 6 From the Node drop-down list, choose the destination node.

Step 7 From the Slot drop-down list, choose the slot containing the OC-N card where the circuit will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the list.)

Step 8 Depending on the card selected in Step 2, choose the destination port and/or STS from the Port and STS drop-down lists. The Port drop-down list is available only if the card has multiple ports. The STSs that appear depend on the card, circuit size, and protection scheme.

Step 9 If you need to create a secondary destination, for example, a path protection bridge/selector circuit entry point in a multivendor path protection configuration, click **Use Secondary Destination** and repeat Steps 6 through 8 to define the secondary destination.

Step 10 Click **Next**.

Step 11 Return to your originating procedure (NTP).

DLP-A99 Determine Available VLANs

Purpose	This task verifies that the network has the capacity to support the additional new VLANs required for the creation E-Series circuits. It does not apply to E-Series cards in port-mapped mode.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed at each end of the Ethernet circuit.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In any CTC view, click the **Circuits** tab.

Step 2 Click any existing Ethernet circuit.

Step 3 Click **Edit**, then click the **VLANs** tab.

The Edit Circuit dialog box shows the number of VLANs used by circuits and the total number of VLANs available for use.

Step 4 Determine that the number of available VLANs listed is sufficient for the number of E-Series Ethernet circuits that you will create.

Caution Multiple E-Series Ethernet circuits with spanning tree enabled block each other if the circuits traverse the same E-Series Ethernet card and use the same VLAN.

Step 5 Return to the originating procedure (NTP).

CHAPTER 18

DLPs A100 to A199

Note The terms “Unidirectional Path Switched Ring” and “UPSR” may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as “Path Protected Mesh Network” and “PPMN,” refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

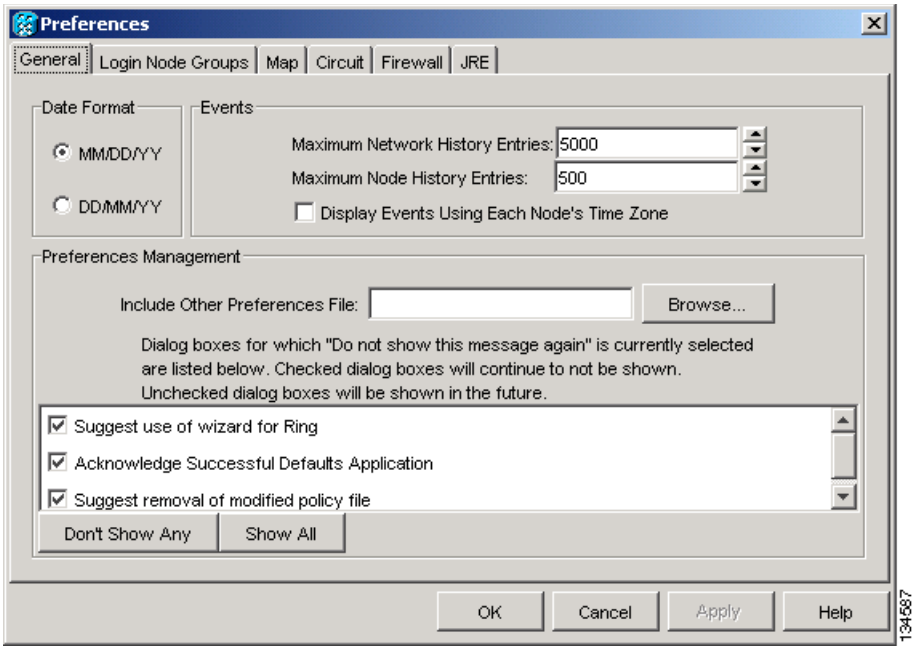
DLP-A111 Changing the Maximum Number of Session Entries for Alarm History

Purpose	This task changes the maximum number of session entries included in the alarm history. Use this task to extend the history list in order to save information for future reference or troubleshooting.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu, choose **Preferences**.

The Cisco Transport Controller (CTC) Preferences dialog box appears (Figure 18-1).

Figure 18-1 CTC Preferences Dialog Box



Step 2 Click the up or down arrow buttons next to the Maximum History Entries field to change the entry.

Step 3 Click **Apply** and **OK**.

Note Setting the Maximum History Entries value to the high end of the range uses more Cisco Transport Controller (CTC) memory and could impair CTC performance.

Note This task changes the maximum history entries recorded for CTC sessions. It does not affect the maximum number of history entries viewable for a network, node, or card.

Step 4 Return to your originating procedure (NTP).

DLP-A112 Display Alarms and Conditions Using Time Zone

Purpose	This task changes the time stamp for events to the time zone of the ONS node reporting the alarm. By default, the events time stamp is set to the time zone for the CTC workstation.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu, choose **Preferences**.

The CTC Preferences dialog box appears (Figure 18-1 on page 18-2).

Step 2 Check the **Display Events Using Each Node's Time Zone** check box. The Apply button is enabled.

Step 3 Click **Apply** and **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-A113 Synchronize Alarms

Purpose	This task is used to view ONS 15454 events at the card, node, or network level and to refresh the alarm listing so that you can check for new and cleared alarms and conditions.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 At the card, node, or network view, click the **Alarms** tab.

Step 2 Click **Synchronize**.

This button causes CTC to retrieve a current alarm summary for the card, node, or network. This step is optional because CTC updates the Alarms window automatically as raise/clear messages arrive from the node.

Note Alarms that have been raised during the session will have a check mark in the Alarms window New column. When you click Synchronize, the check mark disappears.

Step 3 Return to your originating procedure (NTP).

DLP-A114 View Conditions

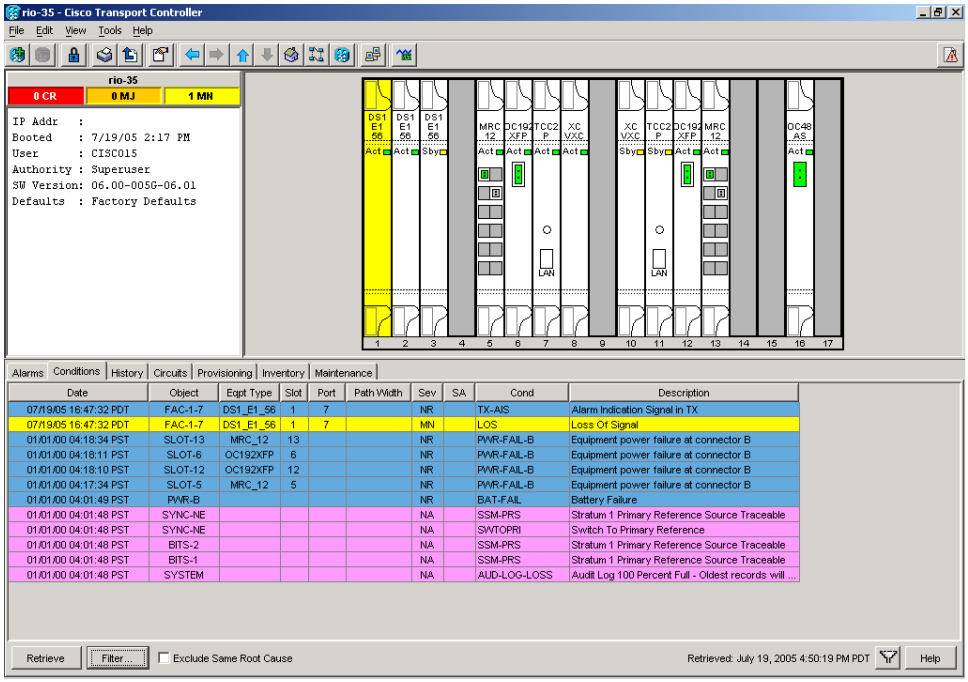
Purpose	This task is used to view conditions (events with a Not Reported [NR] severity) at the card, node, or network level. Conditions give you a clear record of changes or events that do not result in alarms.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From the card, node, or network view, click the **Conditions** tab.

Step 2 Click **Retrieve** (Figure 18-2).

The Retrieve button requests the current set of fault conditions from the node, card, or network. The window is not updated when events change on the node. You must click Retrieve to see any changes.

Figure 18-2 Node View Conditions Window



Conditions include all fault conditions raised on the node, whether or not they are reported.

Note Alarms can be unreported when they are filtered out of the display. See the "DLP-A225 Enable Alarm Filtering" task on page 19-17 for information.

Events that are reported as Major (MJ), Minor (MN), or Critical (CR) severities are alarms. Events that are reported as Not-Alarmed (NA) are conditions. Conditions that are not reported at all are marked Not-Reported (NR) in the Conditions window severity column.

Conditions that have a default severity of Critical (CR), Major (MJ), Minor (MN), or Not-Alarmed (NA) but are not reported due to exclusion or suppression are shown as NR in the Conditions window.

Note For more information about alarm suppression, see the "DLP-A522 Suppress Alarm Reporting" task on page 22-20.

Current conditions are shown with the severity chosen in the alarm profile, if used. For more information about alarm profiles, see the "NTP-A71 Create, Download, and Assign Alarm Severity Profiles" procedure on page 8-6.

Note When a port is placed in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state, it raises an Alarms Suppressed for Maintenance (AS-MT) condition. For information about alarm and condition troubleshooting, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 3 If you want to apply exclusion rules, check the **Exclude Same Root Cause** check box at the node or network view, but do not check the Exclude Same Root Cause check box in card view.

An exclusion rule eliminates all lower-level alarms or conditions that originate from the same cause. For example, a fiber break may cause an LOS alarm, an AIS condition, and an SF condition. If you check the Exclude Same Root Cause check box, only the LOS alarm will appear. According to Telcordia, exclusion rules apply to a query of "all conditions from a node."

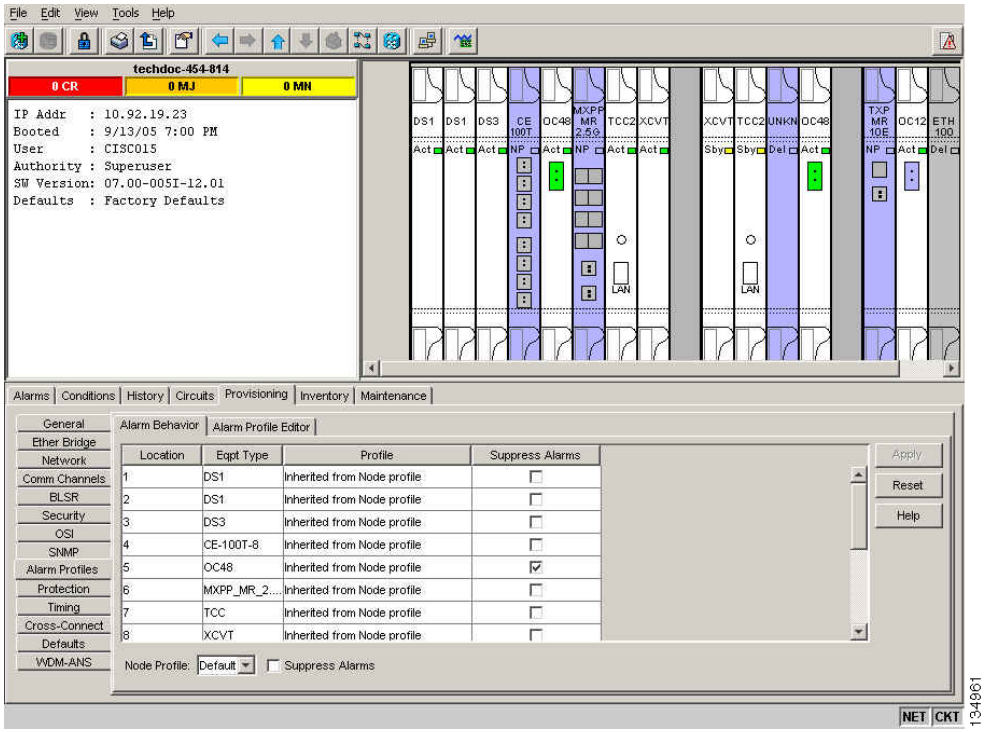
Step 4 Return to your originating procedure (NTP).

DLP-A117 Apply Alarm Profiles to Cards and Nodes

Purpose	This task applies a custom or default alarm profile to cards or nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A518 Create a New or Cloned Alarm Severity Profile, page 22-11 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs (Figure 18-3).

Figure 18-3 Node View Alarm Behavior Window



Step 2 To apply profiles to a card:

- **a.** Click a selection from the Profile column for the card.
- **b.** Choose the new profile from the drop-down list.
- **c.** Click **Apply**.

Step 3 To apply the profile to an entire node:

- **a.** Click the **Node Profile** drop-down arrow at the bottom of the window (Figure 18-3).
- **b.** Choose the new alarm profile from the drop-down list.
- **c.** Click **Apply**.

Step 4 To reapply a previous alarm profile after you have applied a new one, select the previous profile and click **Apply** again.

Step 5 Return to your originating procedure (NTP).

DLP-A121 Enable/Disable Pointer Justification Count Performance Monitoring

Purpose	This task enables or disables pointer justification counts, which provide a way to align the phase variations in synchronous transport signal (STS) payloads and to monitor the clock synchronization between nodes. A consistently large pointer justification count indicates clock synchronization problems between nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Enable Intermediate Path Performance Monitoring as specified in DLP-A122 Enable/Disable Intermediate Path Performance Monitoring, page 18-9

Step 2 In node view, double-click the card you want to monitor. The card view appears.

See Table 18-1 for a list of line terminating equipment (LTE) cards.

Table 18-1 OC-N Cards that Terminate the Line, Called LTEs

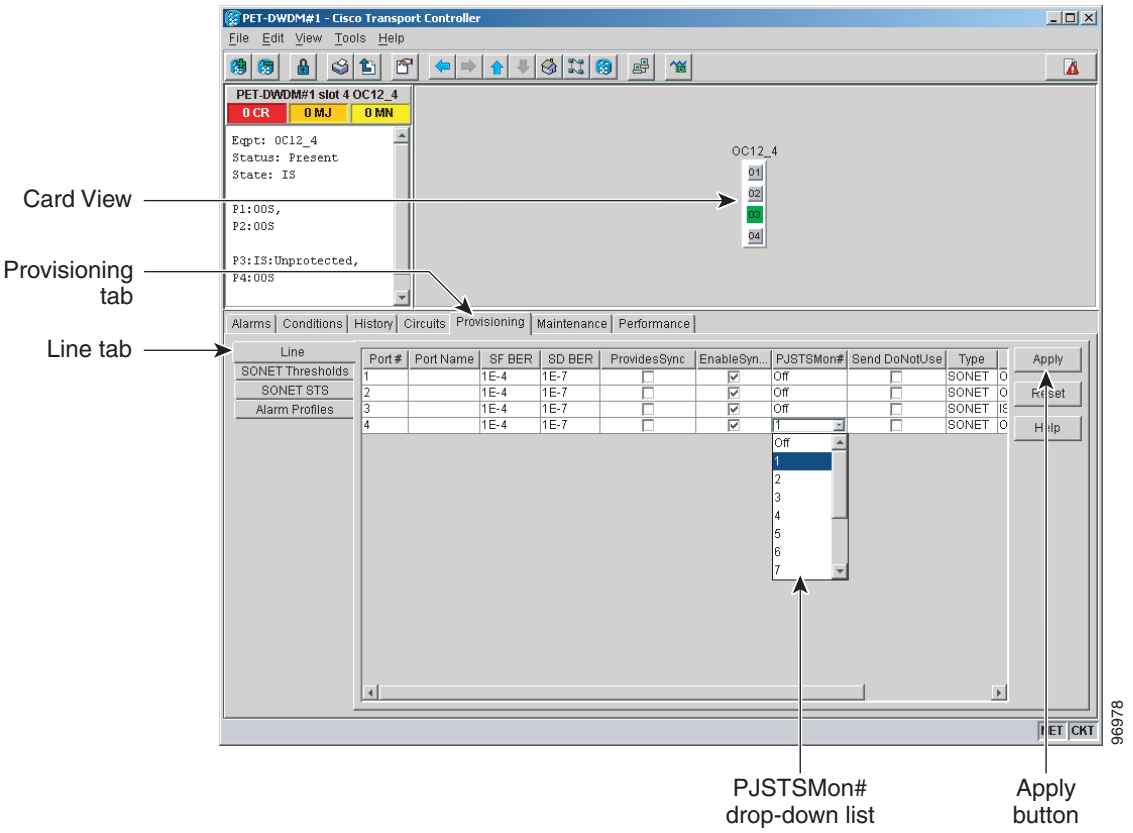
Line Terminating Equipment
EC1-12
OC3 IR 4/STM1 SH 1310
OC3 IR4/STM1 SH 1310-8
OC12 LR/STM4 LH 1310
OC12 IR/STM4 SH 1310
OC12 IR/STM4 SH 1310-4
OC12 LR/STM4 LH 1550
OC48 LR 1550
OC48 IR 1310
OC48 LR/STM16 LH AS 1550
OC48 IR/STM16 SH AS 1310
OC48 ELR 200 GHz
OC48 ELR/STM16 EH 100 GHz
OC192 SR/STM64 IO 1310
OC192 IR/STM64 SH 1550
OC192 LR/STM64 LH 1550
OC192 ELR/STM64 LH ITU 15xx.xx

Step 3 Click the **Provisioning > Line** tabs.

Step 4 From the PJSTSMon# drop-down list, make a selection based on the following rules (Figure 18-4):

- Off means pointer justification monitoring is disabled (default).
- 1 to *n* are the number of STSs on the port. One STS per port can be enabled from the PJSTSMon# card drop-down list.

Figure 18-4 Enabling or Disabling Pointer Justification Count Parameters



Step 5 In the Service State field, confirm that the port is in the In-Service and Normal (IS-NR) service state.

Step 6 If the port is IS-NR, click **Apply**. If the port is in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD), Out-of-Service and Management, Maintenance (OOS-MA,MT), or the Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS) service state, choose **IS** from the Admin State drop-down list and click **Apply**.

Step 7 Click the **Performance** tab to view PM parameters. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Note The count fields for PPJC and NPJC PM parameters appear white and blank unless pointer justification count performance monitoring is enabled.

Step 8 Return to your originating procedure (NTP).

DLP-A122 Enable/Disable Intermediate Path Performance Monitoring

Purpose	This task enables or disables intermediate path performance monitoring, which allows you to monitor large amounts of STS traffic through intermediate nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The monitored IPPM parameters are STS CV-P, STS ES-P, STS SES-P, STS UAS-P, and STS FC-P. Far-end path monitoring can be performed on the OC3-4 and EC-1 cards. For PM parameter definitions, refer to the "Performance Monitoring" chapter of the *Cisco ONS 15454 Reference Manual*.

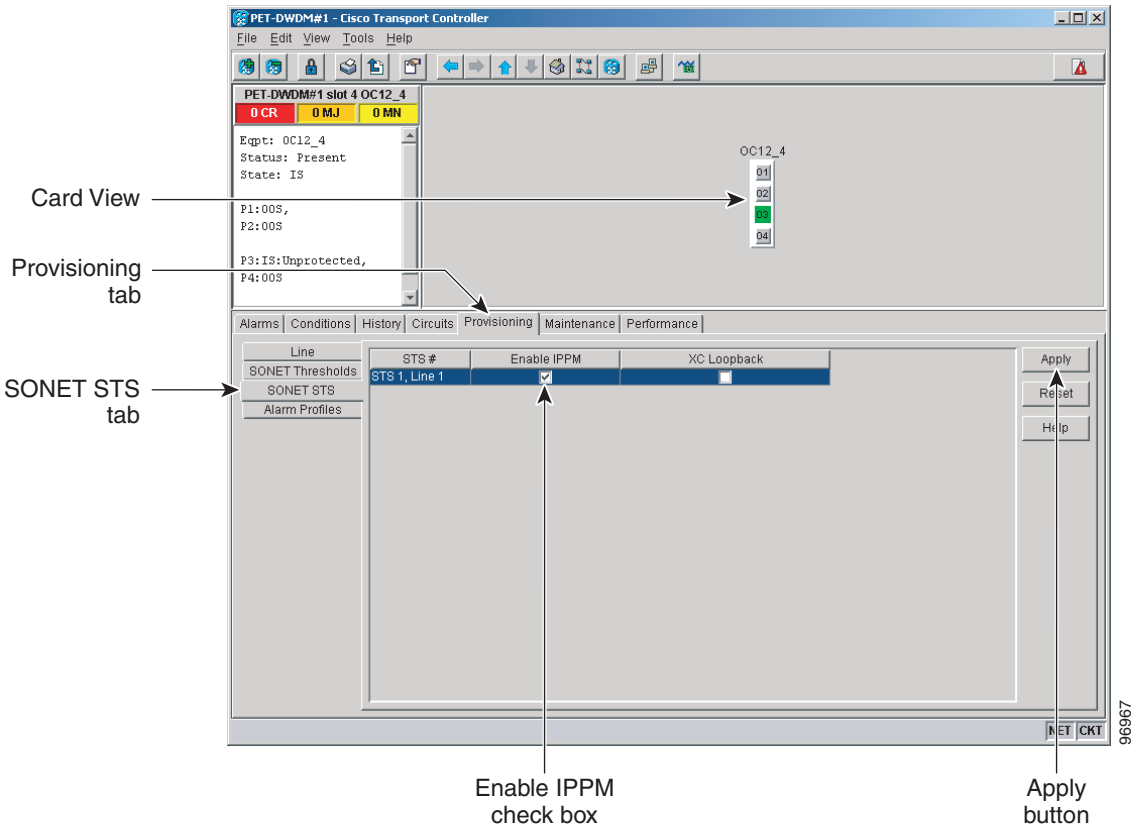
Note An OC-48 IR card used in a BLSR does not support IPPM during a protection switch.

Step 1 In node view, double-click the OC-N card you want to monitor. The card view appears.

See Table 18-1 on page 18-7 for a list of OC-N LTE cards.

Step 2 Click the **Provisioning > SONET STS** tabs (Figure 18-5).

Figure 18-5 SONET STS Tab for Enabling or Disabling IPPM



Step 3 Click the check box in the Enable IPPM column and make a selection based on the following rules:

- Unchecked means IPPM is disabled for that STS (default)
- Checked means IPPM is enabled for that STS

Step 4 Click **Apply**.

Step 5 Click the **Performance** tab to view PM parameters. For IPPM parameter definitions, refer to the "Performance Monitoring" chapter of the *Cisco ONS 15454 Reference Manual*.

Step 6 Return to your originating procedure (NTP).

DLP-A124 Refresh PM Counts at 15-Minute Intervals

Purpose	This task changes the window view to display PM counts in 15-minute intervals.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **15 min** radio button.

Step 4 Click **Refresh**. Performance monitoring parameters appear in 15-minute intervals synchronized with the time of day.

Step 5 View the Curr column to find PM counts for the current 15-minute interval.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 15-minute interval, a threshold crossing alert (TCA) is raised. The number represents the counter value for each specific performance monitoring parameter.

Step 6 View the Prev-*n* columns to find PM counts for the previous 15-minute intervals.

Note If a complete 15-minute interval count is not possible, the value appears with a yellow background. An incomplete or incorrect count can be caused by monitoring for less than 15 minutes after the counter started, changing node timing settings, changing the time zone settings, replacing a card, resetting a card, or changing port service states. When the problem is corrected, the subsequent 15-minute interval appears with a white background.

Step 7 Return to your originating procedure (NTP).

DLP-A125 Refresh PM Counts at One-Day Intervals

Purpose	This task changes the window view to display PM parameters in 1-day intervals.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **1 day** radio button.

Step 4 Click **Refresh**. Performance monitoring appears in 1-day intervals synchronized with the time of day.

Step 5 View the Curr column to find PM counts for the current 1-day interval.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 1-day interval, a threshold crossing alert (TCA) is raised. The number represents the counter value for each specific performance monitoring parameter.

Step 6 View the Prev-*n* columns to find PM counts for the previous 1-day intervals.

Note If a complete count over a 1-day interval is not possible, the value appears with a yellow background. An incomplete or incorrect count can be caused by monitoring for less than 24 hours after the counter started, changing node timing settings, changing the time zone settings, replacing a card, resetting a card, or changing port service states. When the problem is corrected, the subsequent 1-day interval appears with a white background.

Step 7 Return to your originating procedure (NTP).

DLP-A126 View Near-End PM Counts

Purpose	This task enables you to view near-end PM counts for the selected card and port.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Near End** radio button.

Step 4 Click **Refresh**. All PM parameters occurring for the selected card on the incoming signal appear. For PM parameter definitions refer to the "Performance Monitoring" chapter of the *Cisco ONS 15454 Reference Manual*.

Step 5 View the Curr column to find PM counts for the current time interval.

Step 6 View the Prev-*n* columns to find PM counts for the previous time intervals.

Step 7 Return to your originating procedure (NTP).

DLP-A127 View Far-End PM Counts

Purpose	This task enables you to view far-end PM parameters for the selected card and port.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Far End** radio button.

Step 4 Click **Refresh**. All PM parameters recorded by the far-end node for the selected card on the outgoing signal appear. For PM parameter definitions refer to the "Performance Monitoring" chapter of the *Cisco ONS 15454 Reference Manual*.

Step 5 View the Curr column to find PM counts for the current time interval.

Step 6 View the Prev-*n* columns to find PM counts for the previous time intervals.

Step 7 Return to your originating procedure (NTP).

DLP-A129 Reset Current PM Counts

Purpose	This task clears the current PM count, but it does not clear the cumulative PM count. This task allows you to see how quickly PM counts rise.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click **Baseline**.

Note The Baseline button clears the PM counts displayed in the current time interval but does not clear the PM counts on the card. When the current time interval expires or the window view changes, the total number of PM counts on the card and on the window appear in the appropriate column. The baseline values are discarded if you change views to a different window and then return to the Performance window.

Step 4 View the current statistics columns to observe changes to PM counts for the current time interval.

Step 5 Return to your originating procedure (NTP).

DLP-A131 Search for Circuits

Purpose	This task searches for ONS 15454 circuits at the network, node, or card level.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate CTC view:

- To search the entire network, click **View > Go to Network View**.
- To search for circuits that originate, terminate, or pass through a specific node, click **View > Go to Other Node**, then choose the node you want to search and click **OK**.
- To search for circuits that originate, terminate, or pass through a specific card, double-click the card on the shelf graphic in node view to open the card in card view.

Step 2 Click the **Circuits** tab.

Step 3 If you are in node or card view, choose the scope for the search, **Node** or **Network (All)**, from the Scope drop-down list located at the bottom right-hand side of the screen.

Step 4 Click **Search**.

Step 5 In the Circuit Name Search dialog box, complete the following:

- Find What—Enter the text of the circuit name you want to find.
- Match whole word only—Check this check box to instruct CTC to select circuits only if the entire word matches the text in the Find What field.
- Match case—Check this check box to instruct CTC to select circuits only when the capitalization matches the capitalization entered in the Find What field.
- Direction—Choose the direction for the search. Searches are conducted up or down from the currently selected circuit.

Step 6 Click **Find Next**. If a match is found, click **Find Next** again to find the next circuit.

Step 7 Repeat Steps 5 and 6 until you are finished, then click **Cancel**.

Step 8 Return to your originating procedure (NTP).

DLP-A137 Provision Path Trace on OC-N Ports

Purpose	This task monitors a path trace on OC-N ports within the circuit path.
Tools/Equipment	The OC-N ports you want to monitor must be on OC-N cards capable of receiving path trace. See Table 19-3 on page 19-46.
Prerequisite Procedures	DLP-A264 Provision a J1 Path Trace on Circuit Source and Destination Ports, page 19-45 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Other Node**. In the Select Node dialog box, choose the node where path trace was provisioned on the circuit source and destination ports.

Step 2 Click **Circuits**.

Step 3 Choose the STS circuit that has path trace provisioned on the source and destination ports, then click **Edit**.

Step 4 In the Edit Circuit window, click the **Show Detailed Map** check box at the bottom of the window. A detailed circuit graphic showing source and destination ports appears.

Step 5 In the detailed circuit map, right-click the circuit OC-N port (the square on the left or right of the source node icon) and choose **Edit Path Trace** from the shortcut menu.

Note The OC-N port must be on a receive-only card listed in Table 19-3 on page 19-46. If not, the Edit Path Trace menu item will not appear.

Step 6 In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down list:

- Auto—Uses the first string received from the port at the other path trace end as the current expected string. An alarm is raised when a string that differs from the baseline is received. For OC-N ports, Auto is recommended because Manual mode requires you to trace the circuit in the Edit Circuit window to determine whether the port is the source or destination path.
- Manual—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.

Step 7 If you set the Path Trace Mode field to Manual, enter the string that the OC-N port should receive in the New Expected String field. To do this, trace the circuit path on the detailed circuit map to determine whether the port is in the circuit source or destination path, then set the New Expected String to the string transmitted by the circuit source or destination. If you set the Path Trace Mode field to Auto, skip this step.

Step 8 Click **Apply**, then click **Close**.

Step 9 Return to your originating procedure (NTP).

DLP-A140 Change the Node Name, Date, Time, and Contact Information

Purpose	This procedure changes basic information such as node name, date, time, and contact information.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Changing the date, time, or time zone might invalidate the node's performance monitoring counters.

Step 1 In node view, click the **Provisioning > General** tabs.

Step 2 Change any of the following:

- General: Node Name
- General: Contact
- Location: Latitude
- Location: Longitude
- Location: Description

Note To see changes to longitude or latitude on the network map, you must go to network view and right-click the specified node, then click **Reset Node Position**.

- Time: Use NTP/SNTP Server
- Time: Date (M/D/Y)
- Time: Time (H:M:S)
- Time: Time Zone
- Time: Use Daylight Savings Time
- AIS-V Insertion On STS-1 Signal Degrade - Path: Insert AIS-V on STS-1 SD-P
- AIS-V Insertion On STS-1 Signal Degrade - Path: SD-P BER

See the "NTP-A25 Set Up Name, Date, Time, and Contact Information" procedure on page 4-5 for detailed field descriptions.

Step 3 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 4 Return to your originating procedure (NTP).

DLP-A142 Modify a Static Route

Purpose	This task modifies a static route on an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 DLP-A65 Create a Static Route, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** tabs.

Step 2 Click the **Static Routing** tab.

Step 3 Click the static route you want to edit.

Step 4 Click **Edit**.

Step 5 In the Edit Selected Static Route dialog box, enter the following:

- Mask
- Next Hop
- Cost

See the "DLP-A65 Create a Static Route" task on page 17-67 for detailed field descriptions.

Step 6 Click **OK**.

Step 7 Return to your originating procedure (NTP).

DLP-A143 Delete a Static Route

Purpose	This task deletes an existing static route on an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 DLP-A65 Create a Static Route, page 17-67
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** > **Static Routing** tabs.

Step 2 Click the static route you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-A144 Disable OSPF

Purpose	This task disables the Open Shortest Path First (OSPF) routing protocol process for an ONS 15454 LAN.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 DLP-A250 Set Up or Change Open Shortest Path First Protocol, page 19-35
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Network > OSPF** tabs. The OSPF subtab has several options.

Step 2 In the OSPF on LAN area, uncheck the **OSPF active on LAN?** check box.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-A145 Change the Network View Background Color

Purpose	This task changes the network view background color or the domain view background color (the area displayed when you open a domain).
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note If you modify background colors, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 If you want to change a domain background, double-click the domain. If not, continue with Step 3.

Step 3 Right-click the network view or domain map area and choose **Set Background Color** from the shortcut menu.

Step 4 In the Choose Color dialog box, select a background color.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-A148 Create Domain Icons

Purpose	This task creates a domain, which is an icon that groups ONS 15454 icons in CTC network view. By default, domains are visible to all CTC sessions that log into the network.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note Domains created by one user are visible to all users who log into the network.

Note To allow users of any security level to create local domains, that is, domains that are visible on the home CTC session only, superusers can change the CTC.network.LocalDomainCreationAndViewing NE default value to TRUE. A TRUE value means any user can maintain the domain information in his or her Preferences file, meaning domain changes will not affect other CTC sessions. (The default value is FALSE, meaning domain information affects all CTC sessions and only superusers can create a domain or put a node into a domain.) See the "NTP-A336 Edit Network Element Defaults" procedure on page 15-36 to change NE default values.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Right-click the network map and choose **Create New Domain** from the shortcut menu.

Step 3 When the domain icon appears on the map, click the map name and type the domain name.

Step 4 Press **Enter**.

Step 5 Return to your originating procedure (NTP).

DLP-A149 Manage Domain Icons

Purpose	This task manages CTC network view domain icons.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60 DLP-A148 Create Domain Icons, page 18-19
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note All domain changes, such as added or removed nodes, are visible to all users who log into the network.

Note To allow users of any security level to create local domains, that is, domains that are visible on the home CTC session only, superusers can change the CTC.network.LocalDomainCreationAndViewing NE default value to TRUE. A TRUE value means any user can maintain the domain information in his or her Preferences file, meaning domain changes will not affect other CTC sessions. (The default value is FALSE, meaning domain information affects all CTC sessions and only superusers can create a domain or put a node into a domain.) See the "NTP-A336 Edit Network Element Defaults" procedure on page 15-36 to change NE default values.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Locate the domain action you want in Table 18-2 and complete the appropriate steps.

Table 18-2 Managing Domains

Domain action	Steps
Move a domain	Press Ctrl and drag and drop the domain icon to the new location.
Rename a domain	Right-click the domain icon and choose **Rename Domain** from the shortcut menu. Type the new name in the domain name field.
Add a node to a domain	Drag and drop the node icon to the domain icon.
Move a node from a domain to the network map	Open the domain and right-click a node. Choose **Move Node Back to Parent View**.
Open a domain	• Double-click the domain icon. • Right-click the domain and choose **Open Domain**.
Return to network view	Right-click the domain view area and choose **Go to Parent View** from the shortcut menu.
Preview domain contents	Right-click the domain icon and choose **Show Domain Overview**. The domain icon shows a small preview of the nodes in the domain. To turn off the domain overview, right-click the overview and select **Show Domain Overview**.
Remove domain	Right-click the domain icon and choose **Remove Domain**. Any nodes in the domain are returned to the network map.

Step 3 Return to your originating procedure (NTP).

DLP-A150 Modify a 1:1 Protection Group

Purpose	This task modifies a 1:1 protection group for electrical cards (DS-1, DS-3, EC-1, and DS3XM).
Tools/Equipment	None
Prerequisite Procedures	DLP-A71 Create a 1:1 Protection Group, page 17-73 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Protection** tabs.

Step 2 In the Protection Groups area, click the 1:1 protection group you want to modify.

Step 3 In the Selected Group area, you can modify the following, as needed:

- Name—As needed, type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Revertive—Check this box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion Time drop-down list. Uncheck if you do not want traffic to revert.
- Reversion time—If the Revertive check box is selected, choose the reversion time from the Reversion time drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

Step 4 Click **Apply**.

Note To convert electrical protection groups, see the "NTP-A91 Upgrade DS-1 and DS-3 Protect Cards from 1:1 Protection to 1:N Protection" procedure on page 10-4.

Step 5 Return to your originating procedure (NTP).

DLP-A152 Modify a 1:N Protection Group

Purpose	This task modifies a 1:N protection group for DS-1 and DS-3 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A72 Create a 1:N Protection Group, page 17-75 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that the DS-1 or DS-3 cards are installed according to the 1:N specifications in the "DLP-A72 Create a 1:N Protection Group" task on page 17-75.

Step 2 In node view, click the **Provisioning** > **Protection** tabs.

Step 3 In the Protection Groups area, click the 1:N protection group you want to modify.

Step 4 In the Selected Group area, change any of the following, as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Available Entities—If cards are available, they will appear here. Use the arrow buttons to move them into the Working Cards column.
- Working Entities—Use the arrow buttons to move cards out of the Working Cards column.
- Reversion Time—Choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

See the "DLP-A72 Create a 1:N Protection Group" task on page 17-75 for field descriptions.

Step 5 Click **Apply**.

Note To convert electrical protection groups, see the "NTP-A91 Upgrade DS-1 and DS-3 Protect Cards from 1:1 Protection to 1:N Protection" procedure on page 10-4.

Step 6 Return to your originating procedure (NTP).

DLP-A154 Modify a 1+1 Protection Group

Purpose	This task modifies a 1+1 protection group for any optical port (OC-3, OC-12, OC-12 IR, OC-48, OC-48AS, and OC-192).
Tools/Equipment	None
Prerequisite Procedures	DLP-A73 Create a 1+1 Protection Group, page 17-76 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Protection** tabs.

Step 2 In the Protection Groups area, click the 1+1 protection group you want to modify.

Step 3 In the Selected Group area, you can modify the following, as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Bidirectional switching—Check or uncheck.
- Revertive—Check this box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion Time drop-down list. Uncheck if you do not want traffic to revert.
- Reversion time—If the Revertive check box is selected, choose the reversion time from the Reversion time drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

See the "DLP-A73 Create a 1+1 Protection Group" task on page 17-76 for field descriptions.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A155 Delete a Protection Group

Purpose	This task deletes a 1:1, 1:N, 1+1, or Y-cable protection group.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Protection** tabs.

Step 2 In the Protection Groups area, click the protection group you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Yes** in the Delete Protection Group dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-A156 Delete a Section DCC Termination

Purpose	This task deletes a SONET Section DCC termination on the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **Provisioning > Comm Channel > SDCC** tabs.

Step 2 Click the SDCC termination to be deleted and click **Delete**. The Delete SDCC Termination dialog box appears.

Step 3 Click **Yes** in the confirmation dialog box.

Step 4 Return to your originating procedure (NTP).

DLP-A157 Change the Node Timing Source

Purpose	This task changes the SONET timing source for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution The following procedure might be service affecting and should be performed during a scheduled maintenance window.

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 In the General Timing section, change any of the following information:

- Timing Mode

Note Because mixed timing can cause timing loops, Cisco does not recommend using the Mixed Timing option. Use this mode with care.

- SSM Message Set
- Quality of RES
- Revertive
- Revertive Time

See the "DLP-A69 Set Up SONET External or Line Timing" task on page 17-69 for field descriptions.

Step 3 In the BITS Facilities section, you can change the following information:

Note The BITS Facilities section sets the parameters for your BITS1 and BITS2 timing references. Many of these settings are determined by the timing source manufacturer. If equipment is timed through BITS Out, you can set timing parameters to meet the requirements of the equipment.

- BITS In State
- BITS Out State
- State
- Coding
- Framing
- Sync Messaging
- AIS Threshold
- LBO

Step 4 In the Reference Lists area, you can change the following information:

Note Reference lists define up to three timing references for the node and up to six BITS Out references. BITS Out references define the timing references used by equipment that can be attached to the node's BITS Out pins on the backplane. If you attach equipment to BITS Out pins, you normally attach it to a node with Line mode because equipment near the external timing reference can be directly wired to the reference.

- NE Reference
- BITS 1 Out
- BITS 2 Out

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

DLP-A158 Change User Password and Security Level on a Single Node

Purpose	This task changes settings for an existing user at one node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning > Security > Users** tabs.

Step 2 Click the user whose settings you want to modify, then click **Change**.

Step 3 In the Change User dialog box, you can:

- Change a user password
- Modify the user security level
- Lock out the user

See the "NTP-A30 Create Users and Assign Security" procedure on page 4-4 for field descriptions.

Step 4 Click **OK**.

Note User settings that you changed during this task will not appear until that user logs off and logs back in.

Step 5 Return to your originating procedure (NTP).

DLP-A159 Delete a User from a Single Node

Purpose	This task deletes an existing user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note You cannot delete a user who is currently logged in. To log out a user, you can complete the "DLP-A315 Log Out a User on a Single Node" task on page 20-9, or you can choose the "Logout before delete" option in the Delete User dialog box.

Note CTC will allow you to delete other Superusers if one Superuser remains. For example, you can delete the CISCO15 user if you have created another Superuser. Use this option with caution.

Step 1 In node view, click the **Provisioning > Security > Users** tabs.

Step 2 Choose the user you want to delete.

Step 3 Click **Delete**.

Step 4 In the Delete User dialog box, verify that the user name displayed is the one you want to delete.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-A160 Change User Password and Security Level on Multiple Nodes

Purpose	This task changes settings for an existing user at multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note You must add the same user name and password to each node the user will access.

Step 1 From the View menu, choose **Go to Network View**. Verify that you can access all the nodes where you want to add users.

Step 2 Click the **Provisioning > Security > Users** tabs. Highlight the user's name whose settings you want to change.

Step 3 Click **Change**. The Change User dialog box appears.

Step 4 In the Change User dialog box, you can:

- Change a user's password
- Modify the user's security level
- Lock out the user

See the "DLP-A75 Create a New User on Multiple Nodes" task on page 17-78 for field descriptions.

Step 5 In the Select Applicable Nodes area, uncheck any nodes where you do not want to change the user's settings (all network nodes are selected by default).

Step 6 Click **OK**. A Change Results confirmation dialog box appears.

Step 7 Click **OK** to acknowledge the changes.

Step 8 Return to your originating procedure (NTP).

DLP-A161 Delete a User from Multiple Nodes

Purpose	This task deletes an existing user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note You cannot delete a user who is currently logged in. To log out a user, you can complete the "DLP-A316 Log Out a User on Multiple Nodes" task on page 20-9, or you can choose the "Logout before delete" option in the Delete User dialog box.

Note CTC will allow you to delete other Superusers if one Superuser remains. For example, you can delete the CISCO15 user if you have created another Superuser. Use this option with caution.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > Security** tabs. Highlight the name of the user you want to delete.

Step 3 Click **Delete**. The Delete User dialog box appears.

Step 4 In the Select Applicable Nodes area, uncheck any nodes where you do not want to delete this user.

Step 5 Click **OK**. A User Deletion Results confirmation dialog box appears.

Step 6 Click **OK** to acknowledge the changes.

Step 7 Return to your originating procedure (NTP).

DLP-A163 Delete SNMP Trap Destinations

Purpose	This task deletes Simple Network Management Protocol (SNMP) trap destinations on an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP** tabs.

Step 2 In the Trap Destinations area, click the trap you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-A165 Change Line and Threshold Settings for a DS1-14 or DS1N-14 Card

Purpose	This task changes the line and threshold settings for a DS1-14 or DS1N-14 card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 In node view, double-click the DS1-14 or DS1N-14 card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line, Line Thresholds, Elect Path Thresholds, or SONET Thresholds** tab.

Note See Chapter 8, "Manage Alarms" for information about the Alarm Profiles tab.

Note If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 4 Modify the settings found under these subtabs by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

For definitions of the line settings, see Table 18-3 on page 18-30. For definitions of the line threshold settings, see Table 18-4 on page 18-31. For definitions of the electrical path threshold settings, see Table 18-5 on page 18-32. For definitions of the SONET threshold settings, see Table 18-6 on page 18-32.

Table 18-3 describes the values on the Provisioning > Line tabs.

Table 18-3 Line Options for DS1-14 and DS1N-14 Cards

Parameter	Description	Options
Port #	(Display only) Port number.	1 to 14
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 20-8.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Line Type	Defines the line framing type.	• D4 • ESF - Extended Super Frame • Unframed
Line Coding	Defines the DS-1 transmission coding type.	• AMI - Alternate Mark Inversion (default) • B8ZS - Bipolar 8 Zero Substitution
Line Length	Defines the distance (in feet) from the backplane connection to the next termination point.	• 0 - 131 • 132 - 262 • 263 - 393 • 394 - 524 • 525 - 655
Admin State	Sets the port administrative service state unless network conditions prevent the change.	• IS—Puts the port in-service. The port service state changes to IS-NR. • IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. • OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. • OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT. **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.

Table 18-3 Line Options for DS1-14 and DS1N-14 Cards (continued)

Parameter	Description	Options
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—(In-Service and Normal) The port is fully operational and performing as provisioned. • OOS-AU,AINS—(Out-Of-Service and Autonomous, Automatic In-Service) The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD—(Out-of-Service and Management, Disabled) The port is out-of-service and unable to carry traffic. • OOS-MA,MT—(Out-of-Service and Management, Maintenance) The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, in 15-minute increments

Table 18-4 describes the values on the Provisioning > Line Thresholds tabs.

Table 18-4 Line Thresholds Options for DS1-14 and DS1N-14 Cards

Parameter	Description
Port	(Display only) Port number; 1 to 14
CV	Coding violations
ES	Errored seconds
SES	Severely errored seconds
LOSS	Number of one-second intervals containing one or more loss of signal (LOS) defects
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 18-5 describes the values on the Provisioning > Elect Path Thresholds tabs.

Table 18-5 Electrical Path Threshold Options for DS1-14 and DS1N-14 Cards

Parameter	Description
Port	(Display only) Port number; 1 to 14
CV	Coding violations
ES	Errored seconds
SES	Severely errored seconds
SAS	Severely errored frame/alarm indication signal
AISS	Alarm indication signal seconds
UAS	Unavailable seconds
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 18-6 describes the values on the Provisioning > SONET Thresholds tabs for the DS-1 cards.

Table 18-6 SONET Threshold Options for DS1-14 and DS1N-14 Cards

Parameter	Description
Port	(Display only) DS-1 ports partitioned for STS. Line 1, STS 1, Line 2, STS 1 Line 3, STS 1, Line 4, STS 1
CV	Coding violations
ES	Errored seconds
FC	Failure count
SES	Severely errored seconds
UAS	Unavailable seconds
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Note The threshold value appears after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-A166 Change Line and Threshold Settings for a DS3-12 or DS3N-12 Card

Purpose	This task changes the line and threshold settings for a DS3-12 or DS3N-12 card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 Double-click the DS3-12 or DS3N-12 card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line, Line Thresholds, Elect Path Thresholds,** or **SONET Thresholds** tab.

Note See Chapter 8, "Manage Alarms" for information about the Alarm Profiles tab.

Note If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 4 Modify the settings found under these subtabs by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

For definitions of the line settings, see Table 18-7 on page 18-33. For definitions of the line threshold settings, see Table 18-8 on page 18-35. For definitions of the Elect Path Threshold settings, see Table 18-9 on page 18-36. For definitions of the SONET threshold settings, see Table 18-10 on page 18-36.

Table 18-7 describes the values on the Provisioning > Line tabs.

Table 18-7 Line Options for DS3-12 or DS3N-12 Cards

Parameter	Description	Options
Port	(Display only) Port number.	1 to 12
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 20-8.

Table 18-7 Line Options for DS3-12 or DS3N-12 Cards (continued)

Parameter	Description	Options
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450
Admin State	Sets the port administrative service state unless network conditions prevent the change.	• IS—Puts the port in-service. The port service state changes to IS-NR. • IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. • OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. • OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT. **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.

Table 18-7 Line Options for DS3-12 or DS3N-12 Cards (continued)

Parameter	Description	Options
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—(In-Service and Normal) The port is fully operational and performing as provisioned. • OOS-AU,AINS—(Out-Of-Service and Autonomous, Automatic In-Service) The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD—(Out-of-Service and Management, Disabled) The port is out-of-service and unable to carry traffic. • OOS-MA,MT—(Out-of-Service and Management, Maintenance) The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
AINS Soak	Sets the automatic in-service soak period.	Duration of the valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically 0 to 48 hours, 15-minute increments.

Table 18-8 describes the values on the Provisioning > Line Thresholds tabs.

Table 18-8 Line Threshold Options for DS3-12 or DS3N-12 Cards

Parameter	Description
Port	(Display only) Port number; 1 to 12
CV	Coding violations
ES	Errored seconds
SES	Severely errored seconds
LOSS	Loss of signal seconds; number of one-second intervals containing one or more LOS defects
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 18-9 describes the values on the Provisioning > Elect Path Thresholds tabs.

Table 18-9 Electrical Path Threshold Options for DS3-12 or DS3N-12 Cards

Parameter	Description
Port	(Display only) Port number; 1 to 12
EB	Errored blocks
BBE	Background block errors
ES	Errored seconds
SES	Severely errored seconds
UAS	Unavailable seconds
AISS	Alarm indication signal seconds
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 18-10 describes the values on the Provisioning > SONET Thresholds tabs.

Table 18-10 SONET Threshold Options for DS3-12 or DS3N-12 Cards

Parameter	Description
Port	(Display only) DS-3 ports partitioned for STS. Line 1, STS 1, Line 2, STS 1 Line 3, STS 1, Line 4 STS 1
CV	(Near and Far End, STS termination only) Coding violations
ES	(Near and Far End, STS termination only) Errored seconds
FC	(Near and Far End, STS termination only) Failure count
SES	(Near and Far End, STS termination only) Severely errored seconds
UAS	(Near and Far End, STS termination only) Unavailable seconds
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Note The threshold value appears after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-A167 Change Line and Threshold Settings for a DS3E-12 or DS3N-12E Card

Purpose	This task changes the line and threshold settings for a DS3E-12 or DS3N-12E (DS3E) card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Note If the DS3E is installed in an ONS 15454 slot that is provisioned for a DS-3 card, the DS3E enhanced performance monitoring parameters are unavailable. If this occurs, remove the DS3E from the ONS 15454, delete the DS-3 card in CTC using the "DLP-A191 Delete a Card" task on page 18-64, and provision the slot for the DS3E using the "DLP-A330 Preprovision a Card Slot" task on page 20-20.

Step 1 Double-click the DS3E-12 or DS3N-12E card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line, Line Thresholds, Elect Path Thresholds**, or **SONET Thresholds** tab.

Note See Chapter 8, "Manage Alarms" for information about the Alarm Profiles tab.

Note If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 4 Modify the settings found under these subtabs by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has a parameter you want to provision.

For definitions of the line settings, see Table 18-11. For definitions of the line threshold settings, see Table 18-12 on page 18-40. For definitions of the electrical path threshold settings, see Table 18-13 on page 18-41. For definitions of the SONET threshold settings, see Table 18-14 on page 18-41.

Table 18-11 describes the values on the Provisioning > Line tabs.

Table 18-11 Line Options for the DS3-12E and DS3N-12E Cards

Parameter	Description	Options
Port #	(Display only) Port number.	1 to 12
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 20-8.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Line Type	Defines the line framing type.	• M13 • C Bit • Auto Provisioned
Detected Line Type	(Display only) Displays the detected line type.	• M13 • C Bit • Unframed • Unknown
Line Coding	Defines the DS3E transmission coding type.	B3ZS
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450

Table 18-11 Line Options for the DS3-12E and DS3N-12E Cards (continued)

Parameter	Description	Options
Admin State	Sets the port administrative service state unless network conditions prevent the change.	• IS—Puts the port in-service. The port service state changes to IS-NR. • IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. • OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. • OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT. **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.

Table 18-11 Line Options for the DS3-12E and DS3N-12E Cards (continued)

Parameter	Description	Options
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—(In-Service and Normal) The port is fully operational and performing as provisioned. • OOS-AU,AINS—(Out-Of-Service and Autonomous, Automatic In-Service) The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD—(Out-of-Service and Management, Disabled) The port is out-of-service and unable to carry traffic. • OOS-MA,MT—(Out-of-Service and Management, Maintenance) The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed. **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments

Table 18-12 describes the values on the Provisioning > Line Thresholds tabs.

Table 18-12 Line Threshold Options for the DS3-12E and DS3N-12E Cards

Parameter	Description
Port	(Display only) Port number; 1 to 12
CV	Coding violations
ES	Errored seconds
SES	Severely errored seconds
LOSS	Loss of signal seconds; number of one-second intervals containing one or more LOS defects

Table 18-12 Line Threshold Options for the DS3-12E and DS3N-12E Cards (continued)

Parameter	Description
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 18-13 describes the values on the Provisioning > Elect Path Thresholds tabs.

Table 18-13 Electrical Path Options for the DS3-12E and DS3N-12E Cards

Parameter	Description
Port	(Display only) Port number; 1 to 12
CV	Coding violations. Available for DS3 Pbit, Near End only; and DS3 CPbit, Near End and Far End.
ES	Errored seconds. Available for DS3 Pbit, Near End only; and DS3 CPbit: Near end and Far End.
SES	Severely errored seconds. Available for DS3 Pbit, Near End only; and DS3 CPbit, Near End and Far End.
SAS	Severely errored frame/alarm indication signal. Available for DS3 Pbit, Near End only; and DS3 CPbit, Near End and Far End.
AIS	Alarm indication signal. Available for DS3 Pbit, Near End only; and DS3 CPbit, Near End and Far End.
UAS	Unavailable seconds. Available for DS3 Pbit, Near End only; and DS3 CPbit, Near End and Far End.
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 18-14 describes the values on the Provisioning > SONET Thresholds tabs.

Table 18-14 SONET Threshold Options for DS3-12E and DS3N-12E Cards

Parameter	Description
Port	(Display only) DS-3 ports partitioned for STS. Line 1, STS 1, Line 2, STS 1 Line 3, STS 1, Line 4 STS 1
CV	Coding violations. Available for Near and Far End, STS termination only.
ES	Errored seconds. Available for Near and Far End, STS termination only.
FC	Failure count. Available for Near and Far End, STS termination only.

Table 18-14 SONET Threshold Options for DS3-12E and DS3N-12E Cards (continued)

Parameter	Description
SES	Severely errored seconds. Available for Near and Far End, STS termination only.
UAS	Unavailable seconds. Available for Near and Far End, STS termination only.
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Note The threshold value appears after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-A168 Change Line and Threshold Settings for the DS3XM-6 Card

Purpose	This task changes the line and threshold settings for the DS3XM-6 card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The DS3XM-6 (transmux) card can accept up to six channelized DS-3 signals and convert each signal to 28 VT1.5 signals. Conversely, the card can take 28 T-1s and multiplex them into a channeled C-bit or M13 framed DS-3.

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 In node view, double-click the DS3XM-6 card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line, Line Thresholds, Elect Path Thresholds,** or **SONET Thresholds** tab.

Note See Chapter 8, "Manage Alarms" for information about the Alarm Profiles tab.

Note If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 4 Modify the settings found under these subtabs by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

For definitions of the line settings, see Table 18-15. For definitions of the line threshold settings, see Table 18-16 on page 18-45. For definitions of the electrical path threshold settings, see Table 18-17 on page 18-46. For definitions of the SONET threshold settings, see Table 18-18 on page 18-46.

Table 18-15 describes the values on the Provisioning > Line tabs for the DS3XM-6 cards.

Table 18-15 Line Options for the DS3XM-6 Parameters

Parameter	Description	Options
Port	(Display only) Sets the port number	1 to 6
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 20-8.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Line Type	Defines the line framing type.	• M13 - default • C BIT
Line Coding	Defines the DS-1 transmission coding type that is used.	B3ZS
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450

Table 18-15 Line Options for the DS3XM-6 Parameters (continued)

Parameter	Description	Options
Admin State	Sets the port administrative service state unless network conditions prevent the change.	• IS—Puts the port in-service. The port service state changes to IS-NR. • IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. • OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. • OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT. **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.

Table 18-15 Line Options for the DS3XM-6 Parameters (continued)

Parameter	Description	Options
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—(In-Service and Normal) The port is fully operational and performing as provisioned. • OOS-AU,AINS—(Out-Of-Service and Autonomous, Automatic In-Service) The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD—(Out-of-Service and Management, Disabled) The port is out-of-service and unable to carry traffic. • OOS-MA,MT—(Out-of-Service and Management, Maintenance) The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments

Table 18-16 describes the values on the Provisioning > Line Thresholds tabs for DS3XM-6 cards.

Table 18-16 Line Threshold Options for the DS3XM-6 Card

Parameter	Description
Port	(Display only) Port number; 1 to 6
CV	Coding violations
ES	Errored seconds
SES	Severely errored seconds
LOSS	Loss of signal seconds

Table 18-16 Line Threshold Options for the DS3XM-6 Card (continued)

Parameter	Description
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 18-17 describes the values on the Provisioning > Elect Path Thresholds tabs for the DS3XM-6 cards.

Table 18-17 Electrical Path Threshold Options for the DS3XM-6 Card

Parameter	Description
Port	(Display only) Port number. 1 to 6.
CV	Coding violations. Available for DS3, Pbit Near End only; DS3 CPbit, Near End and Far End; and DS1, only if a VT circuit is dropped on the port.
ES	Errored seconds. Available for DS3, Pbit Near End only; DS3 CPbit, Near End and Far End; and DS1, only if a VT circuit is dropped on the port.
SES	Severely errored seconds. Available for DS3, Pbit Near End only; DS3 CPbit, Near End and Far End; and DS1, only if a VT circuit is dropped on the port.
SAS	Severely errored frame/alarm indication signal. Available for DS3, Pbit Near End only; DS3 CPbit, Near End and Far End; and DS1, only if a VT circuit is dropped on the port.
AISS	Alarm indication signal seconds. Available for DS3, Pbit Near End only; DS3 CPbit, Near End and Far End; and DS1, only if a VT circuit is dropped on the port.
UAS	Unavailable seconds. Available for DS3, Pbit Near End only; DS3 CPbit, Near End and Far End; and DS1, only if a VT circuit is dropped on the port.
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 18-18 describes the values on the Provisioning > SONET Thresholds tabs for the DS3XM-6 cards.

Table 18-18 SONET Threshold Options for the DS3XM-6 Card

Parameter	Description
CV	Coding violations
ES	Errored seconds
FC	Failure count

Table 18-18 SONET Threshold Options for the DS3XM-6 Card (continued)

Parameter	Description
SES	Severely errored seconds
UAS	Unavailable seconds
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Note The threshold value appears after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-A169 Change Line and Threshold Settings for the EC1-12 Card

Purpose	This task changes the line and threshold settings for the EC1-12 (EC-1) card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 In node view, double-click the EC-1 card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line** or **SONET Thresholds** tabs.

Note See Chapter 8, "Manage Alarms" for information about the Alarm Profiles tab.

Note The STS subtab is used to provision intermediate path performance monitoring (IPPM). To provision IPPM, circuits must be provisioned on the EC1-12 card. For circuit creation procedures, go to Chapter 6, "Create Circuits and VT Tunnels." To provision IPPM, go to the "DLP-A121 Enable/Disable Pointer Justification Count Performance Monitoring" task on page 18-7.

Note If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 4 Modify the settings found under these subtabs by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

Table 18-19 describes the values on the Line tab for the EC1-12 card. For definitions of the SONET threshold settings, see Table 18-20 on page 18-50.

Table 18-19 Line Options for the EC1-12 Card

Parameter	Description	Options
Port	(Display only) Port number.	1 to 12
Port Name	(Optional) Sets a name for the port.	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 20-8.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
PJStsMon#	Sets the STS that will be used for pointer justification; if set to zero, no STS is used.	• 0 (default) • 1
Line Buildout	Defines the distance (in feet) from backplane to next termination point.	• 0 - 225 (default) • 226 - 450

Table 18-19 Line Options for the EC1-12 Card (continued)

Parameter	Description	Options
Rx Equalization	For early EC1-12 card versions, equalization can be turned off if the line length is short or the environment is extremely cold; Rx Equalization should normally be set to On.	• On (checked, default) • Off (unchecked)
Admin State	Sets the port administrative service state unless network conditions prevent the change.	• IS—Puts the port in-service. The port service state changes to IS-NR. • IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. • OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. • OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT. **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.

Table 18-19 Line Options for the EC1-12 Card (continued)

Parameter	Description	Options
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—(In-Service and Normal) The port is fully operational and performing as provisioned. • OOS-AU,AINS—(Out-Of-Service and Autonomous, Automatic In-Service) The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD—(Out-of-Service and Management, Disabled) The port is out-of-service and unable to carry traffic. • OOS-MA,MT—(Out-of-Service and Management, Maintenance) The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments

Table 18-20 lists the values on the SONET Thresholds tab for EC1-12 cards.

Table 18-20 SONET Threshold Options for the EC1-12 Card

SONET Layer	Parameter	Description
All	Port #	(Display only) EC-1 card port number; 1 to 12
Line (L)	CV	Coding violations
	ES	Errored seconds
Line (L)	SES	Severely errored seconds
	FC	Failure count
	UAS	Unavailable seconds

Table 18-20 SONET Threshold Options for the EC1-12 Card (continued)

SONET Layer	Parameter	Description
Section (S)	CV	Coding violations (Near End only)
	ES	Errored seconds
	SES	Severely errored seconds
	SEFS	Severely errored framing seconds
Path (P)	CV	Coding violations (Near End and Far End)
	ES	Errored seconds
	FC	Failure count
	SES	Severely errored seconds
	UAS	Unavailable seconds

Step 7 Return to your originating procedure (NTP).

DLP-A171 Change Threshold Settings for OC-N Cards

Purpose	This task changes threshold settings for OC-N cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 In node view, double-click the OC-N card where you want to change the threshold settings.

Step 2 Click the **Provisioning > SONET Thresholds** tabs.

Note If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 3 Modify the settings described in Table 18-21 by clicking in the field you want to modify and typing in the desired value.

Step 4 Click **Apply**.

Table 18-21 OC-N Threshold Options

Parameter	Description
Port	Port number • 1 (OC-3, OC-12, OC-48, OC-192) • 1-4 (OC12-4) • 1-12: PPM 1 (MRC_12)
CV	Coding violations
ES	Errored seconds
SES	Severely errored seconds
SEFS	Severely errored framing seconds
FC	Failure count
UAS	Unavailable seconds
PSC	Protection Switching Count (Line)
PSD	Protection Switch Duration (Line)
PSC-W	Protection Switching Count - Working line **Note** Bidirectional line switch rings (BLSRs) are not supported on the OC-3 card; therefore, the PSC-W, PSC-S, and PSC-R performance monitoring parameters (PMs) do not increment.
PSD-W	Protection Switching Duration - Working line **Note** BLSR is not supported on the OC-3 card; therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.
PSC-S	Protection Switching Duration - Span **Note** BLSR is not supported on the OC-3 card; therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.
PSD-S	Protection Switching Duration - Span **Note** BLSR is not supported on the OC-3 card; therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.
PSC-R	Protection Switching Count - Ring **Note** BLSR is not supported on the OC-3 card; therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.
PSD-R	Protection Switching Duration - Ring **Note** BLSR is not supported on the OC-3 card; therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.

Step 5 Return to your originating procedure (NTP).

DLP-A172 Change an Optical Port to SDH

Purpose	This task provisions a port on an OC-N card for SDH. You must put the port in the OOS,MT administrative service state before changing the port to SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 DLP-A214 Change the Service State for a Port, page 19-9
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the OC-N card where you want to provision a port for SDH.

Step 2 Click the **Provisioning > Line** tabs.

Step 3 In the Type field for the desired port, choose **SDH**.

Note Before you change the port type to SDH, ensure the following: the EnableSyncMsg and SendDoNotUse fields are unchecked, the card is not part of a BLSR or 1+1 protection group, the card is not part of an orderwire channel, and the card is not a SONET data communications channel/generic communications channel (DCC/GCC) termination point.

Step 4 Click **Apply**.

Step 5 If the card is a multiport OC-N card, for example a four-port OC-3, eight-port OC-3, four-port OC-12, or MRC-12, you can repeat Steps 3 and 4 for any other ports on that card.

Step 6 Return to your originating procedure (NTP).

DLP-A176 Convert DS1-14 Cards From 1:1 to 1:N Protection

Purpose	This task converts DS1-14 cards in a 1:1 protection scheme to 1:N protection. A 1:N protection group can protect a maximum of five working cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This procedure assumes DS1-14 cards are installed in Slots 1 through 6 and/or Slots 12 through 17. The DS1-14 cards in Slots 3 and 15, which are the protection slots, will be replaced with DS1N-14 cards.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 Click the protection group that contains Slot 3 or Slot 15 (where you will install the DS1N-14 card).

Step 3 Make sure the slot you are upgrading is not carrying working traffic. In the Selected Group list, the protect slot must say Protect/Standby, not Protect/Active. If the protect slot status is Protect/Active, switch traffic to the working card:

a. Under Selected Group, click the protect card.

b. Next to Switch Commands, click **Switch**.

The working slot should change to Working/Active and the protect slot should change to Protect/Standby. If they do not change, do not continue. Troubleshoot the working card and slot to determine why the card cannot carry working traffic.

Step 4 Repeat Steps 1 through 3 for each protection group that you need to convert.

Step 5 Click the **Alarms** tab to verify that no standing alarms exist for any of the DS1-14 cards that you are converting. If alarms exist and you have difficulty clearing them, contact your next level of support.

Step 6 Click the **Provisioning > Protection** tabs.

Step 7 Click the 1:1 protection group that contains the cards that you will move into the new protection group.

Step 8 Click **Delete**.

Step 9 When the confirmation dialog box appears, click **Yes**.

Note Deleting the 1:1 protection group does not disrupt service. However, no protection bandwidth exists for the working circuits until you complete the 1:N protection procedure. Therefore, complete this procedure as quickly as possible.

Step 10 If needed, repeat Steps 7 to 9 for other DS-1 1:1 protection groups that you want to include in a 1:N group.

Step 11 Physically remove the DS1-14 card from Slot 3 or Slot 15. This raises an improper removal alarm (IMPROPRMVL).

Step 12 In node view, right-click the slot that held the removed card and select **Delete** from the shortcut menu. Wait for the card to disappear from node view.

Step 13 Physically insert a DS1N-14 card into the same slot.

Step 14 Verify that the card boots up properly.

Step 15 Click the **Inventory** tab and verify that the new card appears as a DS1N-14.

Step 16 Click the **Provisioning > Protection** tabs.

Step 17 Click **Create**.

Step 18 Type a name for the protection group in the Name field (optional).

Step 19 From the Type drop-down list, choose **1:N (card)**.

Step 20 From the Protect Card drop-down list, choose the DS1N-14 card. Verify that the correct DS1N-14 card appears in the Protect Card field.

Step 21 In the Available Cards list, highlight the cards that you want in the protection group. Click the arrow (>>) tab to move the cards to the Working Cards list.

Step 22 If necessary, set a new reversion time in the Reversion time drop-down list.

Note 1:N protection groups are always revertive.

Step 23 Click **OK**. The protection group appears in the Protection Groups list on the Protection subtab.

Step 24 Return to your originating procedure (NTP).

DLP-A177 Convert DS3-12 Cards From 1:1 to 1:N Protection

Purpose	This task converts DS3-12 cards in 1:1 protection to 1:N protection. A 1:N protection group can protect a maximum of five working cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This procedure assumes that DS3-12 cards are installed in Slots 1 to 6 and/or Slots 12 to 17. The DS3-12 cards in Slots 3 or 15, which are the protection slots, will be replaced with DS3N-12 cards. The ONS 15454 must run CTC Release 2.0 or later. The procedure also requires at least one DS3N-12 card and a protection group with DS3-12 cards.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 Click the protection group containing Slot 3 or Slot 15 (where you will install the DS3N-12 card).

Step 3 Make sure the slot that you are upgrading is not carrying working traffic. In the Selected Group list, the protect slot must say Protect/Standby, and not Protect/Active. If the protect slot status is Protect/Active, switch traffic to the working card:

a. Under Selected Group, click the protect card.

b. Next to Switch Commands, click **Switch**.

The working slot should change to Working/Active and the protect slot should change to Protect/Standby. If they fail to change, do not continue. Troubleshoot the working card and slot to determine why the card cannot carry working traffic.

Step 4 Repeat Steps 2 and 3 for each protection group that you need to convert.

Step 5 Click the **Alarms** tab to verify that no standing alarms exist for any of the DS3-12 cards you are converting. If alarms exist and you have difficulty clearing them, contact your next level of support.

Step 6 Click the **Provisioning > Protection** tabs.

Step 7 Click the 1:1 protection group that contains the cards that you will move into the new protection group.

Step 8 Click **Delete**.

Step 9 When the confirmation dialog box appears, click **Yes**.

Note Deleting the 1:1 protection groups will not disrupt service. However, no protection bandwidth exists for the working circuits until the 1:N protection procedure is completed. Therefore, complete this procedure as soon as possible.

Step 10 If you are deleting more than one DS-3 1:1 protection group, repeat Steps 7 through 9 for each group that you want to include in a 1:N group.

Step 11 Physically remove the protect DS3-12 card from Slot 3 or Slot 15. This raises an improper removal alarm (IMPROPRMVL).

Step 12 In node view, right-click the slot that held the removed card and choose **Delete** from the shortcut menu. Wait for the card to disappear from the node view.

Step 13 Physically insert a DS3N-12 card into the same slot.

Step 14 Verify that the card boots up properly.

Step 15 Click the **Inventory** tab and verify that the new card appears as a DS3N-12 card.

Step 16 Click the **Provisioning > Protection** tabs.

Step 17 Click **Create**.

Step 18 Type a name for the protection group in the Name field (optional).

Step 19 Click **Type** and choose **1:N (card)** from the drop-down list.

Step 20 Verify that the DS3N-12 card appears in the Protect Card field.

Step 21 In the Available Cards list, highlight the cards that you want in the protection group. Click the arrow (>>) tab to move the cards to the Working Cards list.

Step 22 Click **OK**.

The protection group should appear in the Protection Groups list on the Protection subtab.

Step 23 Return to your originating procedure (NTP).

DLP-A178 Convert DS3-12E Cards From 1:1 to 1:N Protection

Purpose	This task converts DS3-12E cards in 1:1 protection to 1:N protection. A 1:N protection group can protect a maximum of five working cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This task assumes that DS3-12E cards are installed in Slots 1 to 6 and/or Slots 12 to 17. The DS3-12E cards in Slots 3 or 15, which are the protection slots, will be replaced with DS3N-12E cards. The procedure requires at least one DS3N-12E card and a protection group with DS3-12E cards.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 Click the protection group containing Slot 3 or Slot 15 (where you will install the DS3N-12E card).

Step 3 Make sure the slot you are upgrading is not carrying working traffic. In the Selected Group list, the protect slot must say Protect/Standby, and not Protect/Active. If the protect slot status is Protect/Active, switch traffic to the working card:

a. Under Selected Group, click the protect card.

b. Next to Switch Commands, click **Switch**.

The working slot should change to Working/Active and the protect slot should change to Protect/Standby. If they fail to change, do not continue. Troubleshoot the working card and slot to determine why the card cannot carry working traffic.

Step 4 Repeat Steps 2 and 3 for each protection group that you need to convert.

Step 5 Click the **Alarms** tab to verify that no standing alarms exist for any of the DS3-12E cards you are converting. If alarms exist and you have difficulty clearing them, contact your next level of support.

Step 6 Click the **Provisioning > Protection** tab.

Step 7 Click the 1:1 protection group that contains the cards that you will move into the new protection group.

Step 8 Click **Delete**.

Step 9 When the confirmation dialog box appears, click **Yes**.

Note Deleting the 1:1 protection groups will not disrupt service. However, no protection bandwidth exists for the working circuits until the 1:N protection procedure is completed. Do not delay when completing this procedure.

Step 10 If you are deleting more than one DS-3 1:1 protection group, repeat Steps 7 through 9 for each group that you want to include in a 1:N group.

Step 11 Physically remove the protect DS3-12E card from Slot 3 or Slot 15. This raises an improper removal alarm (IMPROPRMVL).

Step 12 In node view, right-click the slot that held the removed card and choose **Delete** from the shortcut menu. Wait for the card to disappear from the node view.

Step 13 Physically insert a DS3N-12E card into the same slot.

Step 14 Verify that the card boots up properly.

Step 15 Click the **Inventory** tab and verify that the new card appears as a DS3N-12E.

Step 16 Click the **Provisioning > Protection** tabs.

Step 17 Click **Create**.

Step 18 Type a name for the protection group in the Name field (optional).

Step 19 Click **Type** and choose **1:N (card)** from the drop-down list.

Step 20 Verify that the DS3N-12E card appears in the Protect Card field.

Step 21 In the Available Cards list, highlight the cards that you want in the protection group. Click the arrow (**>>**) tab to move the cards to the Working Cards list.

Step 22 Click **OK**.

The protection group should appear in the Protection Groups list on the Protection subtab.

Step 23 Return to your originating procedure (NTP).

DLP-A189 Verify that a 1+1 Working Slot is Active

Purpose	This task verifies that a working slot in a 1+1 protection scheme is active (and that the protect slot is in standby).
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Selected Group area, verify that the working slot/port is shown as Working/Active. If so, this task is complete.

Step 3 If the working slot says Working/Standby, perform a Manual switch on the working slot:

- **a.** In the Selected Group area, choose the Protect/Active slot.
- **b.** In the Switch Commands field, choose **Manual**.
- **c.** Click **Yes** in the confirmation dialog box.

Step 4 Verify that the working slot is carrying traffic (Working/Active).

Note If the slot is not active, look for conditions or alarms that might be preventing the card from carrying working traffic. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for alarm descriptions and instructions.

Step 5 When the working slot is carrying traffic, clear the Manual switch:

- **a.** In the Switch Commands field, choose **Clear**.
- **b.** Click **Yes** in the confirmation dialog box.

Step 6 Verify that the working slot does not revert to Standby, which might indicate a problem on the working span.

Step 7 Return to your originating procedure (NTP).

DLP-A190 Install a UBIC-V EIA

Purpose	This task installs a Universal Backplane Interface Connector—Vertical (UBIC-V) EIA.
Tools/Equipment	#2 Phillips screwdriver Small slot-head screwdriver 6 perimeter screws, 6-32 x 0.375-inch Phillips head (P/N 48-0422-01) UBIC-V, A side (15454-EIA-UBICV-A) EIA panel and/or UBIC-V, B side (15454-EIA-UBICV-B) EIA panel
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution Always use an electrostatic discharge (ESD) wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Note UBIC-V EIAs can only be installed on shelf assembly 15454-SA-HD. 15454-SA-HD shelf assemblies are differentiated from other shelf assemblies by the blue hexagon symbol, which indicates the available high-density slots, found under Slots 1 through 3 and 15 through 17.

Note UBIC-V or UBIC-H EIAs are required when using high-density (48-port DS-3 and 12-port DS3XM) electrical cards.

Step 1 Locate the correct UBIC-V EIA for the side you want to install and remove the UBIC EIA-V from the packaging.

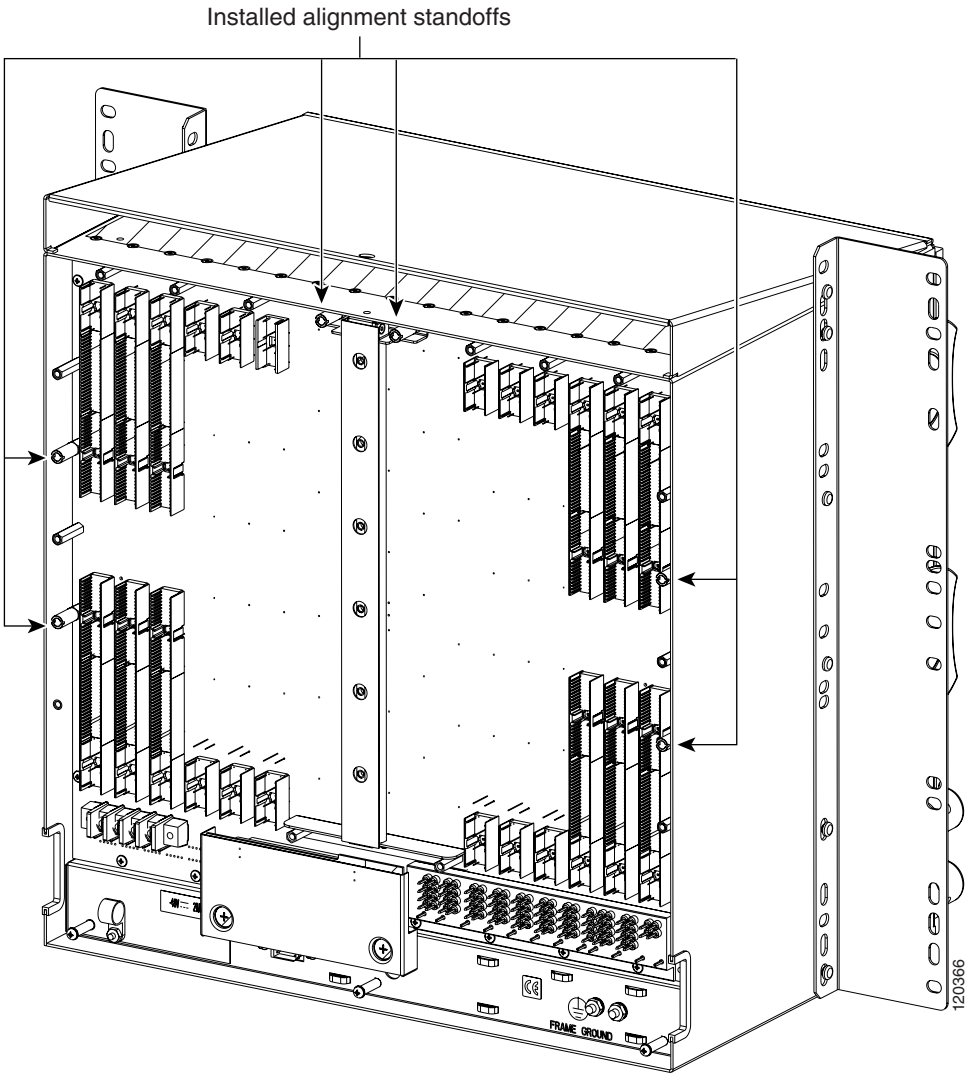
Step 2 Verify that none of the pins on the UBIC EIA are bent.

Step 3 If present, remove the yellow connector protectors.

Step 4 If screws are present in the alignment standoff holes, use a Phillips screwdriver to remove them.

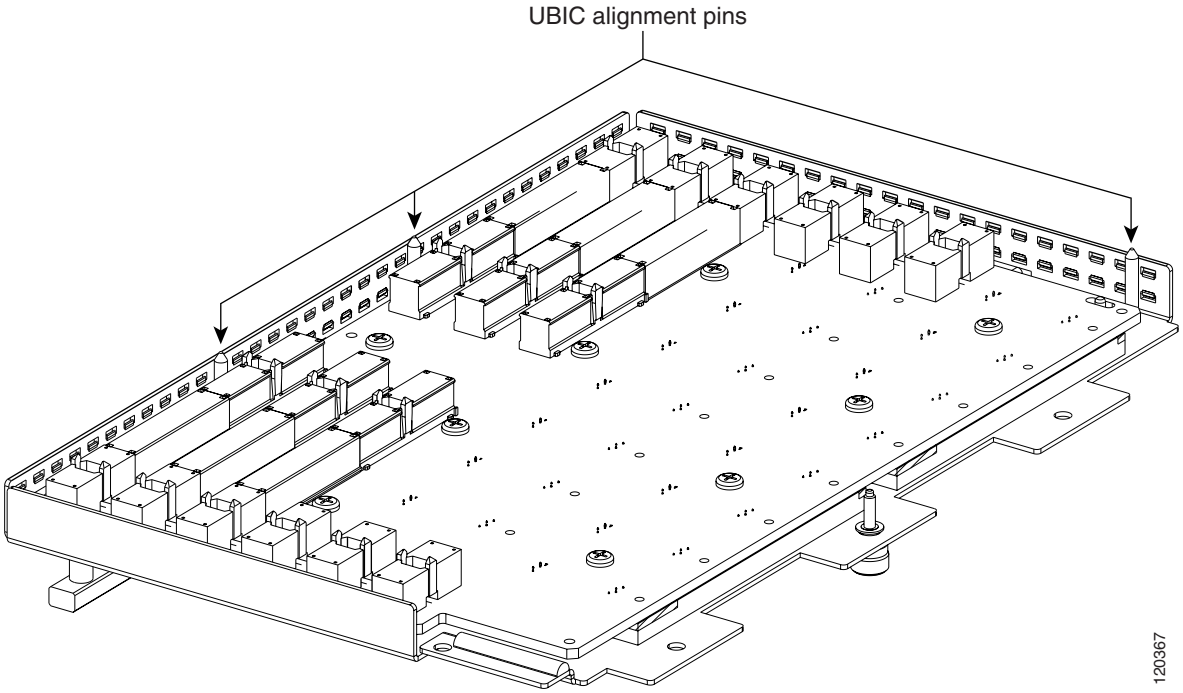
Step 5 Use a flathead screwdriver or 5/16-inch deep socket wrench to tighten the standoffs at 8 to 10 inch pound-force (lb-in) (9.2 to 11.5 centimeter kilogram-force[kgf-cm]). Figure 18-6 shows the alignment standoffs installed on the shelf.

Figure 18-6 Installed Alignment Standoffs



Step 6 Line up the alignment pins on the UBIC EIA with the alignment standoffs on the shelf and push the UBIC EIA with consistent pressure until the pins and standoffs fit together firmly (Figure 18-7).

Figure 18-7 UBIC-V Alignment Pins

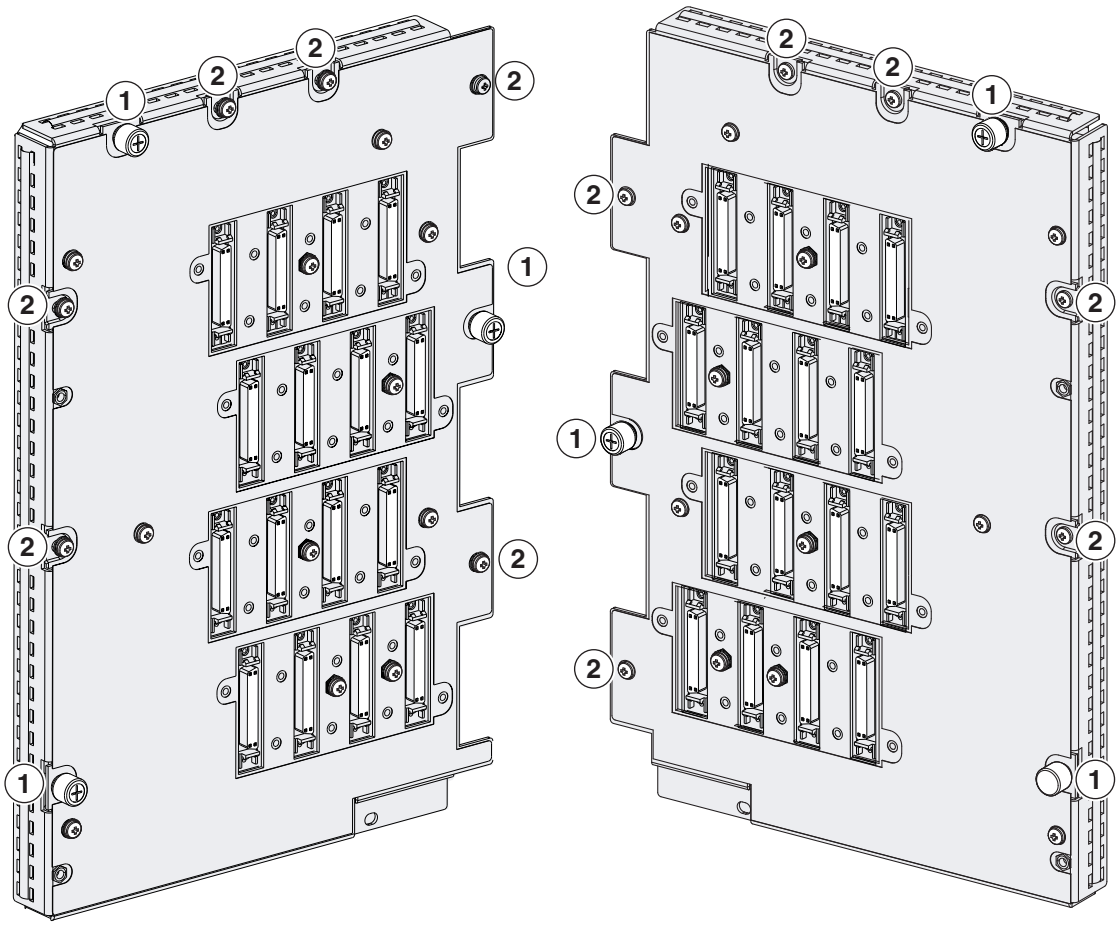


Caution Do not force the UBIC-V EIA onto the shelf if you feel strong resistance.

Step 7 Locate the three jack screws on the UBIC-V (Figure 18-8). Starting with any jack screw, tighten the thumb screw a few turns and move to the next one, turning each thumb screw a few turns at a time until all three screws are hand tight (Figure 18-9).

Caution Tightening the jack screws unevenly could cause damage to the UBIC-V connectors.

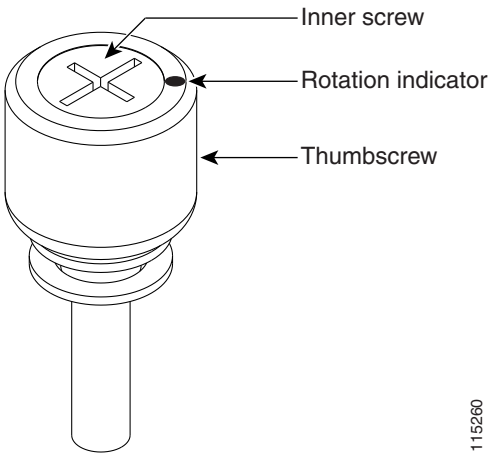
Figure 18-8 UBIC-V EIA Screw Locations



1 Jack screws (3)

2 Perimeter screws, 6-32 x 0.375-inch Phillips head (6)

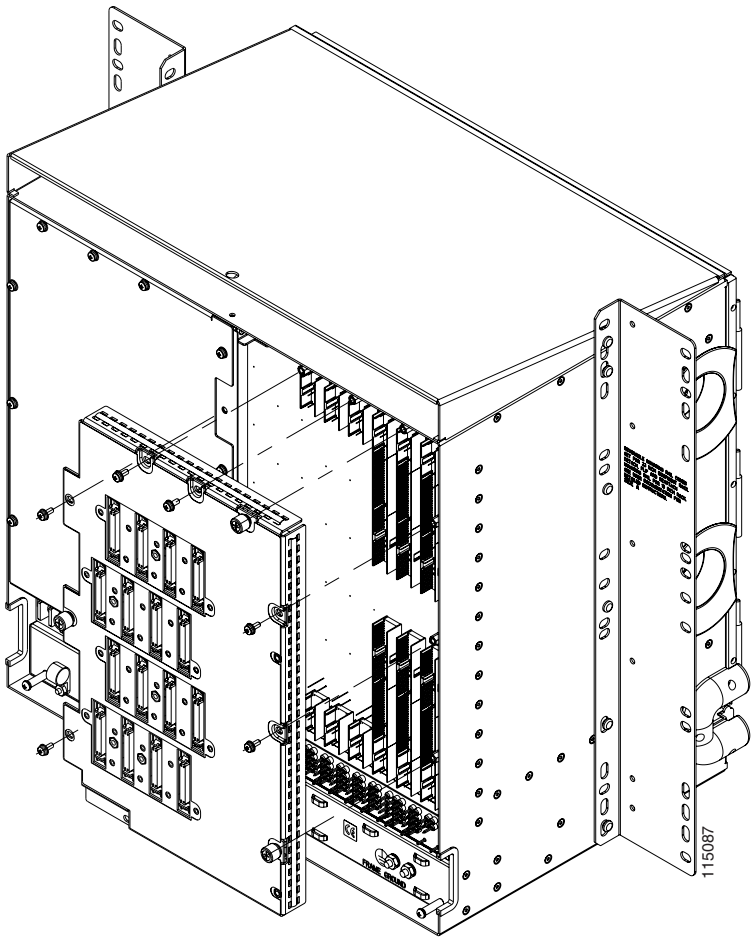
Figure 18-9 UBIC-V EIA Jack Screw



Step 8 Use a Phillips screwdriver to install the six perimeter screws and bracket screws (P/N 48-0422-01) at 8 to 10 lb-inch (9.2 to 11.5kgf-cm) to secure the cover panel to the backplane (Figure 18-8 on page 18-62). Install the alarm and timing panel cover and insert and tighten the last perimeter screw.

Figure 18-10 shows a UBIC-V EIA installation.

Figure 18-10 Installing the UBIC-V EIA



Step 9 Return to your originating procedure (NTP).

DLP-A191 Delete a Card

Purpose	This task deletes a card from CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the shelf graphic in CTC, right-click the card that you want to remove and choose **Delete Card**.

You cannot delete a card if any of the following conditions apply:

- The card is a TCC2/TCC2P card. To replace a TCC2/TCC2P card, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

- The card is part of a protection group; see the "DLP-A155 Delete a Protection Group" task on page 18-23.
- The card has circuits; see the "NTP-A278 Modify and Delete Overhead Circuits and Server Trails" procedure on page 7-5 and the "DLP-A333 Delete Circuits" task on page 20-21.
- The card is part of a BLSR; see the "NTP-A240 Remove a BLSR Node" procedure on page 14-7.
- The card is being used for timing; see the "DLP-A157 Change the Node Timing Source" task on page 18-24.
- The card has a DCC/GCC termination; see the "NTP-A292 Modify or Delete Communications Channel Terminations and Provisionable Patchcords" procedure on page 11-5.

Note If you delete a card in CTC but do not remove it from the shelf, it will reboot and reappear in CTC.

Step 2 Return to your originating procedure (NTP).

DLP-A194 Clear a BLSR Force Ring Switch

Purpose	This task removes a Force switch from a BLSR port.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click **Edit**.

Step 4 To clear a Force switch on the west line:

a. Right-click the BLSR west port where you want to clear the protection switch and choose **Set West Protection Operation**. Ports with a Force switch applied are marked with an F.

b. In the Set West Protection Operation dialog box, choose **CLEAR** from the pull-down menu. Click **OK**.

c. In the Confirm BLSR Operation dialog box, click **Yes**.

Step 5 To clear a Force switch on the east line:

a. Right-click the BLSR east port where you want to clear the protection switch and choose **Set East Protection Operation**. Ports with a Force switch applied are marked with an F.

b. In the Set East Protection Operation dialog box, choose **CLEAR** from the pull-down menu. Click **OK**.

c. In the Confirm BLSR Operation dialog box, click **Yes**.

On the BLSR network graphic, a green and a purple span line connects each node. This is the normal display for BLSRs when protection operations are not invoked.

Step 6 From the File menu, choose **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-A195 Verify Timing in a Reduced Ring

Purpose	This task verifies timing in the ring where you removed a node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite/remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 Observe the Timing Mode field to see the type of timing (Line, External, Mixed) that has been set for that node.

Step 3 Scroll down to the Reference Lists and observe the NE Reference fields to see the timing references provisioned for that node.

Step 4 If the removed node was the only BITS timing source, perform the following:

a. Contact your synchronization coordinator or appropriate personnel before continuing with this procedure.

b. Look for another node on the ring that can be used as a BITS source and set that node's Timing Mode to **External**. Choose that node as the primary timing source for all other nodes in the ring. See the "DLP-A157 Change the Node Timing Source" task on page 18-24.

c. If no node in the reduced ring can be used as a BITS source, choose one node to be your internal timing source. Set that node's Timing Mode to **External**, set BITS-1 and BITS-2 BITS In State to **OOS**, and set the NE Reference to **Internal**. Then, choose line timing for all other nodes in the ring. This forces the first node to be their primary timing source. (See the "DLP-A157 Change the Node Timing Source" task on page 18-24.)

Note This type of timing conforms to Stratum 3 requirements and is not considered optimal.

Step 5 If the removed node was not the only BITS timing source, provision the adjacent nodes to line timing using SONET links (east and west) as timing sources, traceable to the node with external BITS timing. See the "NTP-A28 Set Up Timing" procedure on page 4-13.

Step 6 Return to your originating procedure (NTP).

DLP-A196 Delete a BLSR from a Single Node

Purpose	This task deletes a BLSR from a node after you remove the node from the BLSR.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, display the node that was removed from the BLSR:

- If the node that was removed is connected to the same LAN as your computer, from the File menu, choose **Add Node**, then enter the node name or IP address.
- If the node that was removed is not connected to the same LAN as your computer, you must connect to the node using a direct connection. See Chapter 3, "Connect the PC and Log into the GUI" for procedures.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Highlight the ring and click **Delete**.

Step 4 In the Suggestion dialog box, click **OK**.

Step 5 In the confirmation message, confirm that this is the ring you want to delete. If so, click **Yes**.

Step 6 Return to your originating procedure (NTP).

DLP-A197 Initiate a Path Protection Force Switch

Purpose	This task switches all circuits on a path protection span to another span.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Caution The Force Switch Away command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution Traffic is not protected during a Force protection switch.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Right-click the span where you want to switch path protection traffic away. Choose **Circuits** from the shortcut menu.

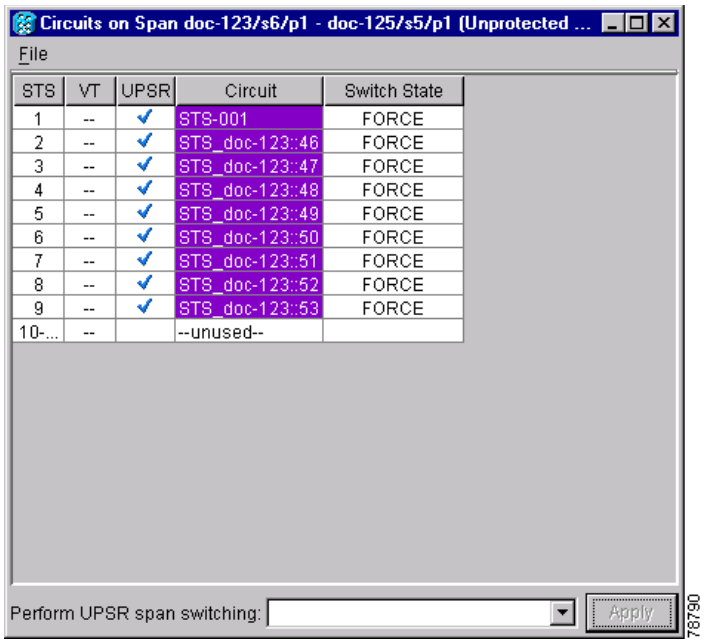
Step 3 In the Circuits on Span dialog box, choose **FORCE SWITCH AWAY**. Click **Apply**.

Step 4 In the Confirm Path Protection Switch dialog box, click **Yes**.

Step 5 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the Switch State for all circuits is FORCE. Figure 18-11 shows an example.

Figure 18-11 Circuits on Span Dialog Box with a Force Switch



Note A Force switch request on a span or card causes CTC to raise a FORCED-REQ condition. The condition clears when you clear the Force switch.

Step 6 Return to your originating procedure (NTP).

DLP-A198 Clear a Path Protection Force Switch

Purpose	This task clears a path protection Force switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 From the View menu at the node view, choose **Go to Network View**.

Step 2 Right-click the span where you want to clear the switch. Choose **Circuits** from the shortcut menu.

Step 3 In the Circuits on Span dialog box, choose **CLEAR** to remove the Force switch. Click **Apply**.

Step 4 In the Confirm Path Protection Switch dialog box, click **Yes**.

Step 5 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the Switch State for all path protection circuits is CLEAR.

Step 6 Return to your originating procedure (NTP).

CHAPTER 19

DLPs A200 to A299

Note The terms “Unidirectional Path Switched Ring” and “UPSR” may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as “Path Protected Mesh Network” and “PPMN,” refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

DLP-A201 Apply a Lock-on

Purpose	This task prevents traffic from being switched from one card or port to another.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Note To apply a lock-on to a protect card in a 1:1 or 1:N protection group, the protect card must be active. If the protect card is in standby, the Lock On button is disabled. To make the protect card active, you must switch traffic from the working card to the protect card (Step 4). When the protect card is active, you can apply the lock on.

Step 1 Use the following rules to determine if you can apply a lock on:

- For a 1:1 electrical protection group, the working or protect cards can be placed in the Lock On state.
- For a 1:N electrical protection group, the working or protect cards can be placed in the Lock On state.
- For a 1+1 optical protection group, only the working port can be placed in the Lock On state.

Step 2 In node view, click the **Maintenance > Protection** tabs.

Step 3 In the Protection Groups list, click the protection group where you want to apply a lock on.

Step 4 If you determine that the protect card is in standby mode and you want to apply the lock on to the protect card, make the protect card active:

a. In the Selected Group list, click the protect card.

b. In the Switch Commands area, click **Force**.

Step 5 In the Selected Group list, click the active card where you want to lock traffic.

Step 6 In the Inhibit Switching area, click **Lock On**.

Step 7 Click **Yes** in the confirmation dialog box.

The lock on has been applied and traffic cannot be switched to the working card. To clear the lock-on, see the "DLP-A203 Clear a Lock-on or Lockout" task on page 19-3.

Step 8 Return to your originating procedure (NTP).

DLP-A202 Apply a Lockout

Purpose	This task switches traffic from one card to another using a lockout, which is a switching mechanism that overrides other external switching commands (Force, Manual, and Exercise).
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Note Multiple lockouts in the same protection group are not allowed.

Step 1 Use the following rules to determine if you can put the intended card in a lockout state:

- For a 1:1 electrical protection group, you can apply a lockout to the working or protect cards.
- For a 1:N electrical protection group, you can apply a lockout to the working or protect cards.
- For a 1+1 optical protection group, you can apply a lockout to the protect port.

Step 2 In node view, click the **Maintenance > Protection** tabs.

Step 3 In the Protection Groups list, click the protection group that contains the card you want to lock out.

Step 4 In the Selected Group list, click the card where you want to lock out traffic.

Step 5 In the Inhibit Switching area, click **Lock Out**.

Step 6 Click **Yes** in the confirmation dialog box.

The lock out has been applied and traffic is switched to the opposite card. To clear the lockout, see the "DLP-A203 Clear a Lock-on or Lockout" task on page 19-3.

Note Provisioning a lockout raises a LOCKOUT-REQ condition in Cisco Transport Controller (CTC). If applied to a span, the FE-LOCKOUTOFPR-SPAN condition is also raised. Clearing the lockout switch request clears these conditions.

Step 7 Return to your originating procedure (NTP).

DLP-A203 Clear a Lock-on or Lockout

Purpose	This task clears a lock-on or lockout.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 DLP-A201 Apply a Lock-on, page 19-1 or DLP-A202 Apply a Lockout, page 19-2
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group that contains the card you want to clear.

Step 3 In the Selected Group list, click the card you want to clear.

Step 4 In the Inhibit Switching area, click **Unlock**.

Step 5 Click **Yes** in the confirmation dialog box.

The lock-on or lockout is cleared.

Step 6 Return to your originating procedure (NTP).

DLP-A204 Clean Multi Fiber-Optic Cable Connectors

Purpose	This task cleans the multi fiber optic connectors
Tools/Equipment	Cleaning Cartridge for multi fiber optic connectors
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Step 1 Remove the protective cap on the optical fiber cable connector.

Step 2 Read the manufacturer (cleaning cartridge) instructions to insert the connector into the cleaning cartridge.

Step 3 Slide the lever on the cartridge to swipe the connector surface.

Step 4 Insert the fiber connector into the applicable adapter or attach a dust cap to the fiber connector.

Note If you must replace a dust cap on a connector, first verify that the dust cap is clean.

Step 5 Return to your originating procedure (NTP).

DLP-A205 Clean Fiber Connectors with CLETOP

Purpose	This task cleans the fiber connectors with CLETOP.
Tools/Equipment	Type A Fiber Optic Connector Cleaner (CLETOP reel) Optical receiver cleaning stick
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Remove the dust cap from the fiber connector.

Step 2 Press the lever down to open the shutter door. Each time you press the lever, you expose a clean wiping surface.

Step 3 Insert the connector into the CLETOP cleaning cassette slot, rotate one quarter turn, and gently swipe downwards.

Step 4 Use an inspection microscope to inspect each fiber connector for dirt, cracks, or scratches. If the connector is not clean, repeat Steps 1 to 3.

Step 5 Insert the fiber connector into the applicable adapter or attach a dust cap to the fiber connector.

Note If you must replace a dust cap on a connector, first verify that the dust cap is clean. To clean the dust cap, wipe the outside of the cap using a dry, lint-free wipe and the inside of the dust cap using a CLETOP stick swab (14100400).

Step 6 Return to your originating procedure (NTP).

DLP-A206 Clean the Fiber Adapters

Purpose	This task cleans the fiber adapters.
Tools/Equipment	CLETOP stick swab

Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Remove the dust plug from the fiber adapter.

Step 2 Insert a CLETOP stick swab (14100400) into the adapter opening and rotate the swab.

Step 3 Place dust plugs on the fiber adapters when not in use.

Step 4 Return to your originating procedure (NTP).

DLP-A207 Install Fiber-Optic Cables on the LGX Interface

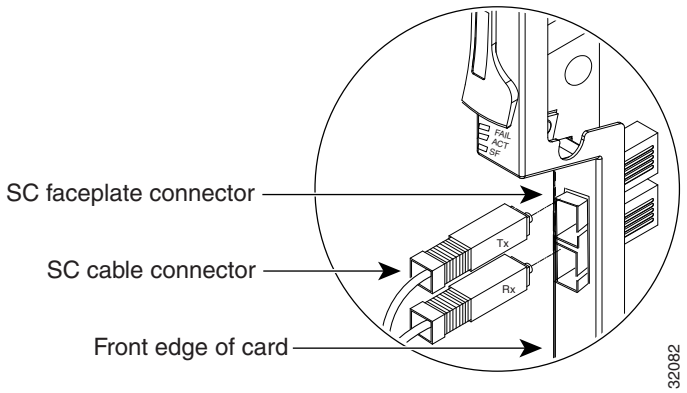
Purpose	This task installs fiber-optic cables on the Lightguide Cross Connect (LGX) interface in the central office.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors, page 15-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Align the keyed ridge of the cable connector with the receiving SC connector on the LGX faceplate connection point. Each module supports at least one transmit and one receive connector to create an optical carrier port.

Step 2 Gently insert the cable connector into the faceplate connection point until the connector snaps into place.

Step 3 Connect the fiber-optic cable to the OC-N card. Figure 19-1 shows the cable location.

Figure 19-1 Installing Fiber-Optic Cables



Step 4 Return to your originating procedure (NTP).

DLP-A208 Change External Alarms Using the AIC-I Card

Purpose	This task changes external alarm settings on the Alarm Interface Controller-International (AIC-I) card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The procedure is the same if you are using the AEP. In this case, the number of contacts that are shown on the screen is changed accordingly.

Step 1 Confirm that external-device relays are wired to the ENVIR ALARMS IN backplane pins. See the "DLP-A19 Install Alarm Wires on the Backplane" task on page 17-21 for more information.

Step 2 Double-click the AIC-I card to display it in card view.

Step 3 Click the **Provisioning > External Alarms** tabs.

Step 4 Modify any of the following fields for each external device wired to the ONS 15454 backplane. For definitions of these fields, see the "NTP-A258 Provision External Alarms and Controls on the Alarm Interface Controller–International" procedure on page 8-8.

- Enabled
- Alarm Type
- Severity
- Virtual Wire
- Raised When
- Description

Step 5 To provision additional devices, complete Step 4 for each additional device.

Step 6 Click **Apply**.

Step 7 Return to your originating procedure (NTP).

DLP-A209 Change External Controls Using the AIC-I Card

Purpose	This task changes external control settings on the AIC-I card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The procedure is the same if you are using the alarm expansion panel (AEP). In this case, the number of contacts that are shown on the screen is changed accordingly.

Step 1 Verify the external control relays to the ENVIR ALARMS OUT backplane pins. See the "DLP-A19 Install Alarm Wires on the Backplane" task on page 17-21 for more information.

Step 2 In node view, double-click the AIC-I card to display it in card view.

Step 3 On the External Controls subtab, modify any of the following fields for each external control wired to the ONS 15454 backplane. For definitions of these fields, see the "NTP-A258 Provision External Alarms and Controls on the Alarm Interface Controller–International" procedure on page 8-8.

- Enabled
- Trigger Type
- Control Type
- Description

Step 4 To provision additional controls, complete Step 3 for each additional device.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

DLP-A210 Change AIC-I Card Orderwire Settings

Purpose	This task changes orderwire settings on the AIC-I card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution When provisioning orderwire for ONS 15454s residing in a ring, do not provision a complete orderwire loop. For example, a four-node ring typically has east and west ports provisioned at all four nodes. However, to prevent orderwire loops, provision two orderwire ports (east and west) at all but one of the ring nodes.

Tip Before you begin, make a list of the ONS 15454 slots and ports that require orderwire communication.

Step 1 In node view, double-click the AIC-I card to display it in card view.

Step 2 Click the **Provisioning > Local Orderwire** tabs or the **Provisioning > Express Orderwire** tabs, depending on the orderwire path that you want to create. Provisioning steps are the same for both types of orderwire.

Step 3 If needed, adjust the transmit (Tx) and receive (Rx) decibels referred to one milliwatt (dBm) by moving the slider to the right or left for the headset type (four-wire or two-wire) that you will use. In general, you should not need to adjust the dBm.

Step 4 If you want to turn on the audible alert (buzzer) for the orderwire, check the **Buzzer On** check box.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

DLP-A212 Create a User Data Channel Circuit

Purpose	This task creates a user data channel (UDC) circuit on the ONS 15454. A UDC circuit allows you to create a dedicated data channel between nodes.
Tools/Equipment	OC-N cards must be installed.
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In network view, click the **Provisioning > Overhead Circuits** tabs.

Step 2 Click **Create**.

Step 3 In the Overhead Circuit Creation dialog box, complete the following fields in the Circuit Attributes area:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces).
- Type—Choose either **User Data-F1** or **User Data D-4-D-12** from the drop-down list. (User Data D-4-D-12 is not available if the ONS 15454 is provisioned for dense wavelength division multiplexing [DWDM].)

Step 4 Click **Next**.

Step 5 In the Circuit Source area, complete the following:

- Node—Choose the source node.
- Slot—Choose the source slot.
- Port—If displayed, choose the source port.

Step 6 Click **Next**.

Step 7 In the Circuit Destination area, complete the following:

- Node—Choose the destination node.
- Slot—Choose the destination slot.
- Port—If displayed, choose the destination port.

Step 8 Click **Finish**.

Step 9 Return to your originating procedure (NTP).

DLP-A214 Change the Service State for a Port

Purpose	This task changes the port service state.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note To provision E-Series Ethernet ports, see the "DLP-A220 Provision E-Series Ethernet Ports" task on page 19-13.

Step 1 In node view on the shelf graphic, double-click the card with the ports you want to put in or out of service. The card view appears.

Step 2 Click the **Provisioning > Line** tabs for all cards except the G-Series cards. For the G-Series cards, choose the **Provisioning > Port** tabs.

Step 3 In the Admin State column for the target port, choose one of the following from the drop-down list:

- IS—Puts the port in the In-Service and Normal (IS-NR) service state.
- OOS, DSBLD—Puts the port in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. In this service state, traffic is not passed on the port until the service state is changed to IS-NR; Out-of-Service and Management, Maintenance (OOS-MA,MT); or Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS).
- OOS, MT—Puts the port in the OOS-MA,MT service state. This service state does not interrupt traffic flow and loopbacks are allowed, but alarm reporting is suppressed. Raised fault conditions, whether or not their alarms are reported, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command. Use the OOS-MA,MT service state for testing or to suppress alarms temporarily. A port must be in the OOS-MA,MT service state before you can apply a loopback. Change to the IS-NR or OOS-AU,AINS service states when testing is complete.
- IS, AINS—Puts the port in the OOS-AU,AINS service state. In this service state, alarm reporting is suppressed, but traffic is carried and loopbacks are allowed. After the soak period passes, the port changes to IS-NR. Raised fault conditions, whether their alarms are reported or not, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command.

Note CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.

For more information about service states, refer to the "Administrative and Service States" appendix of the *Cisco ONS 15454 Reference Manual*.

Step 4 If the port is in loopback (OOS-MA,LPBK & MT) and you set the Admin State to IS, a confirmation window displays indicating that the loopback will be released and that the action could be service affecting. To continue, click **Yes**.

Step 5 If you set the Admin State to IS,AINS, set the soak period time in the AINS Soak field. This is the amount of time that the port will stay in the OOS-AU,AINS service state after a signal is continuously received. When the soak period elapses, the port changes to the IS-NR service state.

Step 6 Click **Apply**. The new port service state appears in the Service State column.

Step 7 As needed, repeat this task for each port.

Step 8 Return to your originating procedure (NTP).

DLP-A217 BLSR Exercise Ring Test

Purpose	This task tests the bidirectional line switched ring (BLSR) functionality without switching traffic. Ring exercise conditions (including the K-byte pass-through) are reported and cleared within 10 to 15 seconds.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

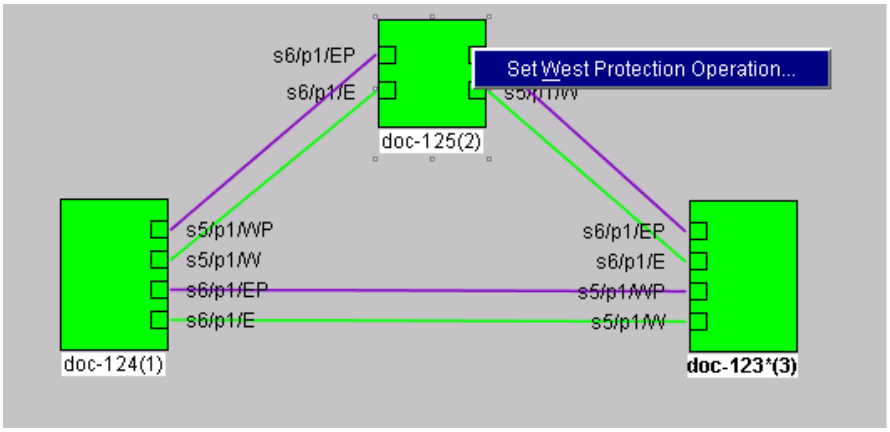
Step 3 Click the row of the BLSR you will exercise, then click **Edit**.

Step 4 Exercise the west port:

a. Right-click the west port of any BLSR node and choose **Set West Protection Operation**. Figure 19-2 shows an example. (To move a graphic icon, press **Ctrl** while you drag and drop it to a new location.)

Note For two fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. Right-click either working or protect ports.

Figure 19-2 Protection Operation on a Three-Node BLSR



b. In the Set West Protection Operation dialog box, choose **EXERCISE RING** from the drop-down list.

c. Click **OK**.

d. In the Confirm BLSR Operation dialog box, click **Yes**.

On the network view graphic, an E appears on the working BLSR channel where you invoked the protection switch. The E will appear for 10 to 15 seconds, then disappear.

Step 5 Exercise the east port:

a. Right-click the east port of any BLSR node and choose **Set East Protection Operation**.

Note For two fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. Right-click either working or protect ports.

b. In the Set East Protection Operation dialog box, choose **EXERCISE RING** from the drop-down list.

c. Click **OK**.

d. In the Confirm BLSR Operation dialog box, click **Yes**.

On the network view graphic, an E appears on the BLSR channel where you invoked the exercise. The E will appear for 10 to 15 seconds, then disappear.

Step 6 In the Cisco Transport Controller window, click the **History** tab.

If you do not see any BLSR exercise conditions, click the **Filter** button and verify that filtering is not turned on. Also, check that alarms and conditions are not suppressed for a node or BLSR drop cards. See the "NTP-A72 Suppress Alarms or Discontinue Alarm Suppression" procedure on page 8-7 for more information.

Step 7 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 8 From the File menu, choose **Close** to close the BLSR window.

Step 9 Return to your originating procedure (NTP).

DLP-A218 Provision Path Protection Selectors

Purpose	This task provisions path protection selectors during circuit creation or during a topology upgrade conversion.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 The Circuit Attributes page of the Circuit Creation wizard must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Provisioning path signal degrade (SD-P) or path signal fail (SF-P) thresholds in the Circuit Attributes page of the Circuit Creation wizard sets the values only for path protection-protected spans. The circuit source and destination use the node default values of 10E-4 for SD-P and 10E-6 for SF-P for unprotected circuits and for the source and drop of path protection circuits.

Step 1 In the path protection area of the Circuit Attributes page of the Circuit Creation wizard, set the path protection selectors:

- Provision working go and return on primary path—Check this box to route the working path on one fiber pair and the protect path on a separate fiber pair. This feature only applies to bidirectional path protection circuits.
- Revertive—Check this box if you want traffic to revert to the working path when the conditions that diverted it to the protect path are repaired. If you do not choose Revertive, traffic remains on the protect path after the switch.
- Reversion time—If Revertive is checked, click the Reversion time field and choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working path. Traffic can revert when conditions causing the switch are cleared.
- SF threshold—Set the path protection path-level signal failure bit error rate (BER) thresholds.
- SD threshold—Set the path protection path-level signal degrade BER thresholds.
- Switch on PDI-P—For synchronous transport signal (STS) circuits, check this box if you want traffic to switch when an STS payload defect indicator is received. Unavailable for Virtual Tributary (VT) circuits.

Step 2 Return to your originating procedure (NTP).

DLP-A219 Provision a VT Tunnel Route

Purpose	This task provisions the route for a manually routed VT tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 The Circuit Creation wizard Route Review and Edit page must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the Circuit Creation wizard on the Route Review and Edit page, click the source node icon if it is not already selected. Arrows indicate the available spans for routing the tunnel from the source node.

Step 2 Click the arrow of the span you want the VT tunnel to travel. The arrow turns yellow. In the Selected Span area, the From and To fields show the slot and port that will carry the tunnel. The source STS appears.

Step 3 If you want to change the source STS, change it in the Source STS field; otherwise, continue with the next step.

Step 4 Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

Step 5 Repeat Steps 3 and 4 until the tunnel is provisioned from the source to the destination node through all intermediary nodes.

Step 6 Return to your originating procedure (NTP).

DLP-A220 Provision E-Series Ethernet Ports

Purpose	This task enables the E100T-12, E100T-G, E1000-2, and E1000-2-G Ethernet ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security	Provisioning or higher

Step 1 In node view, double-click the Ethernet card that you want to provision.

Step 2 Click the **Provisioning** > **Port** tabs.

Step 3 For each Ethernet port, provision the following parameters:

- Port Name—If you want to label the port, type a port name.
- Mode—Choose the appropriate mode for the Ethernet port:
  - Valid choices for the E100T-12 and E100T-G cards are Auto, 10 Half, 10 Full, 100 Half, and 100 Full.

– Valid choices for the E1000-2 and E1000-2-G cards are 1000 Full and Auto.

Note Both 1000 Full and Auto mode set the E1000-2 port to the 1000 Mbps and Full duplex operating mode; however, flow control is disabled when 1000 Full is selected. Choosing Auto mode enables the E1000-2 card to autonegotiate flow control. Flow control is a mechanism that prevents network congestion by ensuring that transmitting devices do not overwhelm receiving devices with data. The E1000-2 port handshakes with the connected network device to determine if that device supports flow control.

- Enabled—Check this check box to activate the corresponding Ethernet port.
- Priority—Choose a queuing priority for the port. Options range from 0 (Low) to 7 (High). Priority queuing (IEEE 802.1Q) reduces the impact of network congestion by mapping Ethernet traffic to different priority levels. Refer to the priority queuing information in the *Cisco ONS 15454 Reference Manual*. This parameter does not apply to an E-Series card in port-mapped mode.
- Stp Enabled—Check this check box to enable the Spanning Tree Protocol (STP) on the port. This parameter does not apply to an E-Series card in port-mapped mode. Refer to the spanning tree information in the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

Step 4 Click **Apply**.

Step 5 Repeat Steps 1 through 4 for all other cards in the VLAN, or if the E-Series card is in port-mapped mode, repeat Steps 1 through 4 for the other card in the point-to-point circuit. Your Ethernet ports are provisioned and ready to be configured for VLAN membership.

Step 6 Return to your originating procedure (NTP).

DLP-A221 Provision E-Series Ethernet Ports for VLAN Membership

Purpose	This task provisions E-Series ports for VLAN membership. It does not apply to E-Series cards in port-mapped mode.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the E-Series card graphic to open the card.

Step 2 Click the **Provisioning** > **VLAN** tabs.

Step 3 To put a port in a VLAN:

a. Click the port and choose either **Tagged** or **Untag**.

b. If a port is a member of only one VLAN, choose **Untag** from the Port column in the VLAN's row. Choose **--** for all of the other VLAN rows in that Port column.

Note The VLAN with Untag selected can connect to the port, but other VLANs cannot access that port.

c. Choose **Tagged** at all VLAN rows that need to be trunked. Choose **Untag** at VLAN rows that do not need to be trunked, for example, the default VLAN.

Note Each Ethernet port must be attached to at least one untagged VLAN. A trunk port connects multiple VLANs to an external device, such as a switch, which also supports trunking. A trunk port must have tagging (IEEE 802.1Q) enabled for all of the VLANs that connect to that external device.

Step 4 After each port is in the appropriate VLAN, click **Apply**. Table 19-1 lists VLAN settings.

Table 19-1 VLAN Settings

Setting	Description
--	A port marked with this symbol does not belong to the VLAN.
Untag	The ONS 15454 tags ingress frames and strips tags from egress frames.
Tagged	The ONS 15454 processes ingress frames according to the VLAN ID; egress frames do not have their tags removed.

Note If Tagged is chosen, the attached external Ethernet devices must recognize IEEE 802.1Q VLANs.

Note Both ports on an E1000-2 or E1000-2-G card cannot be members of the same VLAN.

Step 5 Return to your originating procedure (NTP).

DLP-A222 Provision G-Series Ethernet Ports

Purpose	This task provisions G-Series Ethernet ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You can provision G-Series circuits before or after provisioning the card's ports. See the "NTP-A343 Create an Automatically Routed Optical Circuit" procedure on page 6-40 or the "NTP-A344 Create a Manually Routed Optical Circuit" procedure on page 6-45, as needed.

Step 1 In the node view, double-click the G-Series card graphic to open the card.

Step 2 Click the **Provisioning > Port** tabs.

Step 3 For each G-Series port, provision the following parameters:

- Port Name—If you want to label the port, type the port name.
- Admin State—Select the service state for the port. See the "DLP-A214 Change the Service State for a Port" task on page 19-9 for more information.

  Note CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.

- Auto Negotiation—Click this check box to enable autonegotiation on the port (default). If you do not want to enable autonegotiation control, uncheck the box.
- Flow Control—Click this check box to enable flow control on the port (default). If you do not want to enable flow control, uncheck the box. To set custom flow control watermarks, see the "DLP-A421 Provision G-Series and CE-1000-4 Flow Control Watermarks" task on page 21-6.
- Max Size—To permit the acceptance of jumbo size Ethernet frames, choose **Jumbo** (default). If you do not want to permit jumbo size Ethernet frames, choose **1548**.

  Note The maximum frame size of 1548 bytes enables the port to accept valid Ethernet frames that use protocols such as Inter-Switch Link (ISL). ISL adds 30 bytes of overhead and might cause the frame size to exceed the traditional 1518 byte maximum.

- Payload Type—Click in the Payload Type field and select a cyclic redundancy check (CRC) size to set the G-Series card's LEX encapsulation:
  - **LEX-FCS-16** is 16-bit (2 byte) CRC.
  - **LEX-FCS-32** is 32-bit (4 byte) CRC.

Step 4 Click **Apply**.

Step 5 Refresh the Ethernet statistics:

a. Click the **Performance > Statistics** tabs.

b. Click **Refresh**.

Note Reprovisioning an Ethernet port on the G-Series card does not reset the Ethernet statistics for that port.

Step 6 Return to your originating procedure (NTP).

DLP-A224 Soft-Reset a CE-100T-8 Card Using CTC

Purpose	This procedure soft-resets the CE-100T-8 card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note A soft reset is errorless in most cases. If there is a provisioning change during the soft reset, or if the firmware is replaced during the software upgrade process, the reset is not errorless.

Step 1 In node view, right-click the card to reveal a pop-up menu.

Step 2 Click **Soft-reset Card**.

Step 3 Click **Yes** in the "Are you sure you want to soft-reset this card?" dialog box.

Step 4 Return to your originating procedure (NTP).

DLP-A225 Enable Alarm Filtering

Purpose	This task enables alarm filtering for alarms, conditions, or event history in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 At the node, network, or card view, click the **Alarms** tab.

Step 2 Click the **Filter** tool at the lower-right side of the bottom toolbar.

Alarm filtering is enabled if the tool is selected and disabled if the tool is raised (not selected).

Alarm filtering will be enabled in the card, node, and network views of the Alarms tab at the node and for all other nodes in the network. If, for example, the Alarm Filter tool is enabled in the Alarms tab of the node view at one node, the Alarms tab in the network view and card view of that node will also show the tool enabled. All other nodes in the network will also have the tool enabled.

If you filter an alarm in card view, the alarm will still be displayed in node view. In this view, the card will display the color of the highest-level alarm. The alarm is also shown for the node in the network view.

Step 3 If you want alarm filtering enabled when you view conditions, repeat Steps 1 and 2 using the Conditions window.

Step 4 If you want alarm filtering enabled when you view alarm history, repeat Steps 1 and 2 using the History window.

Step 5 Return to your originating procedure (NTP).

DLP-A227 Disable Alarm Filtering

Purpose	This task turns off specialized alarm filtering in all network nodes so that all severities are reported in CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A225 Enable Alarm Filtering, page 19-17 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 At node, network, or card view, click the **Alarms** tab.

Step 2 Click the **Filter** tool at the lower-right side of the bottom toolbar.

Alarm filtering is enabled if the tool is indented and disabled if the tool is raised (not selected).

Step 3 If you want alarm filtering disabled when you view conditions, click the **Conditions** tab and click the Filter tool.

Step 4 If you want alarm filtering disabled when you view alarm history, click the **History** tab and click the Filter tool.

Step 5 Return to your originating procedure (NTP).

DLP-A229 View Circuits on a Span

Purpose	This task allows you to view circuits on an ONS 15454 span as well as unused STSs and VTs on a span.
Tools/Equipment	None
Prerequisite Procedures	Circuits must be created on the span. See Chapter 6, "Create Circuits and VT Tunnels" for circuit creation procedures. DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, choose **View > Go to Network View**. If you are already in network view, continue with Step 2.

Step 2 Right-click the green line containing the circuits that you want to view and choose one of the following:

- Circuits—To view BLSR, path protection, 1+1, virtual concatenated (VCAT), DWDM optical channel network connections (OCHNCs), or unprotected circuits on the span.
- PCA Circuits—To view circuits routed on a BLSR protected channel. (This option does not appear if the span you right-clicked is not a BLSR span.)

In the Circuits on Span dialog box, you can view the following information about the span. The information that appears depends on the circuit type.

- STS—Lists the STSs.
- VT—Lists the VTs.
- Path Protection—(Path protection span only) If checked, path protection circuits are on the span.
- Circuit—Displays the circuit name. If an STS or VT is not used by a circuit, "unused" appears in this column.
- Switch State—(Path protection span only) Displays the switch state of the circuit, that is, whether any span switches are active. For path protection spans, switch types include: CLEAR (no spans are switched), MANUAL (a manual switch is active), FORCE (a force switch is active), and LOCKOUT OF PROTECTION (a span lockout is active).

Note You can perform other procedures from the Circuits on Span dialog box. If the span is in a path protection configuration, you can switch the span traffic. See the "DLP-A197 Initiate a Path Protection Force Switch" task on page 18-67 for instructions. If you want to edit a circuit on the span, double-click the circuit. See the "DLP-A231 Edit a Circuit Name" task on page 19-20 or the "DLP-A233 Edit Path Protection Circuit Path Selectors" task on page 19-22 for instructions.

Step 3 Return to your originating procedure (NTP).

DLP-A230 Change a Circuit Service State

Purpose	This task changes the service state of a circuit.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Circuits** tab.

Step 3 Click the circuit with the service state that you want to change.

Note You cannot edit the circuit service state if the circuit is routed to nodes with a CTC software release older than Release 3.4. These circuits will automatically be in service (IS).

Step 4 From the Tools menu, choose **Circuits > Set Circuit State**.

Step 5 In the Set Circuit State dialog box, choose the administrative state from the Target Circuit Admin State drop-down list:

- IS—Puts the circuit cross-connects in the IS-NR service state.
- OOS,DSBLD—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
- IS,AINS—Puts the circuit cross-connects in the OOS-AU,AINS service state. When the connections receive a valid signal, the cross-connect service states automatically change to IS-NR.
- OOS,MT—Puts the circuit cross-connects in the OOS-MA,MT service state. This service state does not interrupt traffic flow and allows loopbacks to be performed on the circuit, but suppresses alarms and conditions. Use the OOS,MT administrative state for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; OOS; or IS,AINS when testing is complete.
- OOS,OOG—(VCAT circuits only) Puts the member in the Out-of-Service and Management, Out-of-Group (OOS-MA,OOG) service state. This administrative state is used to place a member circuit out of the group and to stop sending traffic. OOS-MA,OOG only applies to the cross-connects on an end node where VCAT resides. The cross-connects on intermediate nodes are in the OOS-MA,MT service state.

For additional information about circuit and VCAT service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 6 If you want to apply the service state to the circuit source and destination ports, check the **Apply to Drop Ports** check box.

Step 7 Click **Apply**.

Step 8 If the Apply to Ports Results dialog box appears, view the results and click **OK**.

CTC will not change the service state of the circuit source and destination port in certain circumstances. For example, if a port is in loopback (OOS-MA,LPBK & MT), CTC will not change the port to IS-NR. In another example, if the circuit size is smaller than the port, such as a VT1.5 circuit on an STS port, CTC will not change the port service state from IS-NR to OOS-MA,DSBLD. If CTC cannot change the port service state, you must change the port service state manually. For more information, see the "DLP-A214 Change the Service State for a Port" task on page 19-9.

Step 9 Return to your originating procedure (NTP).

DLP-A231 Edit a Circuit Name

Purpose	This task edits the name of a circuit or VCAT member.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Circuits** tab.

Step 3 Select the circuit you want to rename and click **Edit**.

Step 4 If you want to edit a VCAT circuit member name, complete the following steps in the Edit Circuit window. If not, continue with the Step 5.

- **a.** Click the **Members** tab.
- **b.** Click the VCAT member that you want to edit, then click **Edit Member**. The Edit Member window appears.

Step 5 In the General tab, click the **Name** field and edit or rename the circuit.

Note Names can be up to 48 alphanumeric and/or special characters. However, to ensure that a monitor circuit can be created on this circuit, do not make the name longer than 44 characters because monitor circuits will add "_MON" (four characters) to the circuit name.

Step 6 Click **Apply**.

Step 7 From the File menu, choose **Close**.

Step 8 If you changed the name of a VCAT circuit member, repeat Step 7 for the Edit Circuit window.

Step 9 In the Circuits window, verify that the circuit was correctly renamed.

Step 10 Return to your originating procedure (NTP).

DLP-A232 Change Active and Standby Span Color

Purpose	This task changes the color of active (working) and standby (protect) circuit spans shown on the detailed circuit map of the Edit Circuits window. By default, working spans are green and protect spans are purple.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu in any view, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **Circuit** tab.

Step 3 Complete one or more of the following steps, as required:

- To change the color of the active (working) span, go to Step 4.
- To change the color of the standby (protect) span, go to Step 5.
- To return active and standby spans to their default colors, go to Step 6.

Step 4 As needed, change the color of the active span:

- **a.** In the Span Colors area, click the colored square to the right of the word Active.
- **b.** In the Pick a Color dialog box, click the color for the active span, or click the **Reset** button if you want the active span to display the last applied (saved) color.

c. Click **OK** to close the Pick a Color dialog box. If you want to change the standby span color, go to Step 5. If not, click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box open.

Step 5 As needed, change the color of the standby span:

a. In the Span Colors area, click the colored square to the right of the word Standby.

b. In the Pick a Color dialog box, click the color for the standby span, or click the **Reset** button if you want the standby span to display the last applied (saved) color.

c. Click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box open.

Step 6 As needed, return the active and standby spans to their default colors:

a. Click **Reset to Defaults**.

b. Click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box open.

Step 7 Return to your originating procedure (NTP).

DLP-A233 Edit Path Protection Circuit Path Selectors

Purpose	This task changes the path protection SF and SD thresholds, the reversion and reversion time, and the path payload defect indication (PDI-P) settings for one or more path protection circuits.
Tools/Equipment	None
Prerequisite Procedures	NTP-A44 Provision Path Protection Nodes, page 5-20 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Circuits** tab.

Step 3 In the Circuits tab, click the path protection circuit(s) that you want to edit. To change the settings for multiple circuits, press the **Shift** key (to choose adjoining circuits) or the **Ctrl** key (to choose non adjoining circuits) and click each circuit that you want to change.

Step 4 From the Tools menu, choose **Circuits > Set Path Selector Attributes**.

Step 5 In the Path Selectors Attributes dialog box, edit the following path protection selectors, as needed:

- Revertive—If checked, traffic reverts to the working path when conditions that diverted it to the protect path are repaired. If the check box is not checked, traffic does not revert.
- Reversion Time (Min)—If Revertive is checked, this value sets the amount of time that will elapse before traffic reverts to the working path. The range is 0.5 to 12 minutes in 0.5 minute increments.
- In the STS Circuits Only area, set the following thresholds:
  - SF threshold—Sets the path protection signal failure BER threshold.

  - SD threshold—Sets the path protection signal degrade BER threshold.
  - Switch on PDI-P—When checked, traffic switches if an STS payload defect indication is received.
- In the VT Circuits Only area, set the following thresholds:
  - SF threshold—Sets the path protection signal failure BER threshold.
  - SD threshold—Sets the path protection signal degrade BER threshold.

Step 6 Click **OK** and verify that the changed values are correct in the Circuits window.

Step 7 Return to your originating procedure (NTP).

DLP-A241 Clear a BLSR Manual Ring Switch

Purpose	This task clears a Manual ring switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Choose the BLSR and click **Edit**.

Tip To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, click an icon on the Edit BLSR network graphic and while pressing **Ctrl**, drag the icon to a new location.

Step 4 Right-click the BLSR node channel (port) where the Manual ring switch was applied and choose **Set West Protection Operation** or **Set East Protection Operation**, as applicable.

Step 5 In the dialog box, choose **CLEAR** from the drop-down list. Click **OK**.

Step 6 Click **Yes** on the Confirm BLSR Operation dialog box. The letter “M” is removed from the channel (port) and the span turns green on the network view map.

Step 7 From the File menu, choose **Close**.

Step 8 Return to your originating procedure (NTP).

DLP-A242 Create a BLSR on a Single Node

Purpose	This task creates a BLSR on a single node. Use it to add a node to an existing BLSR or when you delete and then recreate a BLSR temporarily on one node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > BLSR** tabs.

Step 2 In the Suggestion dialog box, click **OK**.

Step 3 In the Create BLSR dialog box, enter the BLSR information:

- Ring Type—Enter the ring type (either 2 Fiber or 4 Fiber) of the BLSR.
- Ring Name—Enter the BLSR ring name. If the node is being added to a BLSR, use the BLSR ring name.
- Node ID—Enter the node ID. If the node is being added to a BLSR, use an ID that is not used by other BLSR nodes.
- Ring Reversion—Enter the ring reversion time of the existing BLSR.
- West Line—Enter the slot on the node that will connect to the existing BLSR via the node's west line (port).
- East Line—Enter the slot on the node that will connect to the existing BLSR via the node's east line (port).

If you are adding the node to a four-fiber BLSR, complete the following for the second set of fibers:

- Span Reversion—Enter the span reversion time of the existing BLSR.
- West Line—Enter the slot on the node that will connect to the existing BLSR via the node's west line.
- East Line—Enter the slot on the node that will connect to the existing BLSR via the node's east line.

Step 4 Click **OK**.

Note The BLSR is incomplete and alarms are present until the node is connected to other BLSR nodes.

Step 5 Return to your originating procedure (NTP).

DLP-A244 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)

Purpose	This task reinitializes the ONS 15454 using the CTC reinitialization tool on a Windows computer. Reinitialization uploads a new software package to the TCC2/TCC2P cards, clears the node database, and restores the factory default parameters.
Tools/Equipment	ONS 15454 SONET System Software CD, Version 9.1, 9.2, or 9.2.1 JRE 1.4.2 or JRE 5.0 (JRE 1.6 for Release 9.2 and later) must be installed on the computer to log into the node when the reinitialization is complete. The reinitialization tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 5.0 (JRE 1.6 for Release 9.2 and later).
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution Restoring a node to the factory configuration deletes all cross-connects on the node.

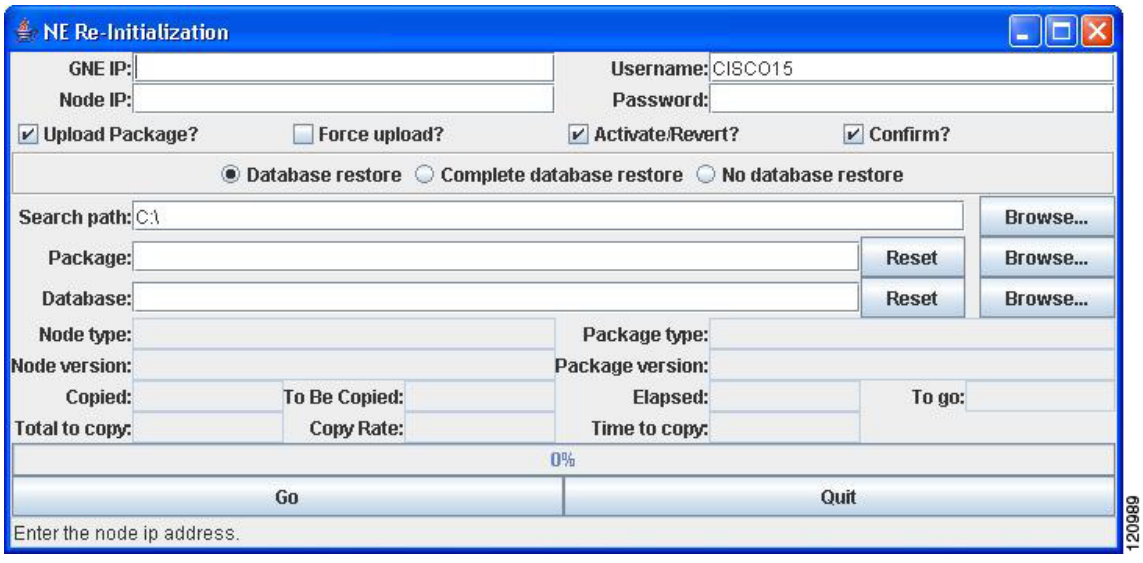
Step 1 Insert the system software CD into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.

Step 2 From the Windows Start menu, choose **Run.** In the Run dialog box, click **Browse** and navigate to the CISCO15454 folder on the software CD.

Step 3 In the Browse dialog box Files of Type field, choose **All Files**.

Step 4 Choose the RE-INIT.jar file and click **Open**. The NE Re-Initialization window appears (Figure 19-3).

Figure 19-3 Reinitialization Tool



Step 5 Complete the following fields:

- GNE IP—If the node you are reinitializing is accessed through another node configured as a gateway network element (GNE), enter the GNE IP address. If you have a direct connection to the node, leave this field blank.
- Node IP—Enter the node name or IP address of the node that you are reinitializing.
- User ID—Enter the user ID needed to access the node.
- Password—Enter the password for the user ID.
- Upload Package—Check this box to send the software package file to the node. If unchecked, the software stored on the node is not modified.
- Force Upload—Check this box to send the software package file to the node even if the node is running the same software version. If unchecked, reinitialization will not send the software package if the node is already running the same version.
- Activate/Revert—Check this box to activate the uploaded software (if the software is a later than the installed version) or revert to the uploaded software (if the software is earlier than the installed version) as soon as the software file is uploaded. If unchecked, the software is not activated or reverted after the upload, allowing you to initiate the functions later from the node view Maintenance > Software tabs.
- Confirm—Check this box if you want a warning message displayed before any operation is performed. If unchecked, reinitialization does not display a warning message.
- Database restore—Check this box if you want to send a new database to the node and to restore node provision values. (This is equivalent to the CTC database restore with the "Complete Database" check box unchecked.)
- Complete database restore—Check this option to send a new database to the node and to restore node provision and system values. (This is equivalent to the CTC database restore with the "Complete Database" check box checked.)
- No database restore—Check this box if you do not want the node database to be modified.
- Search Path—Enter the path to the CISCO15454 folder on the CD drive.

Step 6 Click **Go**.

Caution Before continuing with the next step, verify that the database to upload is correct. You cannot reverse the upload process after you click Yes.

Step 7 Review the information on the Confirm NE Re-Initialization dialog box, then click **Yes** to start the reinitialization.

The reinitialization begins. After the software is downloaded and activated, and the database is uploaded to the TCC2/TCC2P cards, "Complete" appears in the status bar and the TCC2/TCC2P cards will reboot. Wait a few minutes for the reboot to complete.

Step 8 After the reboot is complete, log into the node using the "DLP-A60 Log into CTC" task on page 17-60.

Step 9 Complete the "NTP-A25 Set Up Name, Date, Time, and Contact Information" procedure on page 4-5 and "NTP-A169 Set Up CTC Network Access" procedure on page 4-8.

Step 10 Return to your originating procedure (NTP).

DLP-A245 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)

Purpose	This task reinitializes the ONS 15454 using the CTC reinitialization tool on a UNIX computer. Reinitialization uploads a new software package to the TCC2/TCC2P cards, clears the node database, and restores the factory default parameters.
Tools/Equipment	ONS 15454 SONET System Software CD, Version 9.1, 9.2, or 9.2.1 JRE 1.4.2 or JRE 5.0 (JRE 1.6 for Release 9.2 and later) must be installed on the computer to log into the node when the reinitialization is complete. The reinitialization tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 5.0 (JRE 1.6 for Release 9.2 and later).
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution Restoring a node to the factory configuration deletes all cross-connects on the node.

Step 1 Insert the system software CD containing the reinit tool, software, and defaults database into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.

Step 2 To find the recovery tool file, go to the CISCO15454 directory on the CD (usually /cdrom/cdrom0/CISCO15454).

Step 3 If you are using a file explorer, double-click the **RE-INIT.jar** file. If you are working with a command line, run **java -jar RE-INIT.jar**. The NE Re-Initialization window appears (Figure 19-3).

Step 4 Complete the following fields:

- GNE IP—If the node you are reinitializing is accessed through another node configured as a GNE, enter the GNE IP address. If you have a direct connection to the node, leave this field blank.
- Node IP—Enter the node name or IP address of the node that you are reinitializing.
- User ID—Enter the user ID needed to access the node.
- Password—Enter the password for the user ID.
- Upload Package—Check this box to send the software package file to the node. If unchecked, the software stored on the node is not modified.
- Force Upload—Check this box to send the software package file to the node even if the node is running the same software version. If unchecked, reinitialization will not send the software package if the node is already running the same version.
- Activate/Revert—Check this box to activate the uploaded software (if the software is a later than the installed version) or revert to the uploaded software (if the software is earlier than the installed version) as soon as the software file is uploaded. If unchecked, the software is not activated or reverted after the upload, allowing you to initiate the functions later from the node view Maintenance > Software tabs.
- Confirm—Check this box if you want a warning message displayed before any operation is performed. If unchecked, reinitialization does not display a warning message.

- Database restore—Check this box if you want to send a new database to the node and to restore node provision values. (This is equivalent to the CTC database restore with the "Complete Database" check box unchecked.)
- Complete database restore—Check this option to send a new database to the node and to restore node provision and system values. (This is equivalent to the CTC database restore with the "Complete Database" check box checked.)
- No database restore—Check this box if you do not want the node database to be modified.
- Search Path—Enter the path to the CISCO15454 folder on the CD drive.

Step 5 Click **Go**.

Caution Before continuing with the next step, verify that the database to upload is correct. You cannot reverse the upload process after you click Yes.

Step 6 Review the information on the Confirm NE Re-Initialization dialog box, then click **Yes** to start the reinitialization.

The reinitialization begins. After the software is downloaded and activated and the database is uploaded to the TCC2/TCC2P cards, "Complete" appears in the status bar and the TCC2/TCC2P cards will reboot. Wait a few minutes for the reboot to complete.

Step 7 After the reboot is complete, log into the node using the "DLP-A60 Log into CTC" task on page 17-60.

Step 8 Complete the "NTP-A25 Set Up Name, Date, Time, and Contact Information" procedure on page 4-5 and the "NTP-A169 Set Up CTC Network Access" procedure on page 4-8.

Step 9 Return to your originating procedure (NTP).

DLP-A246 Provision E-Series Ethernet Card Mode

Purpose	This task provisions an E-Series Ethernet card for multicard EtherSwitch Group, single-card EtherSwitch, or port-mapped mode.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution You cannot change the mode while the Ethernet card is carrying circuits. If you want to change the card mode, delete any circuits that it carries first. See the "NTP-A278 Modify and Delete Overhead Circuits and Server Trails" procedure on page 7-5.

Step 1 In the network view, double-click the node containing the E-Series Ethernet card you want to provision, then double-click the Ethernet card.

Step 2 Click the **Provisioning > Card** tabs.

Step 3 In the Card Mode area, choose one of the following:

- For multicard EtherSwitch circuit groups, choose **Multicard EtherSwitch Group**.
- For single-card EtherSwitch circuits, choose **Single-card EtherSwitch**.
- For port-mapped circuits, choose **Port-mapped**.

Step 4 Click **Apply**.

Step 5 If you are using multicard EtherSwitch circuits, repeat Steps 2 through 4 for all other Ethernet cards in the node that will carry the multicard EtherSwitch circuits.

Step 6 Repeat Steps 1 through 5 for other nodes as necessary.

Step 7 Return to your originating procedure (NTP).

DLP-A247 Change an OC-N Card

Purpose	This task changes an OC-N card while maintaining existing provisioning, including data communications channels (DCCs), circuits, protection, timing, and rings. This task is intended to be used when you are replacing a card with a card of identical type and line rate; when a slot is preprovisioned and you want to change the optical speed of the card; or when you have backed out of an automatic span upgrade.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Physically removing an OC-N card can cause a loss of working traffic or a protection switch. See Chapter 12, "Upgrade Cards and Spans" for information on upgrading traffic to a higher speed.

Note You can change a multiport card to a card with a smaller number of ports only if the new card has the same line rate as the multiport card. (The MRC-12 card can be changed to either a single-port OC-12 card or a single-port OC-48 card.)

Step 1 If the card the active card in a 1+1 protection group, switch traffic away from the card:

a. Log into a node on the network. If you are already logged in, go to Step b.
b. Display the CTC node (login) view.
c. Click the **Maintenance > Protection** tabs.
d. Double-click the protection group that contains the reporting card.
e. Click the active card of the selected group.
f. Click **Switch** and **Yes** in the Confirmation dialog box.

Step 2 In CTC, right-click the card that you want to remove and choose **Change Card**.

Step 3 In the Change Card drop-down list, choose the desired card type and click **OK**. A mismatched equipment alarm (MEA) appears until you replace the card.

Step 4 Physically remove the card:

a. Disconnect any fiber connections to the front of the card.

b. Open the card latches/ejectors.

c. Use the latches/ejectors to pull the card forward and away from the shelf.

Step 5 Complete the "NTP-A16 Install Optical Cards and Connectors" procedure on page 2-8.

Step 6 Return to your originating procedure (NTP).

DLP-A249 Provision IP Settings

Purpose	This task provisions IP settings, which includes the IP address, IP address version, default router, Dynamic Host Configuration Protocol (DHCP) access, firewall access, and SOCKS proxy server settings for an ONS 15454 node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution All ONS 15454 IP addresses and network parameters should be reviewed by your network (or LAN) administrator.

Caution Verify that any IPv4 or IPv6 addresses assigned to the node are unique in the network. Duplicate IP addresses in the same network cause loss of visibility.

Step 1 In node view, click the **Provisioning > Network > General** tabs.

Step 2 Complete the following information in the fields listed:

- IP Address—Type the IP address assigned to the ONS 15454 node.

Note If TCC2P cards are installed, dual IP addressing via secure mode is available. When secure mode is off (sometimes called repeater mode), the IP address entered in the IP Address field applies to the backplane LAN port and the TCC2P TCP/IP (LAN) port. When secure mode is on, the IP Address field shows the address assigned to the TCC2P TCP/IP (LAN) port and the Superuser can enable or disable display of the backplane IP address. See the "DLP-A433 Enable Node Secure Mode" task on page 21-10 as needed. Refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual* for more information about secure mode.

- Net/Subnet Mask Length—Type the subnet mask length (decimal number representing the subnet mask length in bits) or click the arrows to adjust the subnet mask length. The subnet mask length is the same for all ONS 15454s in the same subnet.
- MAC Address—(Display only) Displays the ONS 15454 IEEE 802 MAC address.

Note In secure mode, the front and back TCP/IP (LAN) ports are assigned different MAC addresses, and the backplane information can be hidden or revealed by a Superuser.

- Default Router—If the ONS 15454 is connected to a LAN, enter the IP address of the default router. The default router forwards packets to network devices that the ONS 15454 cannot directly access. This field can be set to 0 or 0.0.0.0 if any of the following are true:
  - The ONS 15454 is not connected to a LAN.
  - The SOCKS proxy server is enabled and the ONS 15454 is provisioned as an end network element (ENE).
  - Open Shortest Path First (OSPF) is enabled on both the ONS 15454 and the LAN where the ONS 15454 is connected.
- LCD IP Setting—Choose one of the following:
  - **Allow Configuration**—Displays the node IP address on the LCD and allows users to change the IP settings using the LCD. This option enables the "DLP-A64 Set the IP Address, Default Router, and Network Mask Using the LCD" task on page 17-65.
  - **Display Only**—Displays the node IP address on the LCD but does not allow users to change the IP address using the LCD.
  - **Suppress Display**—Suppresses the node IP address display on the LCD.
- Suppress CTC IP Display—Check this check box if you want to prevent the node IPv4 address and IPv6 address (if enabled) from being displayed in CTC (IP Address field, information area) to users with Provisioning, Maintenance, or Retrieve security levels. If the IP address is not suppressed, both the IPv4 address and IPv6 addresses are shown in the IP Address field.

Note IP address suppression is not applied to users with a Superuser security level. However, in secure mode the backplane IP address visibility can be restricted to only a locally connected Superuser viewing the routing table. In this case, the backplane IP address is not revealed to any user at any other NE on the routing table or in autonomous messages (such as the TL1 REPT^DBCHG command, alarms, and PM reporting).

- IPv6 Configuration—Allows provisioning of IPv6 addresses. After you provision an IPv6 address, you can access the device using the IPv6 address. Configure these settings only if you want to enable IPv6 on the node. IPv6 cannot be configured using the LCD push buttons.
  - **Enable IPv6**—Select this check box to assign an IPv6 address to the node. The IPv6 Address, Prefix Length, and IPv6 Default Router fields are enabled only if this check box is selected. The check box is disabled by default.

Note If TCC2P cards are installed, dual IP addressing through secure mode is available for IPv4 only. If IPv6 is enabled on ONS 15454 with TCC2P in secure mode, IPv6 address support applies to the backplane LAN port only. There is no IPv6 address for the front TCC2P TCP/IP (LAN) port. However, when the TCC2P card is in normal mode (repeater mode), the IPv6 address support applies to both the backplane LAN port as well as the TCC2P TCP/IP (LAN) port.

Note IPv6 address can be enabled only when 'Enable SOCKS Proxy on Port' check box is enabled. For IPv6 connectivity, once the SOCKS Proxy is enabled, the ONS 15454 node can be configured as 'External Network Element (ENE)', 'Gateway Network Element (GNE)' or 'SOCKS proxy only' by enabling the suitable radio button.

Note By default, when IPv6 is enabled, the node processes both IPv4 and IPv6 packets on the LAN interface. If you want the node to process only IPv6 packets, you need to disable IPv4 on the node. For more information, see DLP-A512 Change Node Access and PM Clearing Privilege, page 22-5

- **IPv6 Address**—Enter the IPv6 address that you want to assign to the node. This IP address is the global unicast IPv6 address. This field is disabled if the **Enable IPv6** check box is not selected.
- **Prefix Length**—Enter the prefix length of the IPv6 address. This field is disabled if the **Enable IPv6** check box is not selected. The valid range for Prefix Length is 0 - 128.
- **IPv6 Default Router**—Enter the IPv6 address of the default router of the IPv6 NE. This field is disabled if the **Enable IPv6** check box is not selected. This field can be set to 0 or 0::0 or 0:0:0:0:0:0:0:0 if any of the following are true:

  The ONS 15454 is not connected to a LAN.

  The ONS 15454 is provisioned as an end network element (ENE).

Note The ONS 15454 uses NAT-PT internally to support native IPv6. NAT-PT uses the IPv4 address range 128.x.x.x for packet translation. Do not use this address range when you enable IPv6 feature.

Note You can provision IPv6 in secure or nonsecure mode. To enable secure mode, see "DLP-A433 Enable Node Secure Mode" task on page 21-10. To enable IPv6 in secure mode, see "DLP-A435 Modify Backplane Port IP Settings in Secure Mode" task on page 21-13.

- Forward DHCP Request To—Check this check box to enable DHCP. Also, enter the DHCP server IP address in the Request To field. Unchecked is the default. If you will enable any of the gateway settings to implement the ONS 15454 SOCKS proxy server features, leave this field blank.

Note If you enable DHCP, computers connected to an ONS 15454 node can obtain temporary IP addresses from an external DHCP server. The ONS 15454 only forwards DHCP requests; it does not act as a DHCP server.

- Gateway Settings—Provisions the ONS 15454 SOCKS proxy server features. (SOCKS is a standard proxy protocol for IP-based applications.) Do not change any of these options until you review the SOCKS proxy server scenario in the "Management Network Connectivity" chapter of the *Cisco ONS 15454 Reference Manual*. In SOCKS proxy server networks, the ONS 15454 is either an ENE, GNE, or proxy-only server. Provisioning must be consistent for each NE type.
- Enable SOCKS proxy server on port—If checked, the ONS 15454 serves as a proxy for connections between CTC clients and ONS 15454s that are DCC-connected to the proxy ONS 15454. The CTC client establishes connections to DCC-connected nodes through the proxy node. The CTC client does not require IP connectivity to the DCC-connected nodes, only to the proxy ONS 15454. If Enable SOCKS proxy server on port is off, the node does not proxy for any CTC clients. When this box is checked, you can set the node as an ENE or a GNE:
  - External Network Element (ENE)—Choose this option when the ONS 15454 is not connected to a LAN but has DCC connections to other ONS nodes. A CTC computer connected to the ENE through the TCC2/TCC2P craft port can manage nodes that have DCC connections to the ENE. However, the CTC computer does not have direct IP connectivity to these nodes or to any LAN/WAN that those nodes might be connected to.
  - Gateway Network Element (GNE)—Choose this option when the ONS 15454 is connected to a LAN and has DCC connections to other nodes. A CTC computer connected to the LAN can manage all nodes that have DCC connections to the GNE, but the CTC computer does not have direct IP connectivity to them. The GNE option isolates the LAN from the DCC network so that IP traffic originating from the DCC-connected nodes and any CTC computers connected to them is prevented from reaching the LAN.
  - SOCKS Proxy-Only—Choose this option when the ONS 15454 is connected to a LAN and the LAN is separated from the node by a firewall. The SOCKS Proxy Only is the same as the GNE option, except the SOCKS Proxy Only option does not isolate the DCC network from the LAN.

Note If a node is provisioned in secure mode, it is automatically provisioned as a GNE with SOCKS proxy enabled. However, this provisioning can be overridden, and the secure node can be changed to an ENE. In secure mode, SOCKS cannot be disabled. See the "DLP-A433 Enable Node Secure Mode" task on page 21-10 for provisioning instructions, including GNE or ENE status.

Step 3 Click **Apply**.

Step 4 Click **Yes** in the confirmation dialog box.

Both TCC2/TCC2P cards reboot, one at a time. During this time (approximately 5 minutes), the active and standby TCC2/TCC2P card LEDs go through the cycle shown in Table 19-2. Eventually, a "Lost node connection, switching to network view" message appears.

Table 19-2 LED Behavior During TCC2/TCC2P Reboot

Reboot Activity	Active TCC2/TCC2P LEDs	Standby TCC2/TCC2P LEDs
Standby TCC2/TCC2P card updated with new network information. Memory test (1 to 2 minutes). If an AIC-I card is installed, the AIC FAIL and alarm LEDs light up briefly when the AIC is updated. The standby TCC2/TCC2P becomes the active TCC2/TCC2P.	ACT/STBY: Flashing green.	1. ACT/STBY: Flashing yellow. 2. FAIL LED: Solid red. 3. All LEDs on except ACT/STBY. 4. CRIT turns off. 5. MAJ and MIN turn off. 6. REM, SYNC, and ACO turn off. 7. All LEDs (except A&B PWR) turn off (1 to 2 minutes). 8. ACT/STBY: Solid yellow. 9. Alarm LEDs: Flash once. 10. ACT/STBY: Solid green.
Memory test (1 to 2 minutes). TCC2/TCC2P updated with new network information. The active TCC2/TCC2P becomes the standby TCC2/TCC2P.	1. All LEDs: Turn off (1 to 2 minutes). CTC displays “Lost node connection, switching to network view” message. 2. FAIL LED: Solid red. 3. FAIL LED: Flashing red. 4. All LEDs on except ACT/STBY. 5. CRIT turns off. 6. MAJ and MIN turn off. 7. REM, SYNC, and ACO turn off; all LEDs are off. 8. ACT/STBY: Solid yellow. 9. ACT/STBY: Flashing yellow. 10. ACT/STBY: Solid yellow.	ACT/STBY: Solid green.

Step 5 Click **OK**. The network view appears. The node icon appears in gray, during which time you cannot access the node.

Step 6 Double-click the node icon when it becomes green.

Step 7 Return to your originating procedure (NTP).

DLP-A250 Set Up or Change Open Shortest Path First Protocol

Purpose	This task enables the OSPF routing protocol on the ONS 15454. Perform this task if you want to include the ONS 15454 in OSPF-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 You will need the OSPF Area ID, Hello and Dead intervals, and authentication key (if OSPF authentication is enabled) provisioned on the router to which the ONS 15454 is connected.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Network > OSPF** tabs.

Step 2 On the top left side of the OSPF pane, complete the following:

- DCC/GCC OSPF Area ID Table—In dotted decimal format, enter the number that identifies the ONS 15454s as a unique OSPF area ID. The Area ID can be any number between 000.000.000.000 and 255.255.255.255, but must be unique to the LAN OSPF area.
- SDCC Metric—This value is normally unchanged. It sets a cost for sending packets across the Section DCC, which is used by OSPF routers to calculate the shortest path. This value should always be higher than the LAN metric. The default SDCC metric is 100.
- LDCC Metric—Sets a cost for sending packets across the Line DCC. This value should always be lower than the SDCC metric. The default LDCC metric is 33. It is usually not changed.

Step 3 In the OSPF on LAN area, complete the following:

- OSPF active on LAN—When checked, enables the ONS 15454 OSPF topology to be advertised to OSPF routers on the LAN. Enable this field on ONS 15454s that directly connect to OSPF routers.
- LAN Port Area ID—Enter the OSPF area ID (dotted decimal format) for the router port where the ONS 15454 is connected. (This number is different from the DCC/generic communications channel [GCC] OSPF Area ID.)

Step 4 By default, OSPF is set to No Authentication. If the OSPF router requires authentication, complete the following steps. If not, continue with Step 5.

a. Click the **No Authentication** button.

b. In the Edit Authentication Key dialog box, complete the following:

- Type—Choose **Simple Password**.
- Enter Authentication Key—Enter the password.
- Confirm Authentication Key—Enter the same password to confirm it.

c. Click **OK**.

The authentication button label changes to Simple Password.

Step 5 Provision the OSPF priority and interval settings.

The OSPF priority and interval defaults are ones most commonly used by OSPF routers. Verify that these defaults match the ones used by the OSPF router where the ONS 15454 is connected.

- Router Priority—Selects the designated router for a subnet.

- Hello Interval (sec)—Sets the number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
- Dead Interval—Sets the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.
- Transit Delay (sec)—Indicates the service speed. One second is the default.
- Retransmit Interval (sec)—Sets the time that will elapse before a packet is resent. Five seconds is the default.
- LAN Metric—Sets a cost for sending packets across the LAN. This value should always be lower than the DCC metric. Ten is the default.

Step 6 In the OSPF Area Range Table area, create an area range table if one is needed:

Note Area range tables consolidate the information that is outside an OSPF area border. One ONS 15454 in the ONS 15454 OSPF area is connected to the OSPF router. An area range table on this node points the router to the other nodes that reside within the ONS 15454 OSPF area.

a. In the OSPF Area Range Table area, click **Create**.

b. In the Create Area Range dialog box, enter the following:

- Range Address—Enter the area IP address for the ONS 15454s that reside within the OSPF area. For example, if the ONS 15454 OSPF area includes nodes with IP addresses 10.10.20.100, 10.10.30.150, 10.10.40.200, and 10.10.50.250, the range address would be 10.10.0.0.
- Range Area ID—Enter the OSPF area ID for the ONS 15454s. This is either the ID in the DCC OSPF Area ID field or the ID in the Area ID for LAN Port field.
- Mask Length—Enter the subnet mask length. In the Range Address example, this is 16.
- Advertise—Check this box if you want to advertise the OSPF range table.

c. Click **OK**.

Step 7 All OSPF areas must be connected to area 0. If the ONS 15454 OSPF area is not physically connected to area 0, use the following steps to create a virtual link table that will provide the disconnected area with a logical path to area 0:

a. In the OSPF Virtual Link Table area, click **Create**.

b. In the Create Virtual Link dialog box, complete the following fields. OSPF settings must match OSPF settings for the ONS 15454 OSPF area:

- Neighbor—The router ID of the area 0 router.
- Transit Delay (sec)—The service speed. One second is the default.
- Hello Int (sec)—The number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
- Auth Type—If the router where the ONS 15454 is connected uses authentication, choose **Simple Password**. Otherwise, choose **No Authentication**.
- Retransmit Int (sec)—Sets the time that will elapse before a packet is resent. Five seconds is the default.
- Dead Int (sec)—Sets the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.

c. Click **OK**.

Step 8 After entering ONS 15454 OSPF area data, click **Apply**.

If you changed the Area ID, the TCC2/TCC2P cards reset, one at a time. The reset takes approximately 10 to 15 minutes. Table 19-2 on page 19-34 shows the LED behavior during the TCC2/TCC2P reset.

Step 9 Return to your originating procedure (NTP).

DLP-A251 Set Up or Change Routing Information Protocol

Purpose	This task enables Routing Information Protocol (RIP) on the ONS 15454. Perform this task if you want to include the ONS 15454 in RIP-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 You need to create a static route to the router adjacent to the ONS 15454 for the ONS 15454 to communicate its routing information to non-DCC-connected nodes.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** > **RIP** tabs.

Step 2 Check the **RIP Active** check box if you are activating RIP.

Step 3 Choose either RIP Version 1 or RIP Version 2 from the drop-down list, depending on which version is supported in your network.

Step 4 Set the RIP metric. The RIP metric can be set to a number between 1 and 15 and represents the number of hops.

Step 5 By default, RIP is set to No Authentication. If the router that the ONS 15454 is connected to requires authentication, complete the following steps. If not, continue with Step 6.

a. Click the **No Authentication** button.

b. In the Edit Authentication Key dialog box, complete the following:

- Type—Choose **Simple Password**.
- Enter Authentication Key—Enter the password.
- Confirm Authentication Key—Enter the same password to confirm it.

c. Click **OK**.

The authentication button label changes to Simple Password.

Step 6 If you want to complete an address summary, complete the following steps. If not, continue with Step 7. Complete the address summary only if the ONS 15454 is a gateway NE with multiple external ONS 15454 NEs attached with IP addresses in different subnets.

a. In the RIP Address Summary area, click **Create**.

b. In the Create Address Summary dialog box, complete the following:

- Summary Address—Enter the summary IP address.
- Mask Length—Enter the subnet mask length using the up and down arrows.

- Hops—Enter the number of hops. The smaller the number of hops, the higher the priority.

c. Click **OK.**

Step 7 Return to your originating procedure (NTP).

DLP-A255 Cross-Connect Card Side Switch Test

Purpose	This task verifies that the XCVT, XC10G, and XC-VXC-10G cards can effectively switch service (active to standby and standby to active).
Tools/Equipment	The test set specified by the acceptance test procedure, connected and configured as specified in the acceptance test procedure.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Always wait 60 seconds between cross-connect card (side) switches to allow the system to stabilize. This is applicable to all the types of side switches (soft reset or manual switch using CTC or TL1). This condition is also applicable to all the cross-connect types (XC-10G, XC-VXC-10G, XC-VT).

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 3 Click the **Conditions** tab. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 4 On the network map, double-click the node containing the cross-connect cards you are testing to open it in node view.

Step 5 Click the **Maintenance > Cross-Connect** tabs.

Step 6 In the Cross-Connect Cards area, make a note of the active and standby slots.

Step 7 On the shelf graphic, verify that the active cross-connect card has a green ACT LED and the standby cross-connect card has an amber SBY LED. If these conditions are not present, review the "DLP-A37 Install the XCVT, XC10G, or XC-VXC-10G Cards" task on page 17-40 or contact your next level of support.

Step 8 Click **Switch**.

Step 9 In the Confirm Switch dialog box, click **Yes**.

Note A cross-connect side-switch performed using XC-VXC-10G cards and TCC2/TCC2P cards is errorless.

Step 10 Verify that the active slot noted in Step 6 becomes the standby slot, and that the standby slot becomes the active slot. The switch should appear within 1 to 2 seconds.

Step 11 Verify that traffic on the test set connected to the node is still running. Some bit errors are normal, but traffic flow should not be interrupted. If a traffic interruption occurs, do not continue. Refer to your next level of support.

Step 12 Wait 60 seconds, then repeat Steps 7 through 9 to return the active/standby slots to their configuration at the start of the procedure.

Step 13 Verify that the cross-connect card appears as you noted in Step 6.

Step 14 Return to your originating procedure (NTP).

Note During a maintenance side switch or soft reset of an active XC10G card, the 1+1 protection group might display a protection switch. To disallow the protection switch from being displayed, the protection group should be locked at the node where XC switch or soft reset of an active XC switch is in progress.

DLP-A256 View Ethernet Statistics PM Parameters

Purpose	This task enables you to view current statistical PM counts on an Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the E-Series or G-Series Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Statistics** tabs.

Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names appear in the Param column. The current PM parameter values appear in the Port # columns. For PM parameter definitions, refer to the “Performance Monitoring” chapter in the *Cisco ONS 15454 Reference Manual*.

Note To refresh, reset, or clear PM counts, see the “NTP-A253 Change the PM Display” procedure on page 9-2.

Step 5 Return to your originating procedure (NTP).

DLP-A257 View Ethernet Utilization PM Parameters

Purpose	This task enables you to view line utilization PM counts on an Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the E-Series or G-Series Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Utilization** tabs.

Step 3 Click **Refresh**. Performance monitoring utilization values for each port on the card appear.

Step 4 View the Port # column to find the port you want to monitor.

Step 5 The transmit (Tx) and receive (Rx) bandwidth utilization values for the previous time intervals appear in the Prev-*n* columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 9-2.

Step 6 Return to your originating procedure (NTP).

DLP-A258 View Ethernet History PM Parameters

Purpose	This task enables you to view historical PM counts at selected time intervals on an Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the E-Series or G-Series Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **History** tabs.

Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Prev-*n* columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 9-2.

Step 5 Return to your originating procedure (NTP).

DLP-A259 Refresh Ethernet PM Counts at a Different Time Interval

Purpose	This task changes the window view to display specified PM counts in time intervals depending on the interval option selected.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Note For CE-Series and ML-Series cards, click **Performance** > **Ether Ports** or **Performance** > **POS Ports** tabs

Step 3 Click the **Utilization** tab or the **History** tab.

Step 4 From the Interval drop-down list, choose one of four options:

- **1 min**: This option appears the specified PM counts in one-minute time intervals.
- **15 min**: This option appears the specified PM counts in 15-minute time intervals.
- **1 hour**: This option appears the specified PM counts in one-hour time intervals.
- **1 day**: This option appears the specified PM counts in one-day (24 hours) time intervals.

Step 5 Click **Refresh**. The PM counts refresh with values based on the selected time interval.

Step 6 Return to your originating procedure (NTP).

DLP-A260 Set Auto-Refresh Interval for Displayed PM Counts

Purpose	This task changes the window auto-refresh intervals for updating the displayed PM counts.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 From the Auto-refresh drop-down list, choose one of six options:

- **None**: This option disables the auto-refresh feature.
- **15 Seconds**: This option sets the window auto-refresh to 15-second time intervals.
- **30 Seconds**: This option sets the window auto-refresh to 30-second time intervals.
- **1 Minute**: This option sets the window auto-refresh to 1-minute time intervals.
- **3 Minutes**: This option sets the window auto-refresh to 3-minute time intervals.
- **5 Minutes**: This option sets the window auto-refresh to 5-minute time intervals.

Step 4 Click **Refresh**. The PM counts for the newly selected auto-refresh time interval appear.

Depending on the selected auto-refresh interval, the displayed PM counts automatically update when each refresh interval completes. If the auto-refresh interval is set to None, the PM counts that appear are not updated unless you click Refresh.

Step 5 Return to your originating procedure (NTP).

DLP-A261 Refresh PM Counts for a Different Port

Purpose	This task changes the window view to display PM counts for another port on a multiport card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 In the Port drop-down list, choose a port.

Step 4 Click **Refresh**. The PM counts for the newly selected port appear.

Step 5 Return to your originating procedure (NTP).

DLP-A262 Filter the Display of Circuits

Purpose	This task filters the display of circuits in the Circuits window. You can filter the circuits in network, node, or card view based on circuit name, size, type, direction, and other attributes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate CTC view:

- To filter network circuits, from the View menu, choose **Go to Network View**.
- To filter circuits that originate, terminate, or pass through a specific node, from the View menu, choose **Go to Other Node**, then choose the node you want to search and click **OK**.
- To filter circuits that originate, terminate, or pass through a specific card, double-click the card on the shelf graphic in node view to open the card in card view.

Step 2 Click the **Circuits** tab.

Step 3 Set the attributes for filtering the circuit display:

a. Click the **Filter** button.

b. In the General tab of the Circuit Filter dialog box, set the following filter attributes, as necessary:

- Name—Enter a complete or partial circuit name to filter circuits based on the circuit name; otherwise leave the field blank.
- Direction—Choose one: **Any** (direction not used to filter circuits), **1-way** (display only one-way circuits), or **2-way** (display only two-way circuits).
- OCHNC Dir—(DWDM OCHNCs only) Choose one: **East to West** (displays only east-to-west circuits); **West to East** (displays only west-to-east circuits). For more information, refer to the *Cisco ONS 15454 DWDM Procedure Guide.*
- OCHNC Wlen—(DWDM OCHNCs only) Choose an OCHNC wavelength to filter the circuits. For example, choosing 1530.33 displays channels provisioned on the 1530.33 nm wavelength. For more information, refer to the *Cisco ONS 15454 DWDM Procedure Guide.*
- Status—Choose a circuit status to filter the circuits. For more information about circuit statuses, see Table 21-2 on page 21-3.
- State—Choose one: **OOS** (display only out-of-service circuits), **IS** (display only in-service circuits; OCHNCs have IS status only), or **OOS-PARTIAL** (display only circuits with cross-connects in mixed service states).
- Protection—Choose a protection type to filter the circuits. For more information about protection types, see Table 21-1 on page 21-3.

- Slot—Enter a slot number to filter circuits based on the source or destination slot; otherwise leave the field blank.
- Port—Enter a port number to filter circuits based on the source or destination port; otherwise leave the field blank.
- Type—Choose one: **Any** (type not used to filter circuits), **STS** (displays only STS circuits), **VT** (displays only VT circuits), **VT Tunnel** (displays only VT tunnels), **STS-V** (displays STS VCAT circuits), **VT-V** (displays VT VCAT circuits), **VT Aggregation Point** (displays only VT aggregation points), or **OCHNC** (displays only OCHNCs; refer to the *Cisco ONS 15454 DWDM Procedure Guide*).
- Size—Click the appropriate check boxes to filter circuits based on size: VT1.5, VT2, STS-1, STS3c, STS-6c, STS-9c, STS-12c, STS-18c, STS-24c, STS-36c, STS-48c, STS-192c, Multi-rate, Equipment non specific, 2.5 Gbps FEC, 2.5 Gbps No FEC, 10 Gbps FEC, or 10 Gbps No FEC.

  The check boxes shown depend on the Type field selection. If you chose Any, all sizes are available. If you chose VT, VT1.5 or VT2 are available. If you chose VT-V, only VT1.5 is available. If you chose STS, only STS sizes are available, and if you chose VT Tunnel or VT Aggregation Point, only STS-1 is available. If you chose OCHNC as the circuit type, Multi-rate, Equipment non specific, 2.5 Gbps FEC, 2.5 Gbps No FEC, 10 Gbps FEC, and 10 Gbps No FEC appear (DWDM only; refer to the *Cisco ONS 15454 DWDM Procedure Guide)*. If you chose STS-V, only STS-1, STS3c, and STS-12c are available.

Step 4 To set the filter for ring, node, link, and source and drop type, click the **Advanced** tab and complete the following substeps. If you do not want to make advanced filter selections, continue with Step 5.

a. If you made selections on the General tab, click **Yes** in the confirmation box to apply the settings.

b. In the Advanced tab of the Circuit Filter dialog box, set the following filter attributes as necessary:

- Ring—Choose the ring from the drop-down list.
- Node—Click the check boxes by each node in the network to filter circuits based on node.
- Link—Choose the desired link in the network.
- Source/Drop—Choose one of the following to filter circuits based on whether they have one or multiple sources and drops: **One Source and One Drop Only** or **Multiple Sources or Multiple Drops**.

Step 5 Click **OK**. Circuits matching the attributes in the Filter Circuits dialog box appear in the Circuits window.

Step 6 To turn filtering off, click the Filter icon in the lower right corner of the Circuits window. Click the icon again to turn filtering on, and click the **Filter** button to change the filter attributes.

Step 7 Return to your originating procedure (NTP).

DLP-A263 Edit Path Protection Dual-Ring Interconnect Circuit Hold-Off Timer

Purpose	This task changes the amount of time a path selector switch is delayed for circuits routed on a path protection dual-ring interconnect (DRI) topology. Setting a switch hold-off time (HOT) prevents unnecessary back and forth switching when a circuit is routed through multiple path protection selectors.
Tools/Equipment	None
Prerequisite Procedures	NTP-A44 Provision Path Protection Nodes, page 5-20 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Cisco recommends that you set the DRI port HOT value to zero and the circuit path selector HOT value to a number equal to or greater than zero.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Circuits** tab.

Step 3 Click the path protection circuit you want to edit, then click **Edit**.

Step 4 In the Edit Circuit window, click the **Path Protection Selectors** tab.

Step 5 Create a hold-off time for the circuit source and destination ports:

- **a.** In the Holder Off Timer area, double-click the cell of the circuit source port (top row), then type the new hold-off time. The range is 0 to 10,000 ms in increments of 100.
- **b.** In the Hold-Off Timer area, double-click the cell of the circuit destination port (bottom row), then type the hold-off time entered in Step a.

Step 6 Click **Apply**, then close the Edit Circuit window by choosing **Close** from the File menu.

Step 7 Return to your originating procedure (NTP).

DLP-A264 Provision a J1 Path Trace on Circuit Source and Destination Ports

Purpose	This task creates a path trace on STS circuit source ports and destination ports or a VCAT circuit member.
Tools/Equipment	ONS 15454 cards capable of transmitting and receiving path trace must be installed at the circuit source and destination ports. See Table 19-3 on page 19-46 for a list of cards.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This task assumes you are setting up path trace on a bidirectional circuit and setting up transmit strings at the circuit source and destination.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Circuits** tab.

Step 3 For the STS circuit you want to monitor, verify that the source and destination ports are on a card that can transmit and receive the path trace string. See Table 19-3 for a list of cards.

Table 19-3 Path-Trace-Capable ONS 15454 Cards

J1 Function	Cards
Transmit and Receive	CE-1000-4
	CE-100T-8
	DS1-14[1]
	DS1N-14
	DS1/E1-56
	DS3-12E
	DS3i-N-12
	DS3/EC1-48
	DS3N-12E
	DS3XM-6
	DS3XM-12
	G-Series
	ML-Series
Receive Only	EC1-12
	OC3 IR 4/STM1 SH 1310
	OC3 IR 4/STM1 SH 1310-8
	OC12/STM4-4
	OC48 IR/STM16 SH AS 1310
	OC48 LR/STM16 LH AS 1550
	OC192 SR/STM64 IO 1310
	OC192 LR/STM64 LH 1550
	OC192 IR/STM SH 1550
	ML-Series
	FC_MR-4

1. J1 path trace is not supported for DS-1s used in VT circuits.

Note For FC_MR-4 cards, the path trace string must be identical for all members of the VCAT circuit. You cannot mix path trace strings across members of a VCAT group. When retrieving the path trace string on the FC_MR-4 card view Maintenance > Path Trace subtab, only the member assigned a path trace string displays the path trace information.

Note If neither port is on a transmit/receive card, you will not be able to complete this procedure. If one port is on a transmit/receive card and the other is on a receive-only card, you can set up the transmit string at the transmit/receive port and the receive string at the receive-only port, but you will not be able to transmit in both directions.

Step 4 Choose the STS circuit you want to trace, then click **Edit**.

Step 5 If you chose a VCAT circuit, complete the following. If not, continue with Step 6.

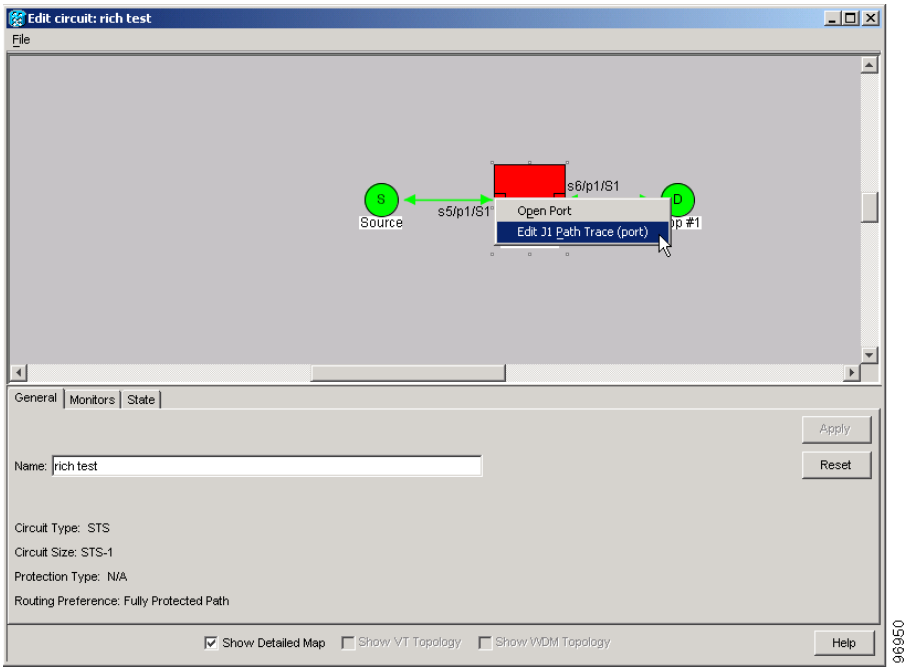
- **a.** In the Edit Circuit window, click the **Members** tab.
- **b.** Click **Edit Member** and continue with Step 6.

Step 6 In the Edit Circuit window, click the **Show Detailed Map** check box at the bottom of the window. A detailed map of the source and destination ports appears.

Step 7 Provision the circuit source transmit string:

- **a.** On the detailed circuit map, right-click the circuit source port (the square on the left or right of the source node icon) and choose **Edit J1 Path Trace (port)** from the shortcut menu. Figure 19-4 shows an example.

Figure 19-4 Selecting the Edit Path Trace Option



b. In the New Transmit String field, enter the circuit source transmit string. Enter a string that makes the source port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J1 transmits a string of null characters.

c. Click **Apply**, then click **Close**.

Step 8 Provision the circuit destination transmit string:

a. On the detailed circuit map, right-click the circuit destination port and choose **Edit Path Trace** from the shortcut menu (Figure 19-4).

b. In the New Transmit String field, enter the string that you want the circuit destination to transmit. Enter a string that makes the destination port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J1 transmits a string of null characters.

c. Click **Apply**.

Step 9 Provision the circuit destination expected string:

a. In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down list:

- Auto—The first string received from the source port is automatically provisioned as the current expected string. An alarm is raised when a string that differs from the baseline is received.
- Manual—The string entered in the Current Expected String field is the baseline. An alarm is raised when a string that differs from the Current Expected String is received.

b. If you set the Path Trace Mode field to Manual, enter the string that the circuit destination should receive from the circuit source in the New Expected String field. If you set Path Trace Mode to Auto, skip this step.

c. Click the **Disable AIS and RDI if TIM-P is detected** check box if you want to suppress the alarm indication signal (AIS) and remote defect indication (RDI) when the STS Path Trace Identifier Mismatch Path (TIM-P) alarm appears. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for descriptions of alarms and conditions.

d. (Check box visibility depends on card selection) Click the **Disable AIS on C2 Mis-Match** check box if you want to suppress the AIS when a C2 mismatch occurs.

e. Click **Apply**, then click **Close**.

Note It is not necessary to set the format (16 or 64 bytes) for the circuit destination expected string; the path trace process automatically determines the format.

Step 10 Provision the circuit source expected string:

a. In the Edit Circuit window (with Show Detailed Map chosen, see Figure 19-4 on page 19-47) right-click the circuit source port and choose **Edit Path Trace** from the shortcut menu.

b. In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down list:

- Auto—Uses the first string received from the port at the other path trace end as the baseline string. An alarm is raised when a string that differs from the baseline is received.
- Manual—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.

c. If you set the Path Trace Mode field to Manual, enter the string that the circuit source should receive from the circuit destination in the New Expected String field. If you set Path Trace Mode to Auto, skip this step.

d. Click the **Disable AIS and RDI if TIM-P is detected** check box if you want to suppress the AIS and RDI when the TIM-P alarm appears. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for descriptions of alarms and conditions.

e. (Check box visibility depends on card selection) Click the **Disable AIS on C2 Mis-Match** check box if you want to suppress the AIS when a C2 mismatch occurs.

f. Click **Apply**.

Note It is not necessary to set the format (16 or 64 bytes) for the circuit source expected string; the path trace process automatically determines the format.

Step 11 After you set up the path trace, the received string appears in the Received field on the path trace setup window. The following options are available:

- Click **Hex Mode** to display path trace in hexadecimal format. The button name changes to ASCII Mode. Click it to return the path trace to ASCII format.
- Click the **Reset** button to reread values from the port.
- Click **Default** to return to the path trace default settings (Path Trace Mode is set to Off and the New Transmit and New Expected Strings are null).

Caution Clicking Default will generate alarms if the port on the other end is provisioned with a different string.

The expect and receive strings are updated every few seconds if the Path Trace Mode field is set to Auto or Manual.

Step 12 Click **Close**.

The detailed circuit map indicates path trace with an M (manual path trace) or an A (automatic path trace) at the circuit source and destination ports.

Step 13 Return to your originating procedure (NTP).

DLP-A265 Change the Login Legal Disclaimer

Purpose	This task modifies the legal disclaimer statement shown in the CTC login dialog box so that it will display customer-specific information when users log into the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning > Security > Legal Disclaimer > HTML** tabs.

Step 2 The existing statement is a default, non-customer-specific disclaimer. If you want to edit this statement with specifics for your company, you can change the text. Use the following HTML commands to format the text, as needed:

- Begins boldface font
- Ends boldface font
- Aligns type in the center of the window
- Ends the center alignment
- <font=n, where n = point size> Changes the font to the new size
- Ends the font size command
- <p> Creates a line break
- <sub> Begins subscript
- </sub> Ends subscript
- <sup> Begins superscript
- </sup> Ends superscript
- <u> Starts underline
- </u> Ends underline

Step 3 If you want to preview your changed statement and formatting, click the **Preview** subtab.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A266 Change IP Settings

Purpose	This task changes the IPv4 address, subnet mask, default router, DHCP access, firewall Internet Inter-ORB Protocol (IIOP) listener port, LCD IP display, IPv6 Address, Prefix Length, IPv6 Default Router, and SOCKS proxy server settings.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 DLP-A249 Provision IP Settings, page 19-30
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution Changing the node IPv4 address, subnet mask, or IIOP listener port causes the TCC2/TCC2P cards to reboot. If Ethernet circuits using Spanning Tree Protocol (STP) originate or terminate on E-Series Ethernet cards installed in the node, circuit traffic will be lost for several minutes while the spanning trees reconverge. Other circuits are not affected by TCC2/TCC2P reboots.

Note If the node contains TCC2P cards and is in default (repeater) mode, the node IPv4 address and IPv6 address (if configured) refers to the TCC2P front-access TCP/IP (LAN) port as well as the backplane LAN port. If the node is in secure mode, this task will only change the front-access port IPv4 address. There is no IPv6 address for the front-access port. If the node is in secure mode and has been locked, the IP address cannot be changed unless the lock is removed by Cisco Technical Support.

Step 1 In node view, click the **Provisioning > Network > General** tabs.

Step 2 Change any of the following:

- IP Address
- Suppress CTC IP Display
- LCD IP Setting
- Default Router
- IPv6 Configuration
  - IPv6 Address
  - Prefix Length
  - IPv6 Default Router
- Forward DHCP Request To
- Net/Subnet Mask Length
- TCC CORBA (IIOP) Listener Port
- Gateway Settings

See the "DLP-A249 Provision IP Settings" task on page 19-30 for detailed field descriptions. For more information about secure mode, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15454 Reference Manual*.

Step 3 Click **Apply**.

If you changed a network field that will cause the node to reboot, such as the IP address, subnet mask, or TCC Common Object Request Broker Architecture (CORBA) Listener Port, the Change Network Configuration confirmation dialog box appears. If you changed a gateway setting, a confirmation appropriate to the gateway field appears. Change in IPv6 configuration such as IPv6 Address, Prefix Length and IPv6 Default Router does not cause the node to reboot.

Step 4 If a confirmation dialog box appears, click **Yes**.

If you changed an IP address, subnet mask length, or TCC CORBA (IIOP) Listener Port, both ONS 15454 TCC2/TCC2P cards reboot, one at a time. A TCC2/TCC2P card reboot causes a temporary loss of connectivity to the node, but traffic is unaffected. See Table 19-2 on page 19-34 for TCC2/TCC2P reboot behavior.

Step 5 Confirm that the changes appear on the **Provisioning > Network > General** tab. If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary.

Step 6 Return to your originating procedure (NTP).

DLP-A268 Apply a Custom Network View Background Map

Purpose	This task changes the background image or map of the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note You can replace the network view background image with any JPEG or GIF image that is accessible on a local or network drive. If you apply a custom background image, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

Step 1 From the Edit menu, choose **Preferences > Map** and uncheck the **Use Default Map** check box.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Right-click the network or domain map and choose **Set Background Image**.

Step 4 Click **Browse**. Navigate to the graphic file you want to use as a background.

Step 5 Select the file. Click **Open**.

Step 6 Click **Apply** and then click **OK**.

Step 7 If the ONS 15454 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat this step until all the ONS 15454 icons are visible.

Step 8 If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.

Step 9 If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15454 icons are displayed at the magnification you want.

Step 10 Return to your originating procedure (NTP).

DLP-A269 Enable Dialog Box Do-Not-Display Option

Purpose	This task ensures that a user-selected do-not-display dialog box preference is enabled for subsequent sessions or it disables the do-not-display option.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If any user who has rights to perform an operation (for example, creating a circuit) selects the "Do not show this dialog again" check box in a dialog box, the dialog box is not displayed for any other users who perform that operation on the network from the same computer unless the command is overridden using the following task. (The preference is stored on the computer, not in the node database.)

Step 1 From the Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **General** tab.

The Preferences Management area field lists all dialog boxes where "Do not show this dialog again" is enabled.

Step 3 Choose one of the following options, or uncheck the individual dialog boxes that you want to appear:

- **Don't Show Any**—Hides all do-not-display check boxes.
- **Show All**—Overrides do-not-display check box selections and displays all dialog boxes.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-A271 Change Security Policy on a Single Node

Purpose	This task changes the security policy for a single node, including idle user timeouts, user lockouts, password changes, and concurrent login policies.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning > Security > Policy** tabs.

Step 2 If you want to modify the idle user timeout period, click the hour (H) and minute (M) arrows in the Idle User Timeout area for the security level you want to provision: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. The idle period time range is 0 and 16 hours, and 0 and 59 minutes. The user is logged out after the idle user timeout period is reached.

Step 3 In the User Lockout area, you can modify the following:

- Failed Logins Allowed Before Lockout—The number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
- Manual Unlock by Superuser—If checked, allows a user with Superuser privileges to manually unlock a user who has been locked out from a node.
- Lockout Duration—Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).

Step 4 In the Password Change area, you can modify the following:

- Prevent Reusing Last [ ] Passwords—Choose a value between 1 and 10 to set the number of different passwords the user must create before they can reuse a password.
- New Password must Differ from the Old Password by [ ] Characters—Choose the number of characters that must differ between the old and new password. The default number is 1.
- Cannot Change New Password for [ ] days—If checked, prevents users from changing their password for the specified period. The range is 20 to 95 days.
- Require Password Change on First Login to New Account—If checked, requires users to change their password the first time they log into their account.

Step 5 To require users to change their password at periodic intervals, check the Enforce Password Aging check box in the Password Aging area. If checked, provision the following parameters:

- Aging Period—Sets the amount of time that must pass before the user must change their password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, and SUPERUSER. The range is 20 to 95 days.
- Warning—Sets the number of days the user will be warned to change his or her password for each security level. The range is 2 to 20 days.

Step 6 In the Other area, you can provision the following:

- Single Session Per User**—**If checked, limits users to one login session at one time.
- Prevent Superuser Disable—If checked, the super user is **NOT** disabled after the period of time specified in the Inactive Duration box expires.
- Disable Inactive User—If checked, disables users who do not log into the node for the period of time specified in the Inactive Duration box. The Inactive Duration range is 0 to 99 days.

Note If you advance the node date to a date beyond the threshold in the Inactive Duration box, the user account is disabled. User accounts are not reenabled if you revise the node date backwards, and the account has already been disabled.

Step 7 Click **Apply**.

Step 8 Return to your originating procedure (NTP).

DLP-A272 Change Security Policy on Multiple Nodes

Purpose	This task changes the security policy for multiple nodes including idle user timeouts, user lockouts, password change, and concurrent login policies.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > Security > Policy** tabs. A read-only table of nodes and their policies appears.

Step 3 Click a node on the table that you want to modify, then click **Change**.

Step 4 If you want to modify the idle user timeout period, click the hour (H) and minute (M) arrows in the Idle User Timeout area for the security level you want to provision: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. The idle period time range is 0 and 16 hours, and 0 and 59 minutes. The user is logged out after the idle user timeout period is reached.

Step 5 In the User Lockout area, you can modify the following:

- Failed Logins Allowed Before Lockout—The number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
- Manual Unlock by Superuser—Allows a user with Superuser privileges to manually unlock a user who has been locked out from a node.
- Lockout Duration—Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).

Step 6 In the Password Change area, you can modify the following:

- Prevent Reusing Last [ ] Passwords—Choose a value between 1 and 10 to set the number of different passwords the user must create before they can reuse a password.
- New Password must Differ from the Old Password by [ ] Characters—Choose the number of characters that must differ between the old and new password. The default number is 1.
- Cannot Change New Password for [ ] days—If checked, prevents users from changing their password for the specified period. The range is 20 to 95 days.
- Require Password Change on First Login to New Account—If checked, requires users to change their password the first time they log into their account.

Step 7 To require users to change their password at periodic intervals, check the Enforce Password Aging check box in the Password Aging area. If checked, provision the following parameters:

- Aging Period—Sets the amount of time that must pass before the user must change his or her password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, and SUPERUSER. The range is 20 to 95 days.
- Warning—Sets the number of days the user will be warned to change their password for each security level. The range is 2 to 20 days.

Step 8 In the Other area, you can provision the following:

- Single Session Per User**—**If checked, limits users to one login session at one time.
- Prevent Superuser Disable—If checked, the superuser is **NOT** disabled after the period of time specified in the Inactive Duration box expires.
- Disable Inactive User—If checked, disables users who do not log into the node for the period of time specified in the Inactive Duration box. The Inactive Duration range is 0 to 99 days.

Note If you advance the node date to a date beyond the threshold in the Inactive Duration box, the user account is disabled. User accounts are not reenabled if you revise the node date backwards, and the account has already been disabled.

Step 9 In the Select Applicable Nodes area, uncheck any nodes where you do not want to apply the changes.

Step 10 Click **OK**.

Step 11 In the Security Policy Change Results dialog box, confirm that the changes are correct, then click **OK**.

Step 12 Return to your originating procedure (NTP).

DLP-A273 Modify SNMP Trap Destinations

Purpose	This task modifies the Simple Network Management Protocol (SNMP) trap destinations on an ONS 15454 including community name, default User Datagram Protocol (UDP) port, SNMP trap version, and maximum traps per second.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **SNMP** tabs.

Step 2 Select a trap from the **Trap Destinations** area.

For a description of SNMP traps, refer to the "SNMP" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 3 Highlight the Destination row field entry under the Community column and change the entry to another valid community name.

Note The community name is a form of authentication and access control. The community name assigned to the ONS 15454 is case-sensitive and must match the community name of the network management system.

Note The default UDP port for SNMP is 162.

Step 4 Set the Trap Version field for either SNMPv1 or SNMPv2.

Refer to your NMS documentation to determine whether to use SNMP v1 or v2.

Step 5 If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If this box is not checked, SET requests are rejected.

Step 6 If you want to set up the SNMP proxy feature to allow network management, message reporting, and performance statistic retrieval across ONS firewalls, click the **Allow SNMP Proxy** check box located on the SNMP tab.

Step 7 If you want to enable using generic SNMP MIBs, click the **Use Generic MIBs** check box.

Step 8 Click **Apply**.

Step 9 SNMP settings are now modified. To view SNMP information for each node, highlight the node IP address in the Trap Destinations area of the Trap Destinations screen.

Step 10 Return to your originating procedure (NTP).

DLP-A293 Perform a Manual Span Upgrade on a Two-Fiber BLSR

Purpose	This task upgrades a two-fiber BLSR span to a higher OC-N rate. To downgrade a span, repeat this task but choose a lower-rate card in Step 5.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade Attenuators might be needed for some applications
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Caution Do not perform any other maintenance operations or add any circuits during a span upgrade.

Note All spans connecting the nodes in a BLSR must be upgraded before the bandwidth is available.

Note BLSR protection channel access (PCA) circuits, if present, will remain in their existing STSs. Therefore, they will be located on the working path of the upgraded span and will have full BLSR protection. To route PCA circuits on protection channels in the upgraded span, delete and recreate the circuits after the span upgrade. For example, if you upgrade an OC-48 span to an OC-192, PCA circuits on the protection STSs (STSs 25 to 48) in the OC-48 BLSR will remain in their existing STSs (STSs 25 to 48), which are working, protected STSs in the OC-192 BLSR. Deleting and recreating the OC-48 PCA circuits moves the circuits to STSs 96 to 192 in the OC-192 BLSR. To delete circuits, see the "NTP-A278 Modify and Delete Overhead Circuits and Server Trails" procedure on page 7-5. To create circuits, see Chapter 6, "Create Circuits and VT Tunnels."

Step 1 Apply a Force switch to both span endpoints (nodes) on the span that you will upgrade first. See the "DLP-A303 Initiate a BLSR Force Ring Switch" task on page 20-3.

Step 2 Remove the fiber from both endpoints and ensure that traffic is still running.

Step 3 Remove the OC-N cards from both endpoints.

Step 4 From both endpoints, in node view right-click each OC-N slot and choose **Change Card**.

Step 5 In the Change Card dialog box, choose the new OC-N card type.

Step 6 Click **OK**.

Step 7 Complete the "NTP-A16 Install Optical Cards and Connectors" procedure on page 2-8 to install the new OC-N cards in both endpoints.

Step 8 Verify that the transmit and receive signals fall within the acceptable range. See Table 2-5 on page 2-20 for OC-N card transmit and receive levels. If the receive level falls outside the acceptable range for that card, attenuate accordingly.

Step 9 Complete the "DLP-A44 Install Fiber-Optic Cables for BLSR Configurations" task on page 17-46 to attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.

Step 10 When cards in both endpoint nodes have been successfully upgraded and all the facility alarms (loss of signal [LOS], SD, and SF) are cleared, remove the forced switch from both endpoints on the upgraded span. See the "DLP-A194 Clear a BLSR Force Ring Switch" task on page 18-65.

Step 11 Perform an exercise ring test to check the BLSR ring functionality without switching traffic. See the "DLP-A217 BLSR Exercise Ring Test" task on page 19-10.

Step 12 Repeat this task for each span in the BLSR. When you are done with each span, the upgrade is complete.

Step 13 Return to your originating procedure (NTP).

DLP-A294 Perform a Manual Span Upgrade on a Four-Fiber BLSR

Purpose	This task upgrades a four-fiber BLSR span to a higher OC-N rate. Repeat the task to upgrade each span to the higher OC-N rate. To downgrade a span, repeat this task but choose a lower-rate card in Step 5.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade Attenuators might be needed for some applications
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Caution Do not perform any other maintenance operations or add any circuits during a span upgrade.

Note All spans connecting the nodes in a BLSR must be upgraded before the bandwidth is available.

Note BLSR PCA circuits, if present, will remain in their existing STSs. Therefore, they will be located on the working path of the upgraded span and will have full BLSR protection. To route PCA circuits on protection channels in the upgraded span, delete and recreate the circuits after the span upgrade. For example, if you upgrade an OC-48 span to an OC-192, PCA circuits on the protection STSs (STSs 25 to 48) in the OC-48 BLSR will remain in their existing STSs (STSs 25 to 48), which are working, protected STSs in the OC-192 BLSR. Deleting and recreating the OC-48 PCA circuits moves the circuits to STSs

96 to 192 in the OC-192 BLSR. To delete circuits, see the "NTP-A278 Modify and Delete Overhead Circuits and Server Trails" procedure on page 7-5. To create circuits, see Chapter 6, "Create Circuits and VT Tunnels."

Step 1 Apply a Force switch to both span endpoints (nodes) on the span that you will upgrade first. See the "DLP-A303 Initiate a BLSR Force Ring Switch" task on page 20-3.

Step 2 Remove the fiber from both working and protect cards at both span endpoints (nodes) and ensure that traffic is still running.

Step 3 Remove the OC-N cards from both end points.

Step 4 For both ends of the span endpoints, in node view right-click each OC-N slot and choose **Change Card**.

Step 5 In the Change Card dialog box, choose the new OC-N card type.

Step 6 Click **OK**.

Step 7 Complete the "NTP-A16 Install Optical Cards and Connectors" procedure on page 2-8 to install the new OC-N cards in both endpoints.

Step 8 Verify that the transmit signal falls within the acceptable range. See Table 2-5 on page 2-20 for OC-N card transmit and receive levels.

Step 9 Complete the "DLP-A44 Install Fiber-Optic Cables for BLSR Configurations" task on page 17-46 to attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.

Step 10 When cards in both endpoint nodes have been successfully upgraded and all the facility alarms (LOS, SD, and SF) are cleared, remove the forced switch from both endpoints (nodes) on the upgraded span. See "DLP-A194 Clear a BLSR Force Ring Switch" task on page 18-65.

Step 11 Perform an exercise ring test to check the BLSR ring functionality without switching traffic. See the "DLP-A217 BLSR Exercise Ring Test" task on page 19-10.

Step 12 Repeat these steps for each span in the BLSR. When all spans in the BLSR have been upgraded, the ring is upgraded.

Step 13 Return to your originating procedure (NTP).

DLP-A295 Perform a Manual Span Upgrade on a Path Protection Configuration

Purpose	This task upgrades path protection spans to a higher OC-N speed. Repeat the task for each span to upgrade the entire ring to the higher OC-N rate. To downgrade a span, repeat this task but choose a lower-rate card in Step 5.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Caution Do not perform any other maintenance operations or add any circuits during a span upgrade.

Step 1 Complete the "DLP-A197 Initiate a Path Protection Force Switch" task on page 18-67 to apply a Force switch on the span that you will upgrade.

Step 2 Remove the fiber from both endpoint nodes in the span and ensure that traffic is still running.

Step 3 Remove the OC-N cards from both span endpoints.

Step 4 For both ends of the span, in node view right-click each OC-N slot and choose **Change Card**.

Step 5 In the Change Card dialog box, choose the new OC-N card type.

Step 6 Click **OK**.

Step 7 Complete the "NTP-A16 Install Optical Cards and Connectors" procedure on page 2-8 to install the new OC-N cards in both endpoints.

Step 8 Verify that the transmit signal falls within the acceptable range. See Table 2-5 on page 2-20 for OC-N card transmit and receive levels.

Step 9 Complete the "DLP-A43 Install Fiber-Optic Cables for Path Protection Configurations" task on page 17-43 to attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.

Step 10 Complete the "DLP-A198 Clear a Path Protection Force Switch" task on page 18-68 when cards in both endpoint nodes have been successfully upgraded and all the facility alarms (LOS, SD, and SF) are cleared.

Step 11 Return to your originating procedure (NTP).

DLP-A296 Perform a Manual Span Upgrade on a 1+1 Protection Group

Purpose	This task upgrades a linear span to a higher OC-N rate. To downgrade a span, follow this task but choose a lower-rate card in Step 6.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Caution Do not perform any other maintenance operations or add any circuits during a span upgrade.

Step 1 Initiate a Force switch on the ports you will upgrade, beginning with the protect port:

a. In node view, click the **Maintenance > Protection** tabs.

b. Choose the protection group from the Protection Groups area. In the Selected Group area, the working and protect spans appear.

c. In the Selected Group area, click the protect OC-N port.

d. In Switch Commands, choose **Force**.

e. Click **Yes** in the confirmation dialog box.

FORCE-SWITCH-TO-WORKING appears next to the forced span.

Step 2 If you are upgrading a multiport card, repeat Step 1 for each port.

Step 3 Remove the fiber from both ends of the span and ensure that traffic is still running.

Step 4 Remove the OC-N cards from both span endpoints.

Step 5 At both ends of the span, in node view, right-click the OC-N slot and choose **Change Card**.

Step 6 In the Change Card dialog box, choose the new OC-N card type.

Step 7 Click **OK**.

Step 8 Complete the "NTP-A16 Install Optical Cards and Connectors" procedure on page 2-8 to install the new OC-N cards in both endpoints.

Step 9 Verify that the transmit signal falls within the acceptable range. See Table 2-5 on page 2-20 for OC-N card transmit and receive levels.

Step 10 Complete the "DLP-A428 Install Fiber-Optic Cables in a 1+1 Configuration" task on page 21-8 to attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.

Step 11 When cards on each end of the span have been successfully upgraded and all the facility alarms (LOS, SD, and SF) are cleared, remove the Force switch:

a. In node view, click the **Maintenance > Protection** tabs.

b. In the Protection Groups area, click the protection group that contains the card/port you want to clear.

c. In the Selected Group area, click the card you want to clear.

d. In Switch Commands, choose **Clear**.

e. Click **Yes** in the confirmation dialog box.

Step 12 Repeat this task for any other spans in the 1+1 linear configuration.

Step 13 Return to your originating procedure (NTP).

DLP-A297 Perform a Manual Span Upgrade on an Unprotected Span

Purpose	This task manually upgrades unprotected spans to a higher OC-N rate.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Caution Upgrading unprotected spans will cause all traffic running on those spans to be lost.

Caution Do not perform any other maintenance operations or add any circuits during a span upgrade.

Caution Removing the fiber will cause all traffic on the unprotected span to be lost.

Step 1 Remove the fiber from both endpoint nodes in the span.

Step 2 Remove the OC-N cards from both span endpoints.

Step 3 For both ends of the span, in node view, right-click each OC-N slot and choose **Change Card**.

Step 4 In the Change Card dialog box, choose the new OC-N type.

Step 5 Click **OK**.

Step 6 When you have finished Steps 2 through 5 for both nodes, install the new OC-N cards in both endpoints and attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.

Step 7 Return to your originating procedure (NTP).

DLP-A298 Check the Network for Alarms and Conditions

Purpose	This task verifies that no alarms or conditions exist on the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From the View menu, choose **Go to Network View**. Verify that all affected spans on the network map are green.

Step 2 Verify that the affected spans do not have active switches on the network map. Span ring switches are represented by the letters “L” for lockout ring, “F” for Force ring, “M” for Manual ring, and “E” for Exercise ring.

Step 3 A second verification method can be performed from the Conditions tab. Click **Retrieve Conditions** and verify that no switches are active. Make sure the Filter button is not selected.

Step 4 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the “DLP-A227 Disable Alarm Filtering” task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 5 Return to your originating procedure (NTP).

DLP-A299 Initiate a BLSR Span Lockout

Purpose	This task allows you to perform a BLSR span lockout, which prevents traffic from switching to the locked out span.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Traffic is not protected during a span lockout.

Step 1 Click the **Provisioning > BLSR** tabs.

Step 2 Choose the BLSR and click **Edit**.

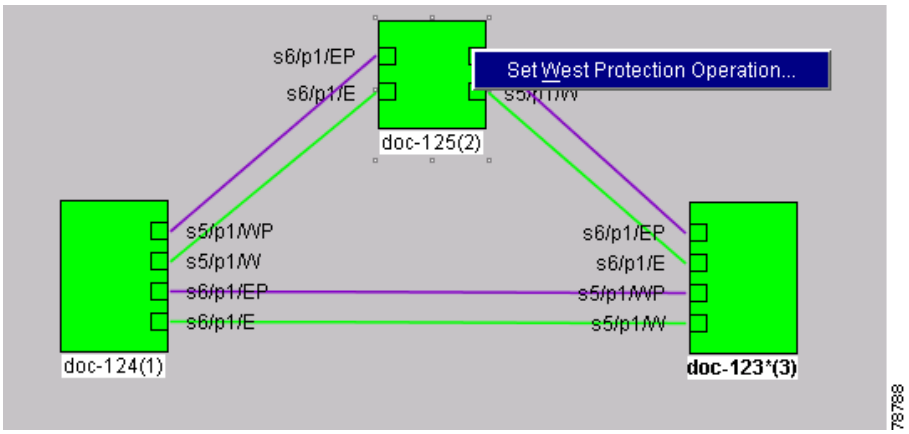
Tip To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, you can drag and drop icons on the Edit BLSR network graphic.

Step 3 To lock out a west span:

a. Right-click any BLSR node west channel (port) and choose **Set West Protection Operation**. Figure 19-5 shows an example.

Note For two-fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. You can right-click either working port.

Figure 19-5 Protection Operation on a Three-Node BLSR



b. In the Set West Protection Operation dialog box, choose **LOCKOUT PROTECT SPAN** from the drop-down list. Click **OK**.

c. In the Confirm BLSR Operation dialog box, click **Yes**. An "L" appears on the selected channel (port) where you created the lock out.

Lockouts generate LKOUTPR-S and FE-LOCKOUTOFPR-SPAN conditions.

Step 4 To lock out an east span:

a. Right-click the node's east channel (port) and choose **Set East Protection Operation**.

b. In the Set East Protection Operation dialog box, choose **LOCKOUT PROTECT SPAN** from the drop-down list. Click **OK**.

c. In the Confirm BLSR Operation dialog box, click **Yes**. An "L" indicating the lockout appears on the selected channel (port) where you invoked the protection switch.

Lockouts generate LKOUTPR-S and FE-LOCKOUTOFPR-SPAN conditions.

Step 5 From the File menu, choose **Close**.

Step 6 Return to your originating procedure (NTP).

CHAPTER 20

DLPs A300 to A399

Note The terms “Unidirectional Path Switched Ring” and “UPSR” may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as “Path Protected Mesh Network” and “PPMN,” refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

DLP-A300 Clear a BLSR Span Lockout

Purpose	This task clears a bidirectional line switched ring (BLSR) span lockout.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Choose the BLSR and click **Edit**.

Tip To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, you can drag and drop icons on the Edit BLSR network graphic.

Step 4 Right-click the BLSR node channel (port) where the lockout will be cleared and choose **Set West Protection Operation** or **Set East Protection Operation**.

Step 5 In the dialog box, choose **CLEAR** from the drop-down list. Click **OK**.

Step 6 In the Confirm BLSR Operation dialog box, click **Yes**. The “L” that indicated the lockout disappears from the network view map.

Step 7 From the File menu, choose **Close**.

Step 8 Return to your originating procedure (NTP).

DLP-A301 Initiate a BLSR Manual Ring Switch

Purpose	This task performs a BLSR Manual ring switch. A Manual ring switch will switch traffic off a span if there is no higher priority switch (Force or lockout) and no signal degrade (SD) or signal failure (SF) conditions.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Choose the BLSR and click **Edit**.

Tip To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, click an icon and drag and drop it in a new location.

Step 4 Right-click any BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).

Note The squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. Right-click either working port.

Step 5 In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **MANUAL RING** from the drop-down list. Click **OK**.

Step 6 Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Step 7 Verify that the channel (port) displays the letter “M” for Manual ring. Also verify that the span lines between the nodes where the Manual switch was invoked turn purple, and that the span lines between all other nodes turn green on the network view map. This confirms the Manual switch.

Step 8 From the File menu, choose **Close**.

Step 9 Return to your originating procedure (NTP).

DLP-A303 Initiate a BLSR Force Ring Switch

Purpose	Use this task to perform a BLSR Force switch on a BLSR port. A Force ring switch will switch traffic off a span if there is no signal degrade (SD), signal failure (SF), or lockout switch present on the span.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution The Force Switch Away command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution Traffic is not protected during a Force protection switch.

Step 1 From the View menu, choose **Go to Network Vie**w.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click **Edit**.

Step 4 To apply a Force switch to the west line:

a. Right-click the west BLSR port where you want to switch the BLSR traffic and choose **Set West Protection Operation**.

Note If node icons overlap, drag and drop the icons to a new location. You can also return to network view and change the positions of the network node icons, because BLSR node icons are based on the network view node icon positions.

Note For two-fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. Right-click either working port.

b. In the Set West Protection Operation dialog box, choose **FORCE RING** from the drop-down list. Click **OK**.

c. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network graphic, an F appears on the working BLSR channel where you invoked the protection switch. The span lines change color to reflect the forced traffic. Green span lines indicate the new BLSR path, and the lines between the protection switch are purple.

Performing a Force switch generates several conditions including FORCED-REQ-RING and WKSWPR.

Step 5 To apply a Force switch to the east line:

a. Right-click the east BLSR port and choose **Set East Protection Operation**.

Note If node icons overlap, drag and drop the icons to a new location or return to network view and change the positions of the network node icons, since BLSR node icons are based on the network view node icon positions.

Note For two-fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. Right-click either working port.

b. In the Set East Protection Operation dialog box, choose **FORCE RING** from the drop-down list. Click **OK**.

c. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network graphic, an F appears on the working BLSR channel where you invoked the protection switch. The span lines change color to reflect the forced traffic. Green span lines indicate the new BLSR path, and the lines between the protection switch are purple.

Performing a Force switch generates several conditions including FORCED-REQ-RING and WKSWPR.

Step 6 From the File menu, choose **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-A309 View the Ethernet MAC Address Table

Purpose	This task displays the Ethernet MAC address table for any node with one or more E-Series Ethernet cards installed.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, click the **Maintenance > Ether Bridge > MAC Table** tabs.

Step 2 Select the appropriate E-Series Ethernet card in the Layer 2 Domain field.

Step 3 Click **Retrieve**.

The MAC address table information appears.

Step 4 Return to your originating procedure (NTP).

DLP-A310 View Ethernet Trunk Utilization

Purpose	This task displays the Ethernet Trunk bandwidth usage on any node with one or more E-Series Ethernet cards installed.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, click the **Maintenance > Ether Bridge > Trunk Utilization** tabs.

Step 2 Select the desired time interval in the Interval field.

Step 3 Click **Refresh**.

The trunk utilization information for the current and previous time intervals appears.

Step 4 Return to your originating procedure (NTP).

DLP-A311 Provision a Half Circuit Source and Destination on a BLSR or 1+1 Configuration

Purpose	This task provisions a half circuit source and destination for BLSR and 1+1 configurations. A half circuit allows you to provision a partial path (one end of a circuit), for example, if you want to provision a circuit with the intent that the path will be completed at a later time or at a different location.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note After you have selected the circuit properties in the Circuit Source dialog box according to the specific circuit creation procedure, you are ready to provision the circuit source and destination.

Step 1 From the Node drop-down list, choose the node that will contain the half circuit.

Step 2 From the Slot drop-down list, choose the slot containing the card where the circuit will originate.

Step 3 From the Port drop-down list, choose the port where the circuit will originate. This field is not available if a DS-1 card is chosen in Step 2.

Step 4 If the circuit is a DS-1 circuit and you choose a DS-1 card as the source, choose the DS-1 where the traffic will originate from the DS1 drop-down list.

Step 5 Click **Next**.

Step 6 From the Node drop-down list, select the node that you chose in Step 1.

Step 7 From the Slot drop-down list, choose the OC-N card that you will use to map the DS-1 to a VT1.5 for OC-N transport or to map the DS-3 or OC-N synchronous transport signal (STS) circuit to an STS.

Step 8 Choose the destination STS or Virtual Tributary (VT) from the drop-down lists that appear.

Step 9 Return to your originating procedure (NTP).

DLP-A312 Provision a Half Circuit Source and Destination on a Path Protection Configuration

Purpose	This task provisions a half circuit source and destination on path protection configurations. A half circuit allows you to provision a partial path (one end of a circuit), for example, if you want to provision a circuit with the intent that the path will be completed at a later time or at a different location.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 The Circuit Creation wizard Circuit Source page must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Node drop-down list, choose the node that will contain the half circuit.

Step 2 From the Slot drop-down list, choose the slot containing the card where the circuit will originate.

Step 3 From the Port drop-down list, choose the port where the circuit will originate. This field is not available if a DS-1 card is chosen in Step 2.

Step 4 If the circuit is a DS-1 circuit and you choose a DS-1 card as the source, choose the DS-1 where the traffic will originate from the DS1 drop-down list.

Step 5 Click **Next**.

Step 6 From the Node drop-down list, choose the node that you selected in Step 1.

Step 7 From the Slot drop-down list, choose the OC-N card that will be used to map the DS-1 to a VT1.5 for OC-N transport or to map the DS-3 or OC-N STS circuit to an STS.

Step 8 Choose the destination STS or VT from the drop-down lists that appear.

Step 9 Click **Use Secondary Destination** and repeat Steps 6 through 8.

Step 10 Return to your originating procedure (NTP).

DLP-A313 Create a DCC Tunnel

Purpose	This task creates a data communications channel (DCC) tunnel to transport traffic from third-party SONET equipment across ONS 15454 networks. Tunnels can be created on the Section DCC channel (D1-D3) (if not used by the ONS 15454 as a terminated DCC), or any Line DCC channel (D4-D6, D7-D9, or D10-D12).
Tools/Equipment	OC-N cards must be installed
Prerequisite Procedures	NTP-A35 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Cisco recommends a maximum of 84 DCC tunnel connections. Terminated Section DCCs used by the ONS 15454 cannot be used as a DCC tunnel endpoint, and a Section DCC that is used as a DCC tunnel endpoint cannot be terminated. All DCC tunnel connections are bidirectional.

Step 1 In network view, click the **Provisioning > Overhead Circuits** tabs.

Step 2 Click **Create**.

Step 3 In the Overhead Circuit Creation dialog box, complete the following in the Circuit Attributes area:

- Name—Type the tunnel name.
- Circuit Type—Choose one:
  - **DCC Tunnel-D1-D3**—Allows you to choose either the Section DCC (D1-D3) or a Line DCC (D4-D6, D7-D9, or D10-D12) as the source or destination endpoints.
  - **DCC Tunnel-D4-D12**—Provisions the full Line DCC as a tunnel.

Step 4 Click **Next**.

Step 5 In the Circuit Source area, complete the following:

- Node—Choose the source node.
- Slot—Choose the source slot.
- Port—If displayed, choose the source port.
- Channel—These options appear if you chose DCC Tunnel-D1-D3 as the tunnel type. Choose one of the following:
  - **DCC1 (D1-D3)**—This is the Section DCC.
  - **DCC2 (D4-D6)**—This is Line DCC 1.
  - **DCC3 (D7-D9)**—This is Line DCC 2.
  - **DCC4 (D10-D12)**—This is Line DCC 3.

  DCC options do not appear if they are used by the ONS 15454 (DCC1) or other tunnels.

Step 6 Click **Next**.

Step 7 In the Circuit Destination area, complete the following:

- Node—Choose the destination node.

- Slot—Choose the destination slot.
- Port—If displayed, choose the destination port.
- Channel—These options appear if you chose DCC Tunnel-D1-D3 as the tunnel type. Choose one of the following:
  - **DCC1 (D1-D3)**—This is the Section DCC.
  - **DCC2 (D4-D6)**—This is Line DCC 1.
  - **DCC3 (D7-D9)—**This is Line DCC 2.
  - **DCC4 (D10-D12)**—This is Line DCC 3.

  DCC options do not appear if they are used by the ONS 15454 (DCC1) or other tunnels.

Step 8 Click **Finish**.

Step 9 Put the ports that are hosting the DCC tunnel in service. See the "DLP-A214 Change the Service State for a Port" task on page 19-9 for instructions.

Step 10 Return to your originating procedure (NTP).

DLP-A314 Assign a Name to a Port

Purpose	This task assigns a name to a port on any ONS 15454 card.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Double-click the card that has the port you want to provision.

Step 2 Click the **Provisioning** tab.

Step 3 Click the **Port Name** column for the port number to which you are assigning a name.

Step 4 Type the port name.

The port name can be up to 32 alphanumeric/special characters. The field is blank by default.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

DLP-A315 Log Out a User on a Single Node

Purpose	This task logs out a user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning > Security > Active Logins** tabs.

Step 2 Choose the user that you want to log out and click **Logout**.

Step 3 In the Logout User dialog box, check **Lockout before Logout** if you want to lock the user out. This prevents the user from logging in after logout based on parameters provided in the user lockouts in the Policy tab. A manual unlock by a Superuser is required, or the user is locked out for the amount of time specified in the Lockout Duration field. See the "DLP-A271 Change Security Policy on a Single Node" task on page 19-53 for more information.

Step 4 Click **OK**.

Step 5 Click **Yes** to confirm the logout.

Step 6 Return to your originating procedure (NTP).

DLP-A316 Log Out a User on Multiple Nodes

Purpose	This task logs out a user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 From the View menu, chose **Go to Network View**.

Step 2 Click the **Provisioning > Security > Active Logins** tabs.

Step 3 Choose the user you want to log out.

Step 4 Click **Logout**.

Step 5 In the Logout User dialog box, check the nodes where you want to log out the user.

Step 6 Check **Lockout before Logout** if you want to lock the user out prior to logout. This prevents the user from logging in after logout based on user lockout parameters provisioned in the Policy tab. A manual unlock by a Superuser is required, or the user is locked out for the amount of time specified in the Lockout Duration field. See the "DLP-A271 Change Security Policy on a Single Node" task on page 19-53 for more information.

Step 7 In the Select Applicable Nodes area, uncheck any nodes where you do not want to change the user's settings (all network nodes are selected by default).

Step 8 Click **OK**.

Step 9 Return to your originating procedure (NTP).

DLP-A320 View ML-Series Ether Ports PM Parameters

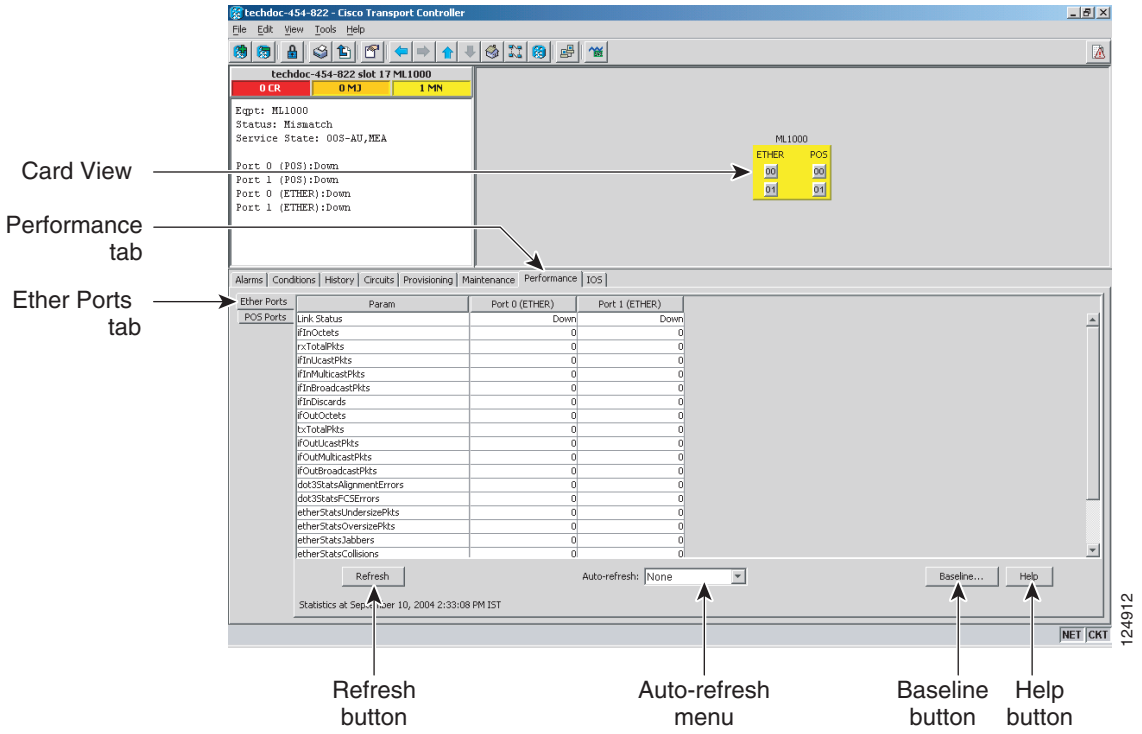
Purpose	This task enables you to view any ML-Series Ethernet card's port PM counts at selected time intervals to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note For ML-Series card provisioning, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

Step 1 In node view, double-click the ML-Series Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance > Ether Ports** tabs (Figure 20-1).

Figure 20-1 Ether Ports on the ML-Series Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Port # columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 9-2.

Step 5 Return to your originating procedure (NTP).

DLP-A321 View ML-Series POS Ports PM Parameters

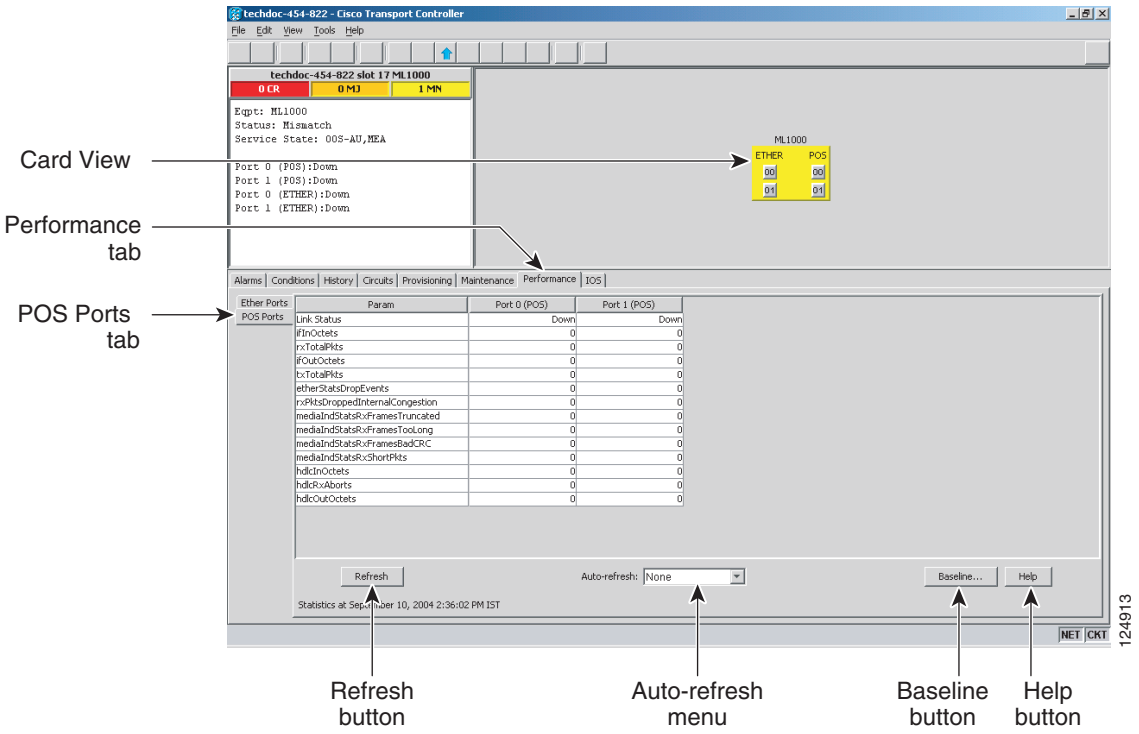
Purpose	This task enables you to view packet-over-SONET (POS) port PM counts at selected time intervals on any ML-Series Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note For ML-Series card provisioning, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide.*

Step 1 In node view, double-click the ML-Series Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **POS Ports** tabs (Figure 20-2).

Figure 20-2 POS Ports on the ML-Series Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Port # columns. For PM parameter definitions refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 9-2.

Step 5 Return to your originating procedure (NTP).

DLP-A322 Manual or Force Switch the Node Timing Reference

Purpose	This task commands the node to switch to the timing reference you have selected if the synchronization status message (SSM) quality of the requested reference is not less than the current reference.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance > Timing > Source** tabs.

Step 2 From the Reference drop-down list for the desired Clock, choose the desired reference.

Step 3 From the Operation drop-down list for the desired Clock, choose one of the following options:

- **Manual**—This operation commands the node to switch to the reference you have selected if the SSM quality of the reference is not lower than the current timing reference.
- **Force**—This operation commands the node to switch to the reference you have selected, regardless of the SSM quality (if the reference is valid).

  For information about the Clear option, see the "DLP-A323 Clear a Manual or Force Switch on a Node Timing Reference" task on page 20-13.

Step 4 Click **Apply** next to the timing source.

Step 5 Click **Yes** in the confirmation dialog box. If the selected timing reference is an acceptable valid reference, the node switches to the selected timing reference.

Step 6 If the selected timing reference is invalid, a warning dialog box appears. Click **OK**; the node does not revert to the normal timing reference.

Step 7 Return to your originating procedure (NTP).

DLP-A323 Clear a Manual or Force Switch on a Node Timing Reference

Purpose	This task clears a Manual or Force switch on a node timing reference and reverts the timing reference to its provisioned reference.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance > Timing > Source** tabs.

Step 2 Find the Clock reference that is currently set to Manual or Force in the Operation menu.

Step 3 From the Operation drop-down list choose **Clear**.

Step 4 Click **Apply**.

Step 5 Click **Yes** in the confirmation dialog box. If the normal timing reference is an acceptable valid reference, the node switches back to the normal timing reference as defined by the system configuration.

Step 6 If the normal timing reference is invalid or has failed, a warning dialog box appears. Click **OK**; the timing reference does not revert.

Step 7 Return to your originating procedure (NTP).

DLP-A324 Provision a VCAT Circuit Source and Destination

Purpose	This task provisions a virtual concatenated (VCAT) circuit source and destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 The Circuit Creation wizard Circuit Source page must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Node drop-down list, choose the node where the circuit will originate.

Step 2 From the Slot drop-down list, choose the slot containing the CE-Series, ML-Series, or FC_MR-4 card where the circuit originates. (If a card's capacity is fully utilized, it does not appear in the list.)

Step 3 Depending on the circuit origination card, choose the source port and/or STS and, if applicable, VT from the Port and STS drop-down lists. The Port drop-down list is only available if the card has multiple ports. STSs and VTs do not appear if they are already in use by other circuits. VTs do not appear for STS-V circuits.

Step 4 Click **Next**.

Step 5 From the Node drop-down list, choose the destination node.

Step 6 From the Slot drop-down list, choose the slot containing the CE-Series, ML-Series, or FC_MR-4 card where the circuit will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the list.)

Step 7 Depending on the card selected in Step 2, choose the source port and/or STS and, if applicable, VT from the Port and STS drop-down lists. The Port drop-down list is only available if the card has multiple ports. STSs and VTs do not appear if they are already in use by other circuits. VTs do not appear for STS-V circuits.

Step 8 Click **Next**.

Step 9 Return to your originating procedure (NTP).

DLP-A325 Provision a VCAT Circuit Route

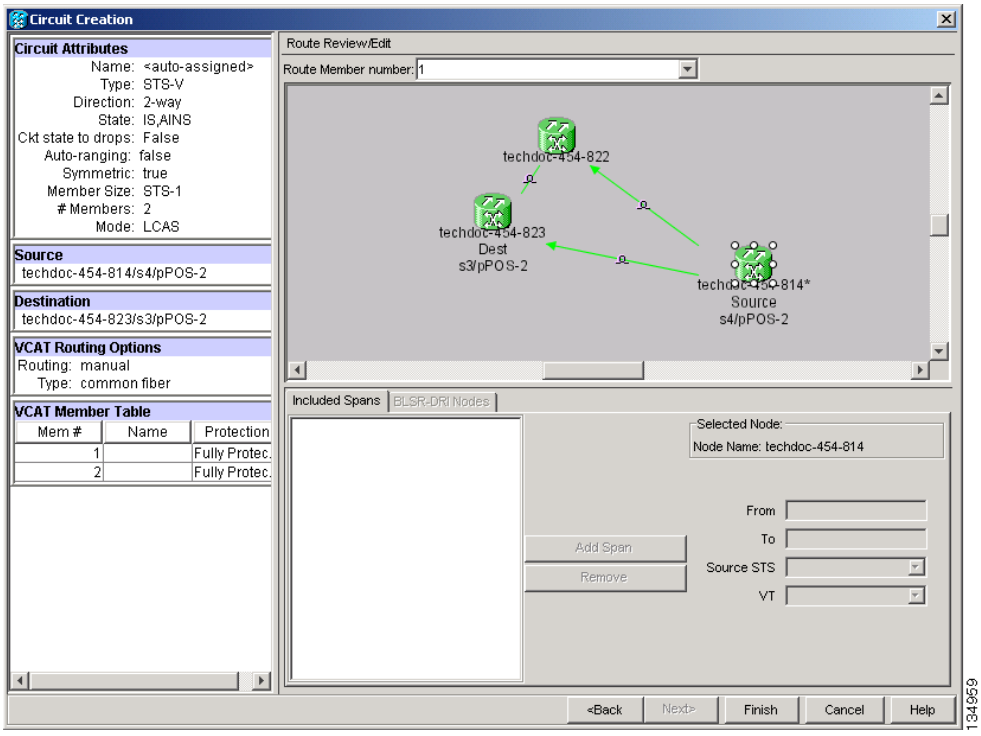
Purpose	This task provisions the circuit route for manually routed VCAT circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 The Circuit Creation wizard Route Review and Edit page must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the Circuit Creation wizard in the Route Review and Edit area, choose the member number from the Route Member Number drop-down list.

Step 2 Click the source node icon if it is not already selected.

Step 3 Starting with a span on the source node, click the arrow of the span you want the circuit to travel. The arrow turns yellow. In the Selected Span area, the From and To fields provide span information. The source STS appears. Figure 20-3 shows an example.

Figure 20-3 Manually Routing a VCAT Circuit



Step 4 Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

Step 5 Repeat Steps 3 and 4 until the circuit is provisioned from the source to the destination node through all intermediary nodes.

Step 6 Repeat Steps 1 through 5 for each member.

Step 7 Return to your originating procedure (NTP).

DLP-A326 Change a BLSR Node ID

Purpose	This task changes a BLSR node ID.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu choose **Go to Network View**.

Step 2 On the network map, double-click the node with the node ID you want to change.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Choose a Node ID number. Do not choose a number already assigned to another node in the same BLSR.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

DLP-A327 Configure the CTC Alerts Dialog Box for Automatic Popup

Purpose	This task sets up the CTC Alerts dialog box to open for all alerts, for circuit deletion errors only, or never. The CTC Alerts dialog box displays network disconnection, Send-PDIP inconsistency, circuit deletion status, condition retrieval errors, and software download failure.
Tools	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **CTC Alerts** toolbar icon.

Step 2 In the CTC Alerts dialog box, choose one of the following:

- **All alerts**—Sets the CTC Alerts dialog box to open automatically for all notifications.
- **Error alerts only**—Sets the CTC Alerts dialog box to open automatically for circuit deletion errors only.
- **Never**—Sets the CTC Alerts dialog box to never open automatically.

Step 3 Click **Close**.

Step 4 Return to your originating procedure (NTP).

DLP-A328 Create a Two-Fiber BLSR Using the BLSR Wizard

Purpose	This task creates a two-fiber BLSR at each BLSR-provisioned node using the CTC BLSR wizard. The BLSR wizard checks to see that each node is ready for BLSR provisioning, then provisions all the nodes at one time.
Tools/Equipment	None
Prerequisite Procedures	NTP-A40 Provision BLSR Nodes, page 5-10 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click **Create BLSR**.

Step 4 In the BLSR Creation dialog box, set the BLSR properties:

- Ring Type—Choose two-fiber.
- Speed—Choose the BLSR ring speed: OC-12, OC-48, or OC-192. The speed must match the OC-N speed of the BLSR trunk (span) cards.

Note If you are creating an OC-12 BLSR and will eventually upgrade it to OC-48 or OC-192, use the single-port OC-12 cards (OC12 IR/STM4 SH 1310, OC12 IR/STM4 SH 1310, or OC12 IR/STM4 SH 1310). You cannot upgrade a BLSR on a four-port OC-12 (OC12/STM4-4) because OC-48 and OC-192 cards are single-port.

- Ring Name—Assign a ring name. The name can be from 1 to 6 characters in length. Any alphanumeric string is permissible, and upper and lower case letters can be combined. Do not use the character string “All” in either upper or lower case letters; this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.
- Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path following a ring switch. The default is 5 minutes. Ring reversion can be set to Never.

Step 5 Click **Next**. If the network graphic appears, go to Step 6.

If CTC determines that a BLSR cannot be created, for example, not enough optical cards are installed or it finds circuits with path protection selectors, a “Cannot Create BLSR” message appears. If this occurs, complete the following steps:

a. Click **OK**.

b. In the Create BLSR window, click **Excluded Nodes**. Review the information explaining why the BLSR could not be created, then click **OK**.

c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.

d. Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 5-10, making sure all steps are completed accurately, then start this procedure again.

Step 6 In the network graphic, double-click a BLSR span line. If the span line is DCC connected to other BLSR cards that constitute a complete ring, the lines turn blue. If the lines do not form a complete ring, double-click span lines until a complete ring is formed. When the ring is DCC connected, go to Step 7.

Step 7 Click **Finish**. If the BLSR window appears with the BLSR you created, go to Step 8. If a "Cannot Create BLSR" or "Error While Creating BLSR" message appears:

a. Click **OK**.

b. In the Create BLSR window, click **Excluded Nodes.** Review the information explaining why the BLSR could not be created, then click **OK**.

c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.

d. Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 5-10, making sure all steps are completed accurately, then start this procedure again.

Note Some or all of the following alarms might briefly appear during BLSR setup: E-W-MISMATCH, RING-MISMATCH, APSCIMP, APSCDFLTK, and BLSROSYNC.

Step 8 Verify the following:

- On the network view graphic, a green span line appears between all BLSR nodes.
- All E-W-MISMATCH, RING-MISMATCH, APSCIMP, APSCDFLTK, and BLSROSYNC alarms are cleared. See the *Cisco ONS 15454 Troubleshooting Guide* for alarm troubleshooting.

Note The numbers in parentheses after the node name are the BLSR node IDs assigned by CTC. Every ONS 15454 in a BLSR is given a unique node ID, 0 through 31. To change it, complete the "DLP-A326 Change a BLSR Node ID" task on page 20-16.

Step 9 Return to your originating procedure (NTP).

DLP-A329 Create a Two-Fiber BLSR Manually

Purpose	This tasks creates a BLSR at each BLSR-provisioned node without using the BLSR wizard.
Tools/Equipment	None
Prerequisite Procedures	NTP-A40 Provision BLSR Nodes, page 5-10 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > BLSR** tabs.

Step 2 Click **Create**.

Step 3 In the Suggestion dialog box, click **OK**.

Step 4 In the Create BLSR dialog box, set the BLSR properties:

- Ring Type—Choose two-fiber.
- Ring Name—Assign a ring name. You must use the same ring name for each node in the BLSR. Any alphanumeric character string is permissible, and upper and lower case letters can be combined. Do not use the character string “All” in either upper or lower case letters; this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.
- Node ID—Choose a Node ID from the drop-down list (0 through 31). The Node ID identifies the node to the BLSR. Nodes in the same BLSR must have unique Node IDs.
- Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path. The default is 5 minutes. All nodes in a BLSR must have the same reversion time setting.
- West Line—Assign the west BLSR port for the node from the drop-down list.

  The east and west ports must match the fiber connections and DCC terminations set up in the “NTP-A40 Provision BLSR Nodes” procedure on page 5-10.
- East Line—Assign the east BLSR port for the node from the drop-down list.

Step 5 Click **OK**.

Note Some or all of the following alarms will appear until all the BLSR nodes are provisioned: E-W-MISMATCH, RING-MISMATCH, APSCIMP, APSCDFLTK, and BLSROSYNC. The alarms will clear after you configure all the nodes in the BLSR.

Step 6 From the View menu, choose **Go to Other Node**.

Step 7 In the Select Node dialog box, choose the next node that you want to add to the BLSR.

Step 8 Repeat Steps 1 through 7 at each node that you want to add to the BLSR. When all nodes have been added, continue with Step 9.

Step 9 From the View menu, choose **Go to Network View**. After 10 to 15 seconds, verify the following:

- A green span line appears between all BLSR nodes.
- All E-W-MISMATCH, RING-MISMATCH, APSCIMP, APSCDFLTK, and BLSROSYNC alarms are cleared.

Step 10 Return to your originating procedure (NTP).

DLP-A330 Preprovision a Card Slot

Purpose	This task preprovisions a card slot in CTC before you physically install the card in the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, right-click the empty slot where you will later install a card.

Step 2 From the Add Card shortcut menu, choose the card type that will be installed. Only cards that can be installed in the slot appear in the Add Card shortcut menu.

When you preprovision a slot, the card appears purple in the CTC shelf graphic, rather than white when a card is installed in the slot. NP (not present) on the card graphic indicates that the card is not physically installed.

Step 3 Return to your originating procedure (NTP).

DLP-A332 Change Tunnel Type

Purpose	This task converts a traditional DCC tunnel to an IP-encapsulated tunnel or an IP-encapsulated tunnel to a traditional SDCC tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-A313 Create a DCC Tunnel, page 20-7 DLP-A341 Create an IP-Encapsulated Tunnel, page 20-32
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > Overhead Circuits** tabs.

Step 3 Click the circuit tunnel that you want to convert.

Step 4 Click **Edit**.

Step 5 In the Edit circuit window, click the **Tunnel** tab.

Step 6 In the Attributes area, complete the following:

- If you are converting a traditional DCC tunnel to an IP-encapsulated tunnel, check the **Change to IP Tunnel** check box and type the percentage of total SDCC bandwidth used in the IP tunnel (the minimum percentage is 10 percent).
- If you are converting an IP tunnel to a traditional DCC tunnel, check the **Change to SDCC Tunnel** check box.

Step 7 Click **Apply**.

Step 8 In the confirmation dialog box, click **Yes** to continue.

Step 9 In the Circuit Changed status box, click **OK** to acknowledge that the circuit change was successful.

Step 10 Return to your originating procedure (NTP).

DLP-A333 Delete Circuits

Purpose	This task deletes circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 2 Verify that traffic is no longer carried on the circuit and that the circuit can be safely deleted.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 5 Click the **Circuits** tab.

Step 6 Choose the circuits you want to delete, then click **Delete**.

Step 7 In the Delete Circuits confirmation dialog box, check one or both of the following, as needed:

- Change drop port admin state—Choose the administrative state for the drop ports:
  - IS—Puts the circuit cross-connects in the In-Service and Normal (IS-NR) service state.
  - OOS,DSBLD—Puts the circuit cross-connects in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. Traffic is not passed on the circuit. If the circuit is not the same size as the port or the only circuit using the port, CTC will not change the port service state.
  - IS,AINS—Puts the circuit cross-connects in the Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS) service state. When the connections receive a valid signal, the cross-connect service states automatically change to IS-NR.
  - OOS,MT—Puts the circuit cross-connects in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state. This service state does not interrupt traffic flow and allows loopbacks to be performed on the circuit, but suppresses alarms and conditions. Use the OOS,MT administrative state for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; OOS; or IS,AINS when testing is complete.

Note CTC will not allow you to change a drop port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.

- Notify when completed—If checked, the CTC Alerts confirmation dialog box indicates when all circuit source/destination ports are out of service (OOS) and the circuit is deleted. During this time, you cannot perform other CTC functions. If you are deleting many circuits, you might need to wait a few minutes for confirmation. Circuits are deleted whether or not this check box is checked.

Note The CTC Alerts dialog box will not automatically open to show a deletion error unless you checked All alerts or Error alerts only in the CTC Alerts check box. For more information, see the "DLP-A327 Configure the CTC Alerts Dialog Box for Automatic Popup" task on page 20-16. If the CTC Alerts dialog box is not set to open automatically with a notification, the red triangle inside the CTC Alerts toolbar icon indicates that a notification exists.

Step 8 Complete one of the following:

- If you checked Notify when completed, the CTC Alerts dialog box appears. If you want to save the information, continue with Step 9. If you do not want to save the information, continue with Step 10.
- If you did not check Notify when completed, the Circuits window appears. Continue with Step 11.

Step 9 If you want to save the information in the CTC Alerts dialog box, complete the following steps. If you do not want to save, continue with the Step 10.

a. Click **Save**.

b. Click **Browse** and navigate to the directory where you want to save the file.

c. Type the file name using a .txt file extension, and click **OK**.

Step 10 Click **Close** to close the CTC Alerts dialog box.

Step 11 Complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 12 Return to your originating procedure (NTP).

DLP-A334 Delete Overhead Circuits

Purpose	This task deletes overhead circuits. Overhead circuits include DCC tunnels, IP-encapsulated tunnels, the AIC-I card orderwire, and the AIC-I card user data channel (UDC).
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Deleting overhead circuits is service affecting if the circuits are in service (IS). To put circuits out of service (OOS), see the "DLP-A214 Change the Service State for a Port" task on page 19-9.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > Overhead Circuits** tabs.

Step 3 Click the overhead circuit that you want to delete: local or express orderwire, user data, IP-encapsulated tunnel, or DCC tunnel.

Step 4 Click **Delete**.

Step 5 In the confirmation dialog box, click **Yes** to continue.

Step 6 Return to your originating procedure (NTP).

DLP-A335 Delete VLANs

Purpose	This task removes VLANs from a domain.
Tools/Equipment	None
Prerequisite Procedures	See Chapter 6, "Create Circuits and VT Tunnels" for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note VLANs in use will not be deleted.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 From the Tools menu, choose **Manage VLANS**.

Step 3 In the All VLANs dialog box, click the VLAN that you want to remove.

Step 4 Click **Delete**.

Step 5 In the confirmation dialog box, click **Yes**.

Step 6 Return to your originating procedure (NTP).

DLP-A336 Repair an IP Tunnel

Purpose	This task repairs circuits that have a OOS-PARTIAL status as a result of node IP address changes.
Tools/Equipment	None
Prerequisite Procedures	See Chapter 6, "Create Circuits and VT Tunnels" for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Obtain the original IP address of the node in question.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 From the Tools menu, choose **Overhead Circuits > Repair IP Circuits**.

Step 4 Review the text in the IP Repair wizard and click **Next**.

Step 5 In the Node IP address area, complete the following:

- Node—Choose the node that has an OOS-PARTIAL circuit.
- Current IP Address—Type the current IP address.
- Old IP Address—Type the node's original IP address.

Step 6 Click **Next**.

Step 7 Click **Finish**.

Step 8 Return to your originating procedure (NTP).

DLP-A337 Run the CTC Installation Wizard for Windows

Purpose	This task installs the CTC online user manuals, Acrobat Reader 6.0.1 (Acrobat Reader 8.1.2 for Release 9.2 and later), JRE 5.0 (JRE 1.6 for Release 9.2 and later), and the CTC JAR files on a Windows computer. JRE 5.0 (JRE 1.6 for Release 9.2 and later) is required to run Release 9.1. Pre-installing the CTC JAR files saves time at initial login. If the JAR files are not installed, they are downloaded from the TCC2/TCC2P card the first time you log in.
Tools/Equipment	Cisco ONS 15454 Release 9.1, 9.2, or 9.2.1 software CD
Prerequisite Procedures	None
Required/As Needed	This task is required if any one of the following is true: • JRE 1.4.2 or JRE 5.0 (JRE 1.6 for Release 9.2 and later) is not installed. • CTC online user manuals are not installed and are needed. • CTC JAR files are not installed and are needed.
Onsite/Remote	Onsite or remote
Security Level	None

Note If you will log into nodes running CTC software earlier than Release 4.6, uninstall JRE 1.4.2 or 5.0 (JRE 1.6 for Release 9.2 and later) and reinstall JRE 1.3.1_2.

Step 1 Verify that your computer has the following:

- Processor—Pentium III, 700 Mhz or faster (Pentium IV or equivalent for Release 9.2 and later)
- RAM—384 MB recommended, 512 MB optimum (1 GB for Release 9.2 and later)

Note Processor and RAM requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM.

- Hard drive—20 GB hard drive recommended with at least 50 MB (250 MB for Release 9.2 and later) of space available
- Operating system— Windows 2000 (with Service Pack 3), Windows XP (with Service Pack 1) or Windows Vista (Windows 7 for Release 9.2 and later). If your operating system is Windows NT 4.0 go to Step 2. If your operating system is Windows Vista or Windows 7 go to Step 3. For all other case go to Step 4.

Step 2 Verify that Service Pack 6a or later is installed. From Windows Start menu, choose **Programs > Administrative Tools > Windows NT Diagnostics** and check the service pack on the Version tab of the Windows NT Diagnostics dialog box. If Service Pack 6a or later is not installed, do not continue. Install Service Pack 6a following the computer upgrade procedures for your site. Go to Step 4.

Step 3 Complete DLP-A578 Configuring Windows Vista to Support CTC, page 22-91 and go toStep 4.

Step 4 Insert the Cisco ONS 15454 Release 9.1, 9.2, or 9.2.1 software CD into your computer CD drive. The installation program begins running automatically. If it does not start, navigate to the CD directory and double-click **setup.exe**.

The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer:

- Java Runtime Environment 5.0 (JRE 1.6 for Release 9.2 and later)
- Acrobat Reader 6.0.1 (Acrobat Reader 8.1.2 for Release 9.2 and later)
- Online User Manuals
- CTC JAR files

Note JRE 5.0 is required to log into nodes running Software Release 9.1 (JRE 1.6 for Release 9.2 and later). Preinstalling the CTC JAR files saves time at initial login. If the JAR files are not installed, they are downloaded from the TCC2/TCC2P card the first time you log in.

Step 5 Click **Next**.

Step 6 Complete one of the following:

- Click **Typical** to install all three components. If you already have JRE 1.4.2 or 5.0 (JRE 1.6 for Release 9.2 and later) installed on your computer, choose **Custom**.
- Click **Custom** if you want to install either the JRE or the online user manuals. By default, the JRE and Acrobat Reader are selected.

Step 7 Click **Next**.

Step 8 Complete the following, as applicable:

- If you selected Typical in Step 6, skip this step and continue with Step 9.
- If you selected Custom, check the CTC component that you want to install and click **Next**.
  - If you selected Online User Manuals, continue with Step 9.
  - If you did not select Online User Manuals, continue with Step 11.

Step 9 The directory where the installation wizard will install CTC online user manuals appears. The default is C:\Program Files\Cisco\CTC\Documentation.

- If you want to change the CTC online user manuals directory, type the new directory path in the Directory Name field, or click **Browse** to navigate to the directory.
- If you do not want to change the directory, skip this step.

Step 10 Click **Next**.

Step 11 Review the components that will be installed. If you want to change the components, complete one of the following:

- If you selected Typical in Step 6, click **Back** twice to return to the installation setup type page. Choose **Custom** and repeat Steps 7 through 10.
- If you selected Custom in Step 6, click **Back** once or twice (depending on the components selected) until the component selection page appears. Repeat Steps 8 through 10.

Step 12 Click **Next**. It might take a few minutes for the JRE installation wizard to appear. If you selected Custom in Step 6 and you need to install the JRE, continue with Step 14.

Step 13 To install the JRE, complete the following:

a. In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and choose one of the following:

- I accept the terms of the license agreement—Accepts the license agreement. Continue with Step b.

- I do not accept the terms of the license agreement—Disables the Next button on the Java 2 Runtime Environment License Agreement dialog box. Click **Cancel** to return to the CTC installation wizard. CTC will not install the JRE. Continue with Step 14.

Note If JRE 1.4.2 is already installed on your computer, the License Agreement page does not appear. You must click Next and then choose Modify to change the JRE installation or Remove to uninstall the JRE. If you choose Modify and click Next, continue with Step e. If you choose Remove and click Next, continue with Step i.

b. Click **Next**.

c. Choose one of the following:

- Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
- Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.

d. Click **Next**.

e. If you selected Typical, continue with Step i. If you selected Custom, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:

- Java 2 Runtime Environment—(Default) Installs JRE 5.0 (JRE 1.6 for Release 9.2 and later) with support for European languages.
- Support for Additional Languages—Adds support for non-European languages.
- Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

The drop-down list options for each program feature include:

- This feature will be installed on the local hard drive—Installs the selected feature.
- This feature and all subfeatures will be installed on the local hard drive—Installs the selected feature and all subfeatures.
- Don't install this feature now—Does not install the feature (not an option for Java 2 Runtime Environment).

To modify the directory where the JRE version is installed, click **Change**, navigate to the desired directory, and click **OK**.

f. Click **Next**.

g. In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.

Note Setting the JRE as the default for these browsers might cause problems with these browsers.

h. Click **Next**.

i. Click **Finish**. If you are uninstalling the JRE, click **Remove**.

Step 14 In the Cisco Transport Controller Installation Wizard, click **Next**. The online user manuals install.

Step 15 Click **Finish**.

Step 16 Return to your originating procedure (NTP).

DLP-A338 Run the CTC Installation Wizard for UNIX

Purpose	This task installs the CTC online user manuals, Acrobat Reader 6.0.1 (Adobe Reader 8.1.2 for Release 9.2 and later), JRE 1.4.2, and the CTC JAR files on a Solaris workstation. JRE 1.4.2 or JRE 1.5 is required to run Release 9.1 (JRE 1.6 for Release 9.2 and later). Pre-installing the CTC JAR files saves time at initial login. If the JAR files are not installed, they are downloaded from the TCC2/TCC2P card the first time you login.
Tools/Equipment	Cisco ONS 15454 Release 9.1, 9.2, or 9.2.1 software CD
Prerequisite Procedures	None
Required/As Needed	Required if any of the following are true: • JRE 1.4.2 or 5.0 (JRE 1.6 for Release 9.2 and later) is not installed. • CTC online user manuals are not installed and are needed. • CTC JAR files are not installed are needed.
Onsite/Remote	Onsite or remote
Security Level	None

Note If you will log into nodes running CTC software earlier than Release 4.6, uninstall JRE 1.4.2 or 5.0 (JRE 1.6 for Release 9.2 and later) and reinstall JRE 1.3.1_2. To run Software R9.1, uninstall JRE 1.3.1_2 and reinstall JRE 5.0 (JRE 1.6 for Release 9.2 and later).

Note JRE 5.0 requires Netscape 7.x or Internet Explorer 6.x.

Step 1 Verify that your computer has the following:

- RAM—384 MB recommended, 512 MB optimum (1 GB for Release 9.2 and later)
- Hard drive—20 GB hard drive recommended with at least 50 MB of space available (250 MB of
- space free space for Release 9.2 and later)
- Operating system—Solaris 8 or 9

Note These requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM.

Step 2 Change the directory, type:

cd /cdrom/cdrom0/

Step 3 From the techdoc454 CD directory, type:

./setup.bat

The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer:

- Java Runtime Environment 5.0 (JRE 1.6 for Release 9.2 and later)
- Acrobat Reader 6.0.1 (Acrobat Reader 8.1.2 for Release 9.2 and later)
- Online User Manuals
- CTC JAR files

Step 4 Click **Next**.

Step 5 Complete one of the following:

- Click **Typical** to install both the Java Runtime Environment and online user manuals. If you already have JRE 5.0 (JRE 1.6 for Release 9.2 and later) installed on your computer, choose **Custom**.
- Click **Custom** if you want to install either the JRE or the online user manuals.

Step 6 Click **Next**.

Step 7 Complete the following, as applicable:

- If you selected Typical in Step 5, continue with Step 8.
- If you selected Custom, check the CTC component that you want to install and click **Next**.
  - If you selected Online User Manuals, continue with Step 8.
  - If you did not select Online User Manuals, continue with Step 10.

Step 8 The directory where the installation wizard will install CTC online user manuals appears. The default is /usr/doc/ctc.

- If you want to change the CTC online user manuals directory, type the new directory path in the Directory Name field, or click **Browse** to navigate to the directory.
- If you do not want to change the CTC online user manuals directory, skip this step.

Step 9 Click **Next**.

Step 10 Review the components that will be installed.

- If you selected Typical in Step 5, click **Back** twice to return to the installation setup type page. Choose **Custom** and repeat Steps 6 through 9.
- If you selected Custom in Step 5, click **Back** once or twice (depending on the components selected) you reach the component selection page and check the desired components. Repeat Steps 7 through 9.

Step 11 Click **Next**. It might take a few minutes for the JRE installation wizard to appear. If you selected Custom in Step 6 and you need to install the JRE, continue with Step 13.

Step 12 To install the JRE, complete the following:

a. In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and choose one of the following:

- I accept the terms of the license agreement—Accepts the license agreement. Continue with Step b.
- I do not accept the terms of the license agreement—Disables the Next button on the Java 2 Runtime Environment License Agreement dialog box. Click **Cancel** to return to the CTC installation wizard. CTC will not install the JRE. Continue with Step 13.

Note If JRE 5.0 (JRE 1.6 for Release 9.2 and later) is already installed on your computer, the License Agreement page does not appear. You must click Next and then choose Modify to change the JRE installation or Remove to uninstall the JRE. If you choose Modify and click Next, continue with Step e. If you choose Remove and click Next, continue with Step i.

b. Click **Next**.

c. Choose one of the following:

- Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
- Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.

d. Click **Next**.

e. If you selected Typical, continue with Step i. If you selected Custom, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:

- Java 2 Runtime Environment—(Default) Installs JRE 5.0 (JRE 1.6 for Release 9.2 and later) with support for European languages.
- Support for Additional Languages—Adds support for non-European languages.
- Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

The drop-down list options for each program feature include:

- This feature will be installed on the local hard drive—Installs the selected feature.
- This feature and all subfeatures will be installed on the local hard drive—Installs the selected feature and all subfeatures.
- Don't install this feature now—Does not install the feature (not an option for Java 2 Runtime Environment).

To modify the directory where the JRE version is installed, click **Change**, navigate to the desired directory, and click **OK**.

f. Click **Next**.

g. In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.

Note Setting the JRE version as the default for these browsers might cause problems with these browsers.

h. Click **Next**.

i. Click **Finish**. If you are uninstalling the JRE, click **Remove**.

Step 13 In the Cisco Transport Controller Installation Wizard, click **Next**. The online user manuals install.

Step 14 Click **Finish**.

Note Be sure to record the names of the directories you choose for JRE and the online user manuals.

Step 15 Return to your originating procedure (NTP).

DLP-A339 Delete a Node from the Current Session or Login Group

Purpose	This task removes a node from the current CTC session or login node group. To remove a node from a login node group that is not the current one, see the "DLP-A372 Delete a Node from a Specified Login Node Group" task on page 20-56.
Tools	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the node that you want to delete.

Step 3 From the CTC File menu, click **Delete Selected Node**.

After a few seconds, the node disappears from the network view map.

Step 4 Return to your originating procedure (NTP).

DLP-A340 View Port Status on the LCD

Purpose	This task allows you to view OC-N port status without using CTC. The LCD shows the working/protection provisioning status and the active/standby line status for ports in 1+1 and BLSR configurations. For unprotected and path protection ports, the LCD always displays "Working/Active."
Tools/Equipment	None
Prerequisite Procedures	NTP-A16 Install Optical Cards and Connectors, page 2-8
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

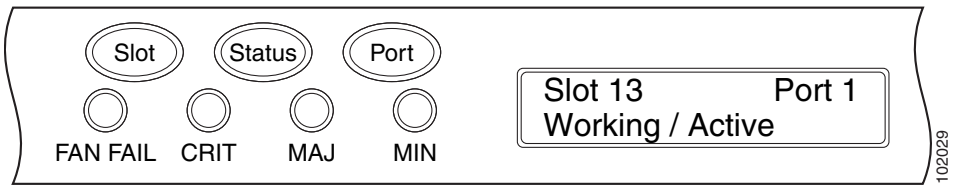
Step 1 Press the **Slot** button on the LCD panel until the desired slot appears on the LCD.

Step 2 Press the **Port** button until the desired port appears on the LCD. (Only Port 1 of single-port cards will display actual port status.)

Step 3 Press the **Status** button. The LCD will display alarm information for approximately 10 seconds, and then will indicate if the port is in working or protect mode and is active or standby.

Figure 20-4 shows an example of port status on the LCD panel.

Figure 20-4 Port Status on the LCD Panel



Note A blank LCD results when the fuse on the AIP board has blown. If this occurs, contact Cisco Technical Assistance (TAC). See the "Obtaining Documentation and Submitting a Service Request" section on page lxiv for more information.

Step 4 Return to your originating procedure (NTP).

DLP-A341 Create an IP-Encapsulated Tunnel

Purpose	This task creates a an IP-encapsulated tunnel to transport traffic from third-party SONET equipment across ONS 15454 networks. IP-encapsulated tunnels are created on the Section DCC channel (D1-D3) (if not used by the ONS 15454 as a terminated DCC).
Tools/Equipment	OC-N cards must be installed.
Prerequisite Procedures	NTP-A35 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Each ONS 15454 can have up to ten IP-encapsulated tunnel connections. Terminated Section DCCs used by the ONS 15454 cannot be used as tunnel endpoints, and a Section DCC that is used as a tunnel endpoint cannot be terminated. All tunnel connections are bidirectional.

Step 1 Verify that IP addresses are provisioned at both the source and destination nodes of the planned tunnel. For more information, see the "DLP-A249 Provision IP Settings" task on page 19-30.

Step 2 In network view, click the **Provisioning > Overhead Circuits** tabs.

Step 3 Click **Create**.

Step 4 In the Overhead Circuit Creation dialog box, complete the following in the Circuit Attributes area:

- Name—Type the tunnel name.
- Type—Choose **IP Tunnel-D1-D3**.

- Maximum Bandwidth—Type the percentage of total SDCC bandwidth used in the IP tunnel (the minimum percentage is 10 percent).

Step 5 Click **Next**.

Step 6 In the Circuit Source area, complete the following:

- Node—Choose the source node.
- Slot—Choose the source slot.
- Port—If displayed, choose the source port.
- Channel—Displays IPT (D1-D3).

Step 7 Click **Next**.

Step 8 In the Circuit Destination area, complete the following:

- Node—Choose the destination node.
- Slot—Choose the destination slot.
- Port—If displayed, choose the destination port.
- Channel—Displays IPT (D1-D3).

Step 9 Click **Finish**.

Step 10 Put the ports that are hosting the IP-encapsulated tunnel in service. See the "DLP-A214 Change the Service State for a Port" task on page 19-9 for instructions.

Step 11 Return to your originating procedure (NTP).

DLP-A347 Refresh E-Series and G-Series Ethernet PM Counts

Purpose	This task changes the window view to display E-Series and G-Series Ethernet PM parameters intervals.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance > History** tabs.

Step 3 From the Interval drop-down list click one of the following:

- 1 min
- 15 min
- 1 hour
- 1 day

Step 4 Click **Refresh**. Performance monitoring appears in the interval selected synchronized with the time of day.

Step 5 View the Prev column to find PM counts for the latest selected interval.

Each monitored performance parameter has corresponding threshold values for the latest time period. If the value of the counter exceeds the threshold value for a particular selected interval, a threshold crossing alert (TCA) is raised. The number represents the counter value for each specific performance monitoring parameter.

Step 6 View the Prev-*n* columns to find PM counts for the previous intervals.

If a complete count over the selected interval is not possible, the value appears with a yellow background. For example, if you selected the 1-day interval, an incomplete or incorrect count can be caused by monitoring for less than 24 hours after the counter started, changing node timing settings, changing the time zone settings, replacing a card, resetting a card, or changing port service states. When the problem is corrected, the subsequent 1-day interval appears with a white background.

Step 7 Return to your originating procedure (NTP).

DLP-A348 Monitor PM Counts for a Selected Signal

Purpose	This task enables you to view near-end or far-end PM counts for a specific signal (STS*n*), path (VT*n*), and port (DS*n*) on a selected card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

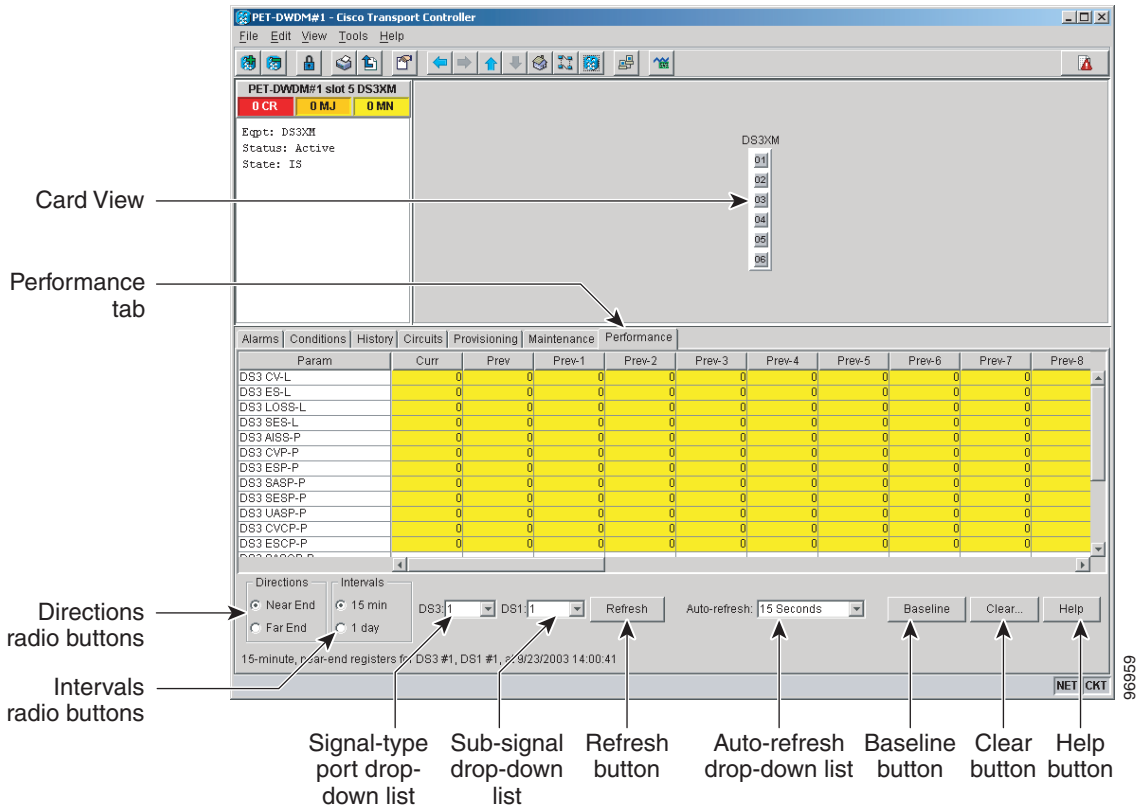
Different port and signal-type menus appear depending on the card type and the circuit type. The appropriate types (DS1, DS3, VT path, STS path) appear based on the card. For example, the DS3XM cards list DS3, DS1, VT path, and STS path PM parameters as signal types. This enables you to select both the DS-3 port and the DS-1 within the specified DS-3.

Step 3 In the signal type drop-down lists, click the following options as appropriate:

- DS: *n* or Port: *n* (card port number)
- VT: *n* (VT path number)
- STS: *n* (STS number within the VT path)

Figure 20-5 shows the port and signal type drop-down lists on the Performance window for a DS3XM-6 card.

Figure 20-5 Signal Type Drop-Down Lists for a DS3XM-6 Card



Step 4 Click **Refresh**. All PM counts recorded by the near-end or far-end node for the specified outgoing signal type on the selected card and port appear. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 5 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 6 Return to your originating procedure (NTP).

DLP-A349 Clear Selected PM Counts

Purpose	This task uses the Clear button to clear specified PM counts depending on the option selected.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution Pressing the Clear button can mask problems if used incorrectly. This button is commonly used for testing purposes. After pressing this button the current bin is marked invalid. Also note that the UAS state is not cleared if you were counting UAS; therefore, this count could be unreliable when UAS is no longer counting.

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click **Clear**.

Step 4 From the Clear Statistics drop-down list, choose one of these three options:

- **Displayed statistics**: Clearing displayed statistics erases from the card and the window all PM counts associated with the current combination of statistics on the selected port. This means the selected time interval, direction, and signal type counts are erased from the card and the window.
- **All statistics for port** *x*: Clearing all statistics for port *x* erases from the card and the window all PM counts associated with all combinations of the statistics on the selected port. This means all time intervals, directions, and signal type counts are erased from the card and the window.
- **All statistics for card**: Clearing all statistics for card erases from the card and the window all PM counts for all ports.

Step 5 From the Clear Statistics drop-down list, choose **OK** to clear the selected statistics.

Step 6 Verify that the selected PM counts have been cleared.

Step 7 Return to your originating procedure (NTP).

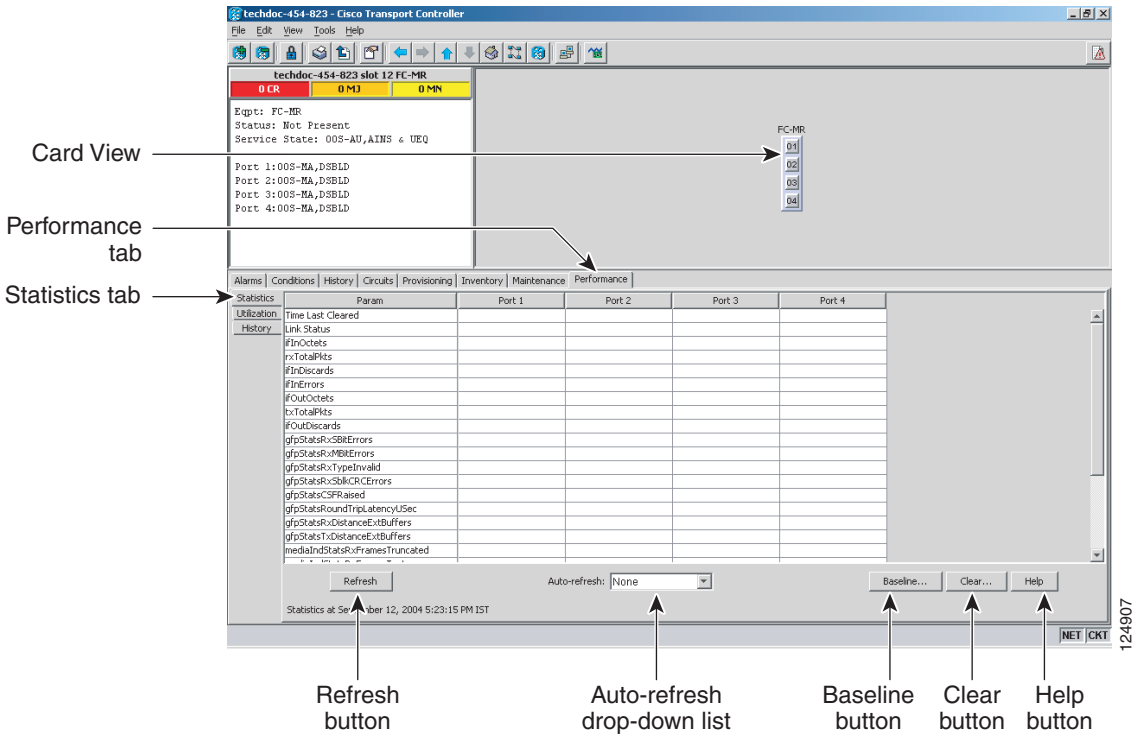
DLP-A350 View FC_MR-4 Statistics PM Parameters

Purpose	This task enables you to view current statistical PM counts on an FC_MR-4 card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the FC_MR-4 card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Statistics** tabs (Figure 20-6).

Figure 20-6 FC_MR-4 Statistics on the Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names appear in the Param column. The current PM parameter values appear in the Port # columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 5 Return to your originating procedure (NTP).

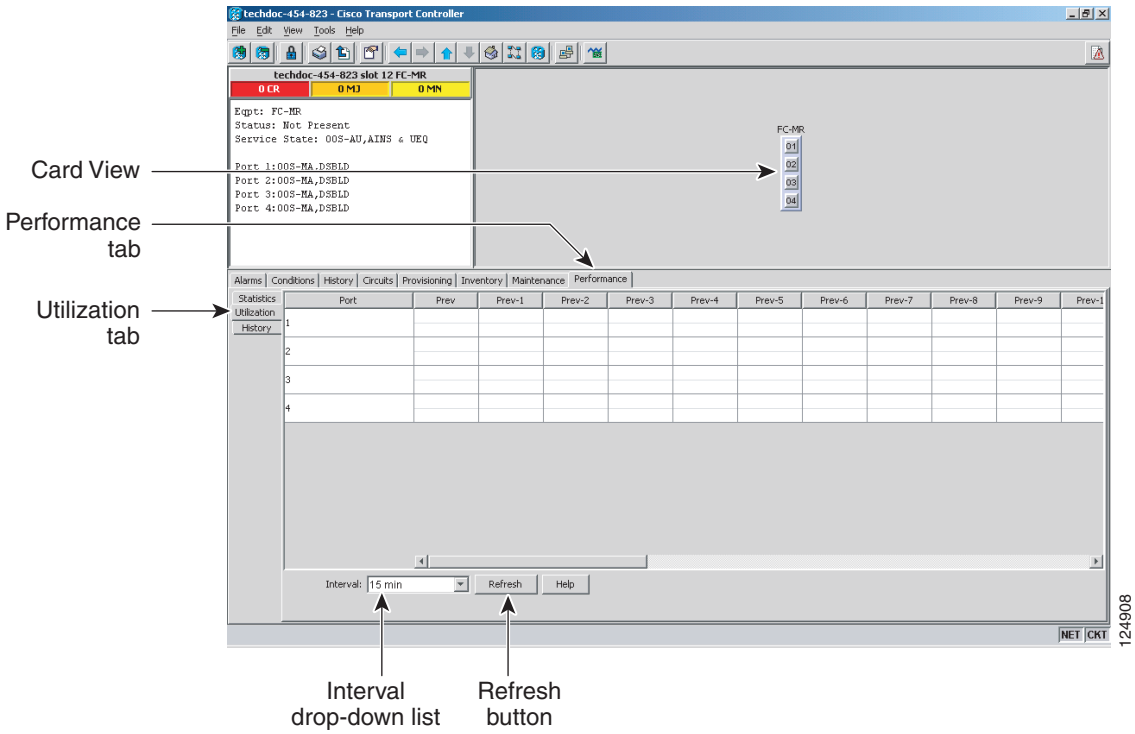
DLP-A351 View FC_MR-4 Utilization PM Parameters

Purpose	This task enables you to view line utilization PM counts on an FC_MR-4 card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the FC_MR-4 card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Utilization** tabs (Figure 20-7).

Figure 20-7 FC_MR-4 Utilization on the Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring utilization values for each port on the card appear.

Step 4 View the Port # column to find the port you want to monitor.

Step 5 The transmit (Tx) and receive (Rx) bandwidth utilization values for the previous time intervals appear in the Prev-*n* columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 6 Return to your originating procedure (NTP).

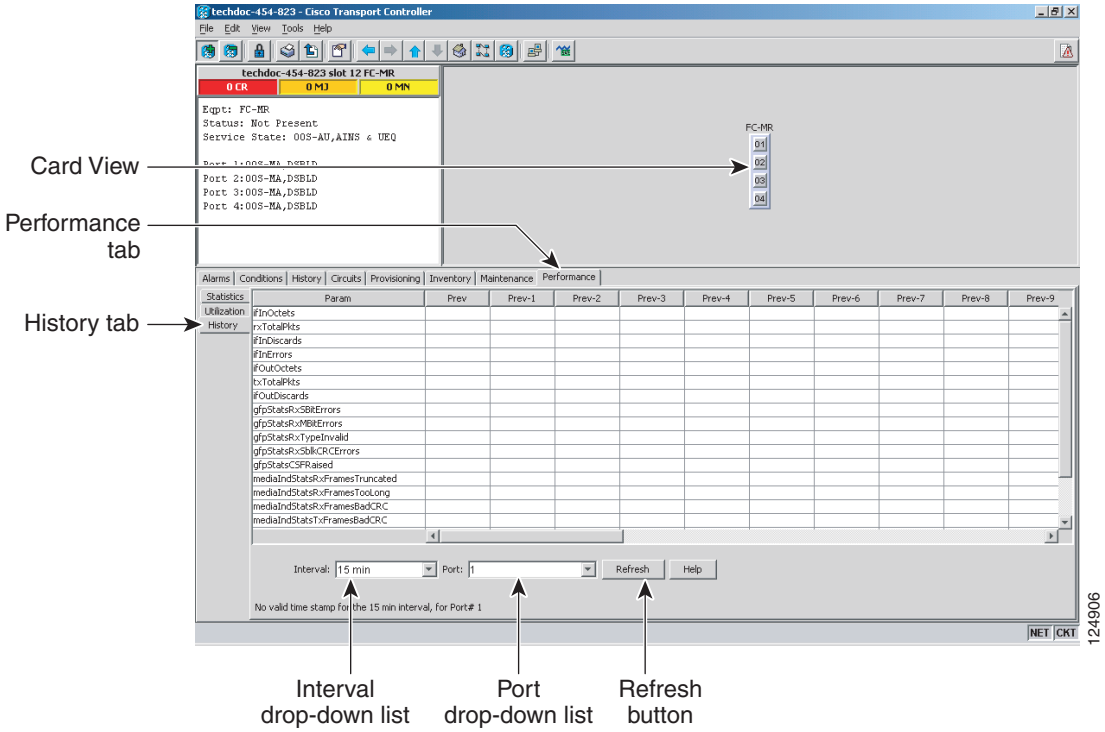
DLP-A352 View FC_MR-4 History PM Parameters

Purpose	This task enables you to view historical PM counts at selected time intervals on an FC_MR-4 card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the FC_MR-4 card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **History** tabs (Figure 20-8).

Figure 20-8 FC_MR-4 History on the Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Prev-*n* columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 5 Return to your originating procedure (NTP).

DLP-A353 Refresh FC_MR-4 PM Counts at a Different Time Interval

Purpose	This task changes the window view to display specified PM counts in time intervals depending on the interval option selected.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the FC_MR-4 card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Utilization** or the **History** tab.

Step 4 From the Interval drop-down list, choose one of four options:

- **1 min**: This option appears the specified PM counts in one-minute time intervals.
- **15 min**: This option appears the specified PM counts in 15-minute time intervals.
- **1 hour**: This option appears the specified PM counts in one-hour time intervals.
- **1 day**: This option appears the specified PM counts in one-day (24 hours) time intervals.

Step 5 Click **Refresh**. The PM counts refresh with values based on the selected time interval.

Step 6 Return to your originating procedure (NTP).

DLP-A356 TCC2/TCC2P Card Active/Standby Switch Test

Purpose	This task verifies that the TCC2/TCC2P cards can effectively switch from one to another.
Tools/Equipment	The test set specified by the acceptance test procedure, connected and configured as specified in the acceptance test procedure.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 3 Click the **Conditions** tab. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 4 On the network map, double-click the node containing the TCC2/TCC2P cards you are testing to open it in node view.

Step 5 Make a note of which TCC2/TCC2P card is active and which is standby by examining the LEDs on the shelf graphic. TCC2/TCC2P cards are installed in Slot 7 and Slot 11. The active TCC2/TCC2P card has a green ACT LED, and the standby TCC2/TCC2P card has an amber SBY LED.

Step 6 On the shelf graphic, right-click the active TCC2/TCC2P card and choose **Reset** from the shortcut menu.

Step 7 In the Resetting Card dialog box, click **Yes**. After 20 to 40 seconds, a "lost node connection, changing to network view" message appears. On the network view map, the node where you reset the TCC2/TCC2P card will be gray.

Step 8 After the node icon becomes available (within 1 to 2 minutes), double-click it. On the shelf graphic, observe the following:

- The previous standby TCC2/TCC2P card has a green ACT LED.
- The previous active TCC2/TCC2P card LEDs go through the following LED sequence: NP (card not present), Ldg (software is loading), amber SBY LED (TCC2/TCC2P is in standby mode).

Step 9 Verify that traffic on the test set connected to the node is still running. If a traffic interruption occurs, do not continue, refer to your next level of support.

Step 10 Repeat Steps 2 through 9 to return the active/standby TCC2/TCC2P cards to their configuration at the start of the procedure.

Step 11 Verify that the TCC2/TCC2P cards appear as noted in Step 5.

Step 12 Return to your originating procedure (NTP).

DLP-A357 Create FC_MR-4 RMON Alarm Thresholds

Purpose	This task sets up remote monitoring (RMON) to allow network management systems to monitor FC_MR-4 ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 at the node where you want to set up RMON
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 In node view, double-click the FC_MR-4 card where you want to create the RMON alarm thresholds.

Step 2 Click the **Provisioning > RMON Thresholds** tabs.

Step 3 Click **Create**. The Create Threshold dialog box appears.

Step 4 From the Slot drop-down list, choose the appropriate FC_MR-4 card.

Step 5 From the Port drop-down list, choose the applicable port on the FC_MR-4 card you selected.

Step 6 From the Variable drop-down list, choose the variable. See Table 20-1 for a list of the FC_MR-4 threshold variables available in this field.

Table 20-1 FC_MR-4 Threshold Variables Fibre Channel/FICON Line Rate Mode (MIBs)

Variable	Definition
iflnOctets	Total number of octets received on the interface, including framing octets.
ifInDiscards	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.
iflnErrors	Number of inbound packets discarded because they contain errors.
ifOutOctets	Total number of transmitted octets, including framing packets.
ifOutDiscards	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted.
txTotalPkts	Total number of transmit packets.
rxTotalPkts	Total number of receive packets.
fibreStatsInvalidOrderedSets	Received ordered sets that are not recognized as part of the defined Fibre Channel control words.
fibreStatsEncodingDispErrors	Received control words that cannot be decoded due to invalid disparity.
fibreStatsRxFramesTooLong	Received oversize Fibre Channel frames > 2148 including cyclic redundancy check (CRC).
fibreStatsRxFramesBadCRC	Received Fibre Channel frames with bad CRC.
fibreStatsRxFrames	Received total Fibre Channel frames.
fibreStatsRxOctets	Received total Fibre Channel data bytes within a frame.
fibreStatsTxFramesBadCRC	Transmitted Fibre Channel frames with bad CRC.
fibreStatsTxFrames	Transmitted total Fibre Channel frames.
fibreStatsTxOctets	Transmitted total Fibre Channel data bytes within a frame.
fibreStatsLinkResets	Total number of link resets initiated by an FCMR port when the link recovery port setting is enabled.
gfpStatsRxSBitErrors	Received generic framing protocol (GFP) frames with single bit errors in the core header (these errors are correctable).
gfpStatsRxMBitErrors	Received GFP frames with multiple bit errors in the core header (these errors are not correctable).
gfpStatsRxTypeInvalid	Received GFP frames with invalid type (these are discarded). For example, receiving GFP frames that contain Ethernet data when we expect Fibre Channel data.
gfpStatsRxSblkCRCErrors	Total number of superblock CRC errors with the receive transparent GFP frame. A transparent GFP frame has multiple superblocks which each contain Fibre Channel data.
gfpStatsCSFRaised	Number of Rx client management frames with Client Signal Fail indication.

Table 20-1 FC_MR-4 Threshold Variables Fibre Channel/FICON Line Rate Mode (MIBs) (continued)

Variable	Definition
mediaIndStatsTxFramesTooLong	Number of packets transmitted that are greater than 1548 bytes
mediaIndStatsRxFramesTruncated	Total number of frames received that are less than 5 bytes

Table 20-2 lists the enhanced mode MIBs available.

Table 20-2 FC_MR-4 Threshold Variables Fiber Channel/FICON Enhanced Mode (MIBs)

Variable	Definition
iflnOctets	Total number of octets received on the interface, including framing octets.
ifInDiscards	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.
iflnErrors	Number of inbound packets discarded because they contain errors.
ifOutOctets	Total number of transmitted octets, including framing packets.
ifOutDiscards	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted.
fcIngressRxDistanceExtBuffers	The maximum number of GFP buffers that are available at the GFP receiver.
fcEgressTxDistanceExtBuffers	The number of GFP buffers that the GFP transmitter is allowed to transmit. Remote GFP receiver tells the GFP transmitter how many buffers it has available.
fcStatsLinkRecoveries	The number of times a link reset was initiated due to a GFP out of frame condition. This is only valid when link recovery is enabled and is not valid when distance extension is enabled.
fcStatsRxCredits	The maximum number of Fibre Channel credits that the Fibre Channel/fiber connectivity (FICON) link partner will allow the FCMR Fibre Channel/FICON transmitter to transmit. (The maximum number of frames the link partner can receive.)
fcStatsTxCredits	The number of Fibre Channel credits that the FCMR Fibre Channel/FICON transmitter is left with. This is the number of frames that the Fibre Channel/FICON transmitter has available to send. **Note** The Tx credits increment whenever a credit is received from the link partner, and decrement when a frame is sent.
fcStatsZeroTxCredits	This is a count that increments when the Fibre Channel/FICON Tx credits go from a non-zero value to zero.
fibreStatsInvalidOrderedSets	Received ordered sets that are not recognized as part of the defined Fibre Channel control words.
fibreStatsEncodingDispErrors	Received control words that cannot be decoded due to invalid disparity.

Table 20-2 FC_MR-4 Threshold Variables Fiber Channel/FICON Enhanced Mode (MIBs) (continued)

Variable	Definition
fibreStatsRxFramesTooLong	Received oversize Fibre Channel frames > 2148 including CRC.
fibreStatsRxFramesBadCRC	Received Fibre Channel frames with bad CRC.
fibreStatsRxFrames	Received total Fibre Channel frames.
fibreStatsRxOctets	Received total Fibre Channel data bytes within a frame.
fibreStatsTxFramesBadCRC	Transmitted Fibre Channel frames with bad CRC.
fibreStatsTxFrames	Transmitted total Fibre Channel frames.
fibreStatsTxOctets	Transmitted total Fibre Channel data bytes within a frame.
fibreStatsLinkResets	Total number of link resets initiated by FCMR port when link recovery port setting is enabled.
gfpStatsRxSBitErrors	Received GFP frames with single bit errors in the core header (these errors are correctable).
gfpStatsRxMBitErrors	Received GFP frames with multiple bit errors in the core header (these errors are not correctable).
gfpStatsRxTypeInvalid	Received GFP frames with invalid type (these are discarded). For example, receiving GFP frames that contain Ethernet data when we expect Fibre Channel data.
gfpStatsRxSblkCRCErrors	Total number of superblock CRC errors with the receive transparent GFP frame. A transparent GFP frame has multiple superblocks which each contain Fibre Channel data.
8b10bInvalidOrderedSets	Total number of ordered sets not complaint to GE/FC (Gigabit Ethernet/Fibre Channel) standard
8b10bStatsEncodingDispErrors	Total number of code groups that violate GE/FC disparity errors

Step 7 From the Alarm Type drop-down list, indicate whether the event will be triggered by the rising threshold, falling threshold, or both the rising and falling thresholds.

Step 8 From the Sample Type drop-down list, choose either **Relative** or **Absolute**. Relative restricts the threshold to use the number of occurrences in the user-set sample period. Absolute sets the threshold to use the total number of occurrences, regardless of time period.

Step 9 Type in an appropriate number of seconds for the Sample Period field.

Step 10 Type in the appropriate number of occurrences for the Rising Threshold field.

For a rising type of alarm, the measured value must move from below the falling threshold to above the rising threshold. For example, if a network is running below a rising threshold of 1000 collisions every 15 minutes and a problem causes 1001 collisions in 15 minutes, the excess occurrences trigger an alarm.

Step 11 Enter the appropriate number of occurrences in the Falling Threshold field. In most cases a falling threshold is set lower than the rising threshold.

A falling threshold is the counterpart to a rising threshold. When the number of occurrences is above the rising threshold and then drops below a falling threshold, it resets the rising threshold. For example, when the network problem that caused 1001 collisions in 15 minutes subsides and creates only 799 collisions in 15 minutes, occurrences fall below a falling threshold of 800 collisions. This resets the rising threshold so that if network collisions again spike over a 1000 per 15-minute period, an event again

triggers when the rising threshold is crossed. An event is triggered only the first time a rising threshold is exceeded (otherwise, a single network problem might cause a rising threshold to be exceeded multiple times and cause a flood of events).

Step 12 Click **OK**.

Step 13 Return to your originating procedure (NTP).

DLP-A358 Delete FC_MR-4 RMON Alarm Thresholds

Purpose	This task deletes RMON threshold crossing alarms for FC_MR-4 ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A357 Create FC_MR-4 RMON Alarm Thresholds, page 20-41 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the FC_MR-4 card where you want to delete the RMON alarm thresholds.

Step 2 Click the **Provisioning > RMON Thresholds** tabs.

Step 3 Click the RMON alarm threshold that you want to delete.

Step 4 Click **Delete**. The Delete Threshold dialog box appears.

Step 5 Click **Yes** to delete the threshold.

Step 6 Return to your originating procedure (NTP).

DLP-A359 Delete a Line DCC Termination

Purpose	This task deletes a SONET LDCC termination on the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Deleting a DCC termination can cause you to lose visibility of nodes that do not have other DCCs or network connections to the CTC computer.

Step 1 Click the **Provisioning > Comm Channel > LDCC** tabs.

Step 2 Click the LDCC termination to be deleted and click **Delete**. The Delete LDCC Termination dialog box appears.

Step 3 Click **Yes** in the confirmation dialog box. Confirm that the changes appear; if not, repeat the task.

Step 4 Return to your originating procedure (NTP).

DLP-A362 Create a Four-Fiber BLSR Using the BLSR Wizard

Purpose	This task creates a four-fiber BLSR at each BLSR-provisioned node using the CTC BLSR wizard. The BLSR wizard checks to see that each node is ready for BLSR provisioning, then provisions all the nodes at one time.
Tools/Equipment	None
Prerequisite Procedures	NTP-A40 Provision BLSR Nodes, page 5-10 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click **Create BLSR**.

Step 4 In the BLSR Creation dialog box, set the BLSR properties:

- Ring Type—Choose four-fiber.
- Speed—Choose the BLSR ring speed: OC-48 or OC-192. The speed must match the OC-N speed of the BLSR trunk (span) cards.
- Ring Name—Assign a ring name. The name can be from 1 to 6 characters in length. Any alphanumeric string is permissible, and upper and lower case letters can be combined. Do not use the character string “All” in either upper or lower case letters; this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.
- Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path following a ring switch. The default is 5 minutes. Ring reversion can be set to Never.
- Span Reversion—Set the amount of time that will pass before the traffic reverts to the original working path following a span switch. The default is 5 minutes. Span reversion can be set to Never.

Step 5 Click **Next**. If the network graphic appears, go to Step 6.

If CTC determines that a BLSR cannot be created, for example, not enough optical cards are installed or it finds circuits with path protection selectors, a “Cannot Create BLSR” message appears. If this occurs, complete the following steps:

a. Click **OK**.

b. In the Create BLSR window, click **Excluded Nodes**. Review the information explaining why the BLSR could not be created, then click **OK**.

c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.

d. Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 5-10, making sure all steps are completed accurately, then start this procedure again.

Step 6 In the network graphic, double-click a BLSR span line. If the span line is DCC connected to other BLSR cards that constitute a complete ring, the lines turn blue. If the lines do not form a complete ring, double-click span lines until a complete ring is formed. When the ring is DCC connected, go to Step 7.

Step 7 Click **Next**. In the Protect Port Selection section, choose the protect ports from the West Protect and East Protect columns.

Step 8 Click **Finish**. If the BLSR window appears with the BLSR you created, go to Step 9. If a "Cannot Create BLSR" or "Error While Creating BLSR" message appears:

a. Click **OK**.

b. In the Create BLSR window, click **Excluded Nodes.** Review the information explaining why the BLSR could not be created, then click **OK**.

c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.

d. Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 5-10, making sure all steps are completed accurately, then start this procedure again.

Note Some or all of the following alarms might briefly appear during BLSR setup: E-W-MISMATCH, RING-MISMATCH, APSCIMP, APSCDFLTK, and BLSROSYNC.

Step 9 Verify the following:

- On the network view graphic, a green span line appears between all BLSR nodes.
- All E-W-MISMATCH, RING-MISMATCH, APSCIMP, APSCDFLTK, and BLSROSYNC alarms are cleared. See the *Cisco ONS 15454 Troubleshooting Guide* for alarm troubleshooting.

Note The numbers in parentheses after the node name are the BLSR node IDs assigned by CTC. Every ONS 15454 in a BLSR is given a unique node ID, 0 through 31. To change it, complete the "DLP-A326 Change a BLSR Node ID" task on page 20-16.

Step 10 Return to your originating procedure (NTP).

DLP-A363 Create a Four-Fiber BLSR Manually

Purpose	This tasks creates a four-fiber BLSR at each BLSR-provisioned node without using the BLSR wizard.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > BLSR** tabs.

Step 2 Click **Create**.

Step 3 In the Suggestion dialog box, click **OK**.

Step 4 In the Create BLSR dialog box, set the BLSR properties:

- Ring Type—Choose four-fiber.
- Ring Name—Assign a ring name. You must use the same ring name for each node in the BLSR. Any alphanumeric character string is permissible, and upper and lower case letters can be combined. Do not use the character string "All" in either upper or lower case letters; this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.
- Node ID—Choose a Node ID from the drop-down list (0 through 31). The Node ID identifies the node to the BLSR. Nodes in the same BLSR must have unique Node IDs.
- Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path. The default is 5 minutes. All nodes in a BLSR must have the same reversion time setting.
- West Line—Assign the west BLSR port for the node from the drop-down list.

  The east and west ports must match the fiber connections and DCC terminations set up in the "NTP-A40 Provision BLSR Nodes" procedure on page 5-10.
- East Line—Assign the east BLSR port for the node from the drop-down list.
- Span Reversion—Set the amount of time that will pass before the traffic reverts to the original working path following a span reversion. The default is 5 minutes. Span reversion can be set to Never. If you set a reversion time, the times must be the same for both ends of the span. That is, if Node A's west fiber is connected to Node B's east port, the Node A west span reversion time must be the same as the Node B east span reversion time. To avoid reversion time mismatches, Cisco recommends that you use the same span reversion time throughout the ring.
- West Protect—Assign the west BLSR port that will connect to the west protect fiber from the drop-down list.
- East Protect—Assign the east BLSR port that will connect to the east protect fiber from the drop-down list.

Step 5 Click **OK**.

Note Some or all of the following alarms will appear until all the BLSR nodes are provisioned: E-W-MISMATCH, RING-MISMATCH, APSCIMP, APSCDFLTK, and BLSROSYNC. The alarms will clear after you configure all the nodes in the BLSR.

Step 6 From the View menu, choose **Go to Other Node**.

Step 7 In the Select Node dialog box, choose the next node that you want to add to the BLSR.

Step 8 Repeat Steps 1 through 7 at each node that you want to add to the BLSR. When all nodes have been added, continue with Step 9.

Step 9 From the View menu, choose **Go to Network View**. After 10 to 15 seconds, verify the following:

- A green span line appears between all BLSR nodes.
- All E-W-MISMATCH, RING-MISMATCH, APSCIMP, APSCDFLTK, and BLSROSYNC alarms are cleared.

Step 10 Return to your originating procedure (NTP).

DLP-A364 Reset the TCC2/TCC2P Card Using CTC

Purpose	This task resets the TCC2/TCC2P card and switches the node to the redundant card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A36 Install the TCC2/TCC2P Cards, page 17-37
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Note Before you reset the TCC2/TCC2P, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Note When a software reset is performed on an active TCC2/TCC2P, the AIC-I card goes through an initialization process and also resets. The AIC-I card reset is normal and happens each time an active TCC2/TCC2P card goes through a software-initiated reset.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to reset the TCC2/TCC2P card. If you are already logged in, continue with Step 2.

Step 2 In node view, right-click the TCC2/TCC2P card to reveal a shortcut menu.

Step 3 Click **Reset Card**.

Step 4 Click **Yes** when the confirmation dialog box appears.

Step 5 Click **OK** when the "Lost connection to node, changing to Network View" dialog box appears.

Note For LED behavior during a TCC2/TCC2P reboot, see Table 19-2 on page 19-34.

Step 6 Confirm that the TCC2/TCC2P card LED is amber (standby).

Step 7 Return to your originating procedure (NTP).

DLP-A365 Initiate an Optical Protection Switch

Purpose	This procedure explains how to initiate a Manual or Force switch on an optical port.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, select the protection group you want to switch.

Step 3 In the Selected Group area, select the card and port you want to switch.

Step 4 Click **Manual** or **Force**.

If you choose a Manual switch, the command will switch traffic only if the path has an error rate less than the signal degrade bit error rate threshold. A Force switch will switch traffic even if the path has SD or SF conditions; however, a Force switch will not override an SF on a 1+1 protection channel A Force switch has a higher priority than a Manual switch.

Step 5 In the confirmation dialog box, click **Yes**.

Step 6 Return to your originating procedure (NTP).

DLP-A366 Initiate an Electrical Protection Switch

Purpose	This task explains how to initiate a traffic witch on an electrical card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Note A user-initiated switch overrides the revertive delay, that is, when you clear a switch you clear the timer and traffic reverts immediately.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, select the protection group you want to switch.

Step 3 In the Selected Group area, select the card you want to switch.

Step 4 Click **Switch**.

Step 5 In the confirmation dialog box, click **Yes**.

Step 6 Return to your originating procedure (NTP).

DLP-A367 Create a Provisionable Patchcord

Purpose	This task creates a provisionable patchcord, which is a user-provisioned link that is advertised by OSPF throughout the network.Provisionable patchcords appear as dashed lines in CTC network view. For the specific situations in which a patchcord is necessary, refer to the *Cisco ONS 15454 Reference Manual*.
Tools/Equipment	OC-N, transponder/muxponder, optical add/drop multiplexer, and multiplexer/demultiplexer cards. For the card combinations that support patchcords, refer to the *Cisco ONS 15454 Reference Manual*.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

Note To set up a provisionable patchcord between an optical port and a transponder/muxponder, optical add/drop multiplexer, or multiplexer/demultiplexer port, the optical port must have an SDCC/LDCC termination provisioned. If the port is the protection port in a 1+1 group, the working port must have an SDCC/LDCC termination provisioned. As needed, complete the "DLP-A377 Provision Section DCC Terminations" task on page 20-69 or the "DLP-A378 Provision Line DCC Terminations" task on page 20-71.

Note An optical port requires two patchcords when the remote end is Y-cable protected or is an optical add/drop multiplexer or multiplexer/demultiplexer port.

Note An optical patchcord must be provisioned between an OCH filter and an OCH trunk port.

Note If a provisionable patchcord is created manually by CTC, it automatically tunes the TXP or MXP trunk as an OCH filter if the TXP or MXP is set to autoprovisioning at the first tunable wavelength. On the TL1 interface, this feature is supported for internal patchcords only (OPR-LNK).

Step 1 In node view, click the **Provisioning > Comm Channels > Provisionable Patchcords** tabs. If you are in network view, click the **Provisioning > Provisionable Patchcords** tabs.

Step 2 Click **Create**. The Provisionable Patchcord dialog box appears.

Step 3 In the Origination Node area, complete the following:

a. If you are in node view, the Origination Node defaults to the current node. If you are in network view, click the desired origination node from the drop-down list.

b. Type a patchcord identifier (0 through 32767) in the TX/RX ID field.

c. Click the desired origination slot/port from the list of available slots/ports.

Step 4 In the Termination Node area, complete the following:

a. Click the desired termination node from the drop-down list. If the remote node has not previously been discovered by CTC but is accessible by CTC, type the name of the remote node.

b. Type a patchcord identifier (0 through 32767) in the TX/RX ID field. The origination and termination IDs must be different if the patchcord is set up between two cards on the same node.

c. Click the desired termination slot/port from the list of available slots/ports. The origination port and the termination port must be different.

Step 5 If you need to provision Tx and Rx separately for multiplexer/demultiplexer cards, check the **Separate Tx/Rx** check box. If not, continue with Step 6. The origination and termination TX ports are already provisioned. Complete the following to provision the RX ports:

a. In the Origination Node area, type a patchcord identifier (0 through 32767) in the RX ID field. The origination Tx and Rx and termination Tx and Rx IDs must be different.

b. Click the desired origination slot/port from the list of available slots/ports.

c. In the Termination Node area, type a patchcord identifier (0 through 32767) in the RX ID field. The origination Tx and Rx and termination Tx and Rx IDs must be different.

d. Click the desired termination slot/port from the list of available slots/ports.

Step 6 Click **OK**.

Step 7 If you provisioned a patchcord on a port in a 1+1 protection group, a dialog box appears to ask if you would like to provision the peer patchcord. Click **Yes**. Repeat Steps 3 through 6.

Step 8 Return to your originating procedure (NTP).

DLP-A368 Delete a Provisionable Patchcord

Purpose	This task deletes a provisionable patchcord.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

Note Deleting the last DCC termination on an optical port automatically deletes all provisionable patchcords provisioned on the port. If the port is in a 1+1 protection group, CTC automatically deletes the patchcord link on the protection port.

Step 1 In node view, click the **Provisioning > Comm Channels > Provisionable Patchcords** tabs. If you are in network view, click the **Provisioning > Provisionable Patchcords** tabs.

Step 2 Click the provisionable patchcord that you want to delete.

Step 3 Click **Delete**.

Step 4 In the confirmation dialog box, click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-A369 Provision an OC-N Circuit Route

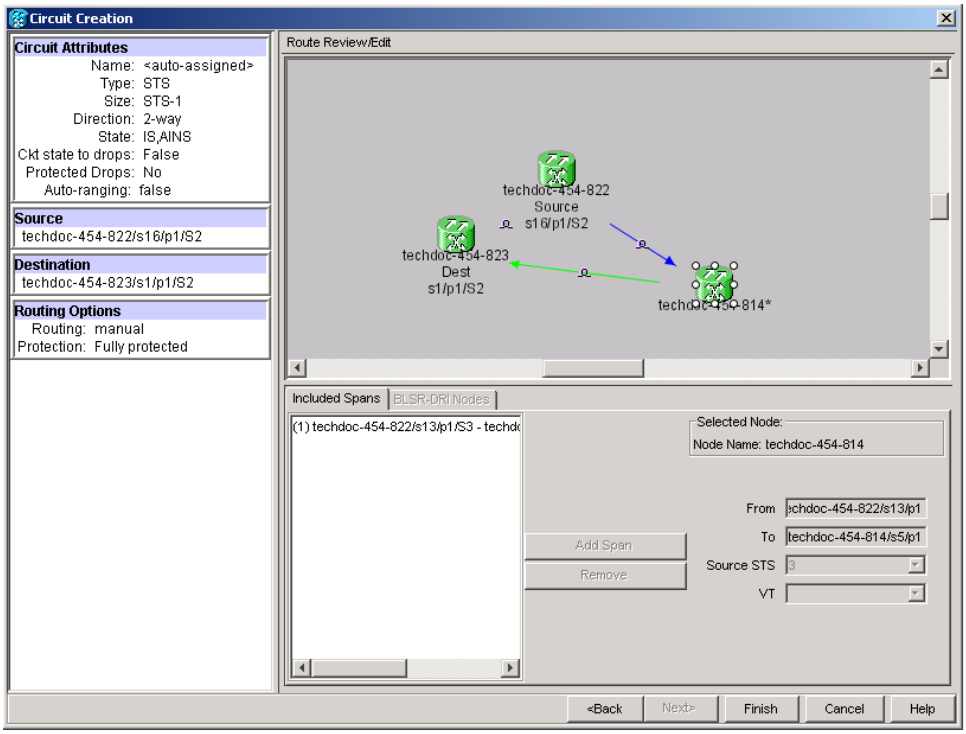
Purpose	This task provisions the circuit route for manually routed OC-N circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 The Circuit Creation wizard, Route Review/Edit area, must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the Circuit Creation wizard in the Route Review/Edit area, click the source node icon if it is not already selected.

Step 2 Starting with a span on the source node, click the arrow of the span you want the circuit to travel. To reverse the direction of the arrow, click the arrow twice.

The arrow turns yellow. In the Selected Span area, the From and To fields provide span information. The source STS appears. Figure 20-9 shows an example of a manually routed circuit.

Figure 20-9 Manually Routing an OC-N Circuit



Step 3 If you want to change the source STS, adjust the Source STS field; otherwise, continue with Step 4.

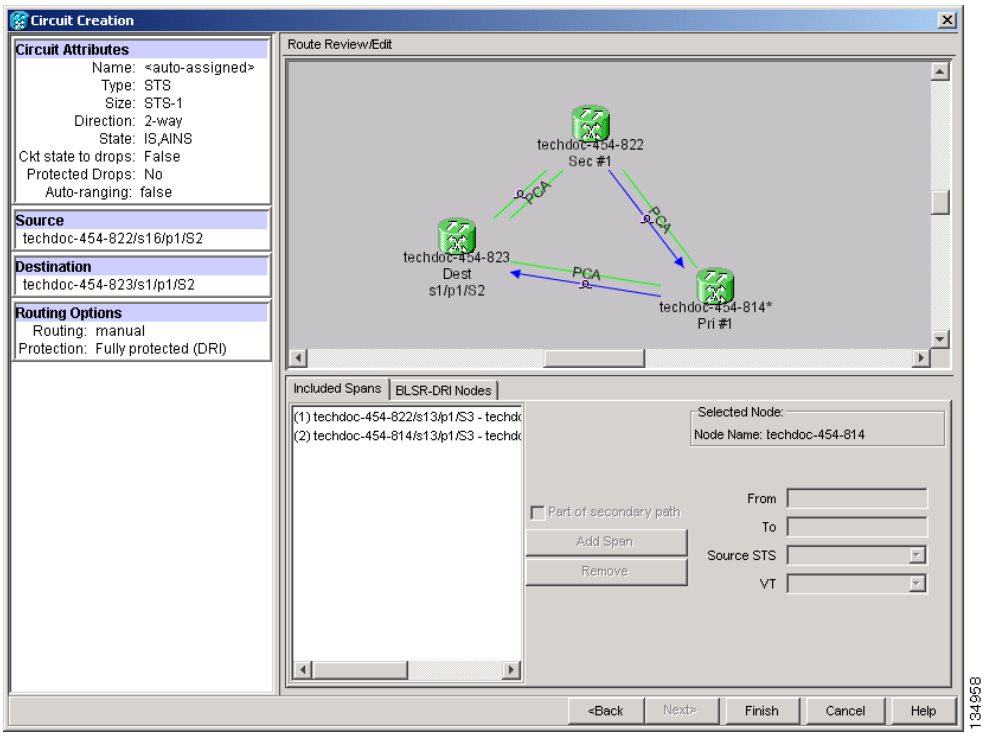
Note The VT option is disabled for OC-N circuits.

Step 4 Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

Step 5 Repeat Steps 2 through 4 until the circuit is provisioned from the source to the destination node through all intermediary nodes. If Fully Protected Path is checked in the Circuit Routing Preferences page, you must:

- Add two spans for all path protection or unprotected portions of the circuit route from the source to the destination.
- Add one span for all BLSR or 1+1 portions of route from the source to the destination.
- Add primary spans for BLSR-DRI from the source to the destination through the primary nodes, and then add spans through the secondary nodes as an alternative route. Figure 20-10 shows an example of a manually routed BLSR DRI circuit. PCA spans can only be chosen as part of the secondary path.

Figure 20-10 Manually Routing a BLSR DRI Circuit Route



Step 6 Return to your originating procedure (NTP).

DLP-A371 Remove Pass-through Connections

Purpose	This task removes pass-through connections from a node deleted from a ring.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into the deleted node.

Step 2 In the CTC Login dialog box, check the **Disable Network Discovery** check box.

Step 3 Choose **None** from the Additional Nodes drop-down list.

Step 4 Click the **Login** button.

Step 5 Click the **Circuits** tab. All internode circuits are shown as PARTIAL.

Step 6 Refer to the diagram or CTC print out you created in the "NTP-A240 Remove a BLSR Node" procedure on page 14-7 or the "NTP-A294 Remove a Path Protection Node" procedure on page 14-13. Find the circuits on the line cards of the removed node.

Step 7 Click the **Filter** button.

Step 8 Type the slot and port of a trunk card on the removed node.

Step 9 Click **OK**.

Step 10 In the Circuits tab, select all PARTIAL circuits that pass the filter and click the **Delete** button.

Note To select more than one circuit, press the **Shift** key and simultaneously click on all circuits to be deleted.

Step 11 Repeat Steps 6 through 10 for the other trunk card.

Step 12 Log out of CTC.

Step 13 Return to your originating procedure (NTP).

DLP-A372 Delete a Node from a Specified Login Node Group

Purpose	This task removes a node from a specified login node group. To remove a node from the current login node group, see the "DLP-A339 Delete a Node from the Current Session or Login Group" task on page 20-31.
Tools	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the CTC Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **Login Node Groups** tab.

Step 3 Click the login node group tab containing the node you want to remove.

Step 4 Click the node you want to remove, then click **Remove**.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-A373 Install a MiniBNC EIA

Purpose	This task installs a MiniBNC EIA. You can use MiniBNC EIAs with DS-1, DS-3, or DS3XM cards.
Tools/Equipment	#2 Phillips screwdriver Small slot-head screwdriver 6 perimeter screws, 6-32 x 0.375-inch Phillips head (P/N 48-0422-01) MiniBNC, A side (15454-xxxx) EIA panel and/or MiniBNC, B side (15454-xxx) EIA panel
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution Always use an electrostatic discharge (ESD) wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Note MiniBNC EIAs can only be installed on shelf assembly 15454-SA-HD. 15454-SA-HD shelf assemblies are differentiated from other shelf assemblies by the blue hexagon symbol, which indicates the available high-density slots, found under Slots 1 through 3 and 15 through 17.

Note MiniBNC or UBIC EIAs are required when using high-density (48-port DS-3 and DS3XM-12) electrical cards.

Step 1 Locate the correct MiniBNC EIA for the side you want to install, and remove the MiniBNC EIA from the packaging.

Step 2 Verify that none of the pins on the MiniBNC EIA are bent.

Step 3 If present, remove the yellow connector protectors.

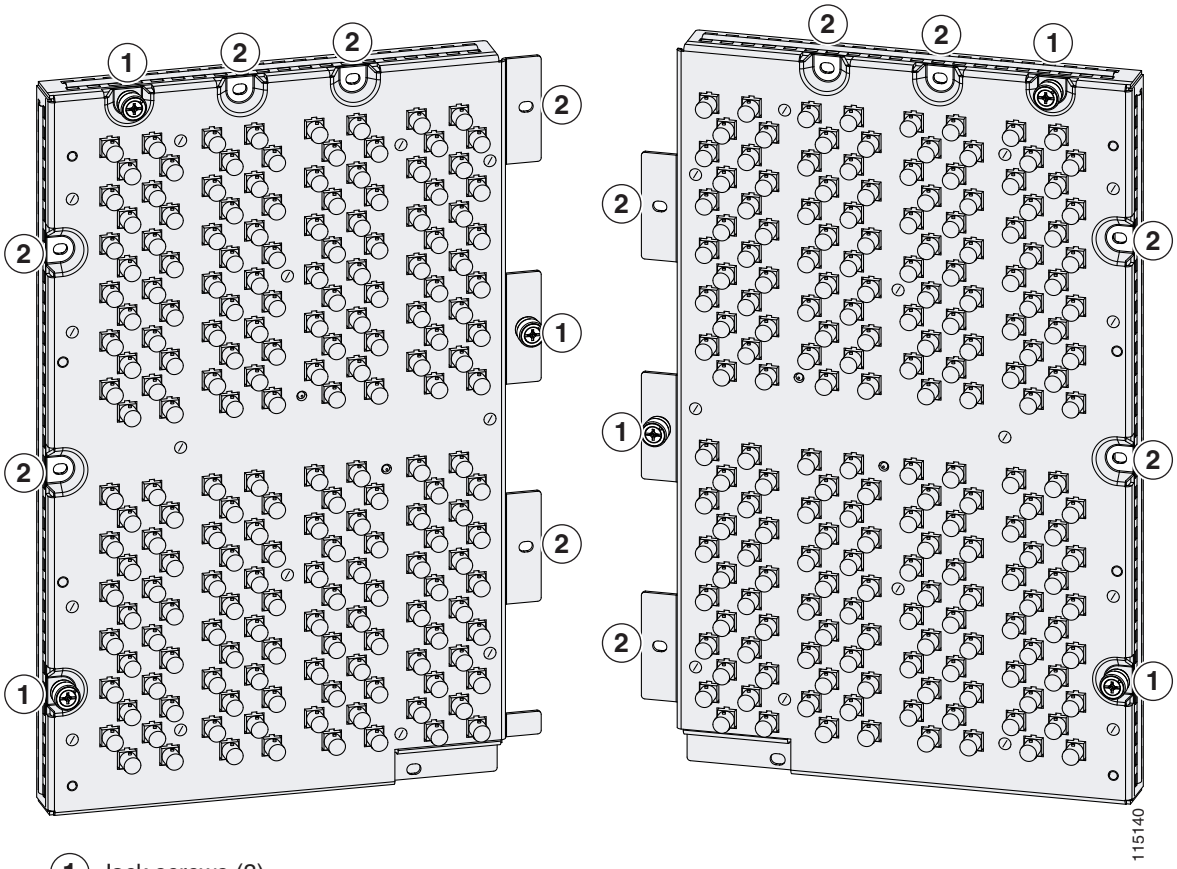
Step 4 Line up the connectors on the card with the mating connectors on the backplane, making sure the keys on the back of the card line up properly with the backplane. Push the card with consistent pressure until the connectors fit together firmly.

Caution Do not force the MiniBNC EIA onto the backplane if you feel strong resistance. Make sure that the MinBNC EIA lines up properly on the backplane and that no backplane pins are bent.

Step 5 Locate the three jack screws on the MiniBNC (Figure 20-11). Starting with any thumbscrew, tighten it a few turns and move to the next one, turning each thumbscrew a few turns at a time until all three screws are hand tight (Figure 20-12).

Caution Tightening the jack screws unevenly could cause damage to the MiniBNC connectors.

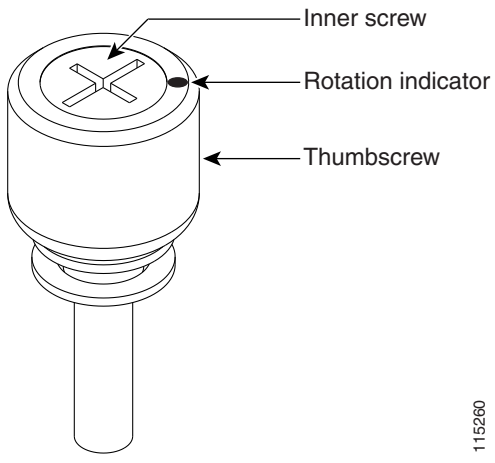
Figure 20-11 MiniBNC EIA Screw Locations



1 Jack screws (3)

2 Perimeter screws, 6-32 x 0.375-inch Phillips head (6)

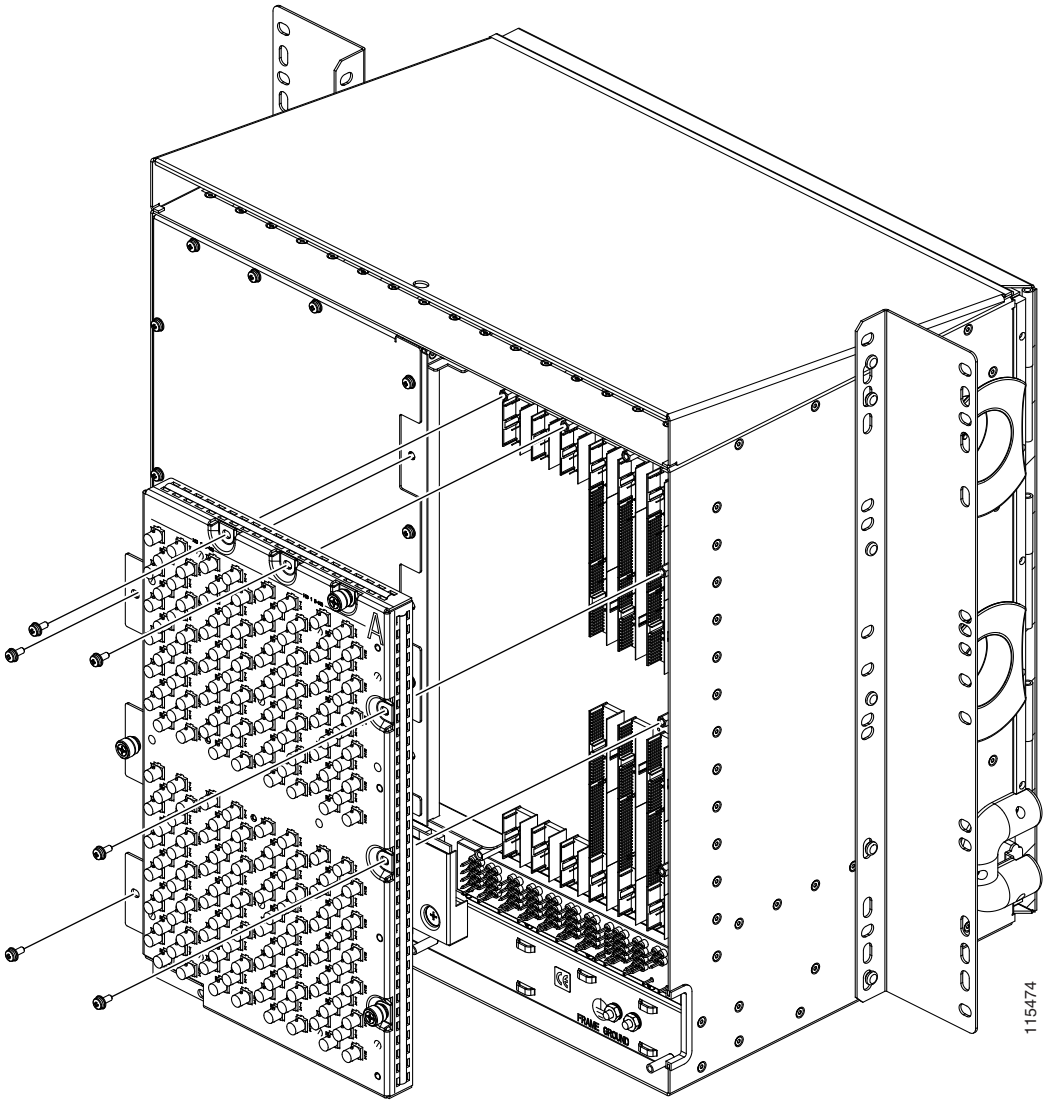
Figure 20-12 MiniBNC EIA Jack Screw



Step 6 Use a Phillips screwdriver to install the six perimeter screws and bracket screws (P/N 48-0422-01) at 8 to 10 lbf-inch (9.2 to 11.5 kgf-cm) to secure the cover panel to the backplane (Figure 20-11 on page 20-58). Install the alarm and timing panel cover and then insert and tighten the last perimeter screw.

Figure 20-13 shows a MiniBNC EIA installation.

Figure 20-13 Installing the MiniBNC EIA



Step 7 Return to your originating procedure (NTP).

DLP-A374 Change a Section DCC Termination

Purpose	This task modifies an SDCC. You can enable or disable Open Shortest Path First (OSPF) and enable or disable the foreign node setting.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	Provisioning or higher

Step 1 Click the **Provisioning > Comm Channels > SDCC** tabs.

Step 2 Click the SDCC that you want to change.

Step 3 Click **Edit**.

Step 4 In the SDCC Termination Editor dialog box, complete the following as necessary:

- Disable OSPF on SDCC Link—If checked, OSPF is disabled on the link. OSPF should be disabled only when the slot and port connect to third-party equipment that does not support OSPF.
- Far End is Foreign—Check this box to specify that the SDCC termination is a non-ONS node.
- Far End IP—If you checked the Far End is Foreign check box, type the IP address of the far-end node or leave the 0.0.0.0 default. An IP address of 0.0.0.0 means that any address can be used by the far end.

Step 5 Click **OK**.

Step 6 Return to your origination procedure (NTP).

DLP-A375 Change a Line DCC Termination

Purpose	This task modifies an LDCC. You can enable or disable OSPF and enable or disable the foreign node setting.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	Provisioning or higher

Step 1 Click the **Provisioning > Comm Channels > LDCC** tabs.

Step 2 Click the LDCC that you want to change.

Step 3 Click **Edit**.

Step 4 In the LDCC Termination Editor dialog box, complete the following as necessary:

- Disable OSPF on LDCC Link—If checked, OSPF is disabled on the link. OSPF should be disabled only when the slot and port connect to third-party equipment that does not support OSPF.

- Far End is Foreign—Check this box to specify that the LDCC termination is a non-ONS node.
- Far end IP—If you checked the Far End is Foreign check box, type the IP address of the far-end node or leave the 0.0.0.0 default. An IP address of 0.0.0.0 means that any address can be used by the far end.

Step 5 Click **OK**.

Step 6 Return to your origination procedure (NTP).

DLP-A376 Change Line and Threshold Settings for the DS1/E1-56 Cards

Purpose	This task changes the line and threshold settings for the DS1/E1-56 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 Double-click the DS1/E1-56 card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line**, **Line Thresholds**, **Elect Path Thresholds**, **SONET Thresholds**, **or Cards** tab.

Note See Chapter 8, "Manage Alarms" for information about the Alarm Profiles tab.

Note If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 4 Modify the settings found under these subtabs by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

For definitions of the line settings, see Table 20-3. For definitions of the line threshold settings, see Table 20-4 on page 20-65. For definitions of the electrical path threshold settings, see Table 20-5 on page 20-66. For definitions of the SONET threshold settings, see Table 20-6 on page 20-66. For definitions of the card settings, see Table 20-7 on page 20-67.

Table 20-3 describes the values on the Provisioning > Line tabs for the DS1/E1-56 cards.

Table 20-3 Line Options for the DS1/E1-56 Card

Parameter	Description	Options
Port	(Display only) Port number.	1 to 56
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 20-8.
Admin State	Sets the port service state unless network conditions prevent the change.	• IS—Puts the port in-service. The port service state changes to IS-NR. • IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. • OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. • OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT. **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.

Table 20-3 Line Options for the DS1/E1-56 Card (continued)

Parameter	Description	Options
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—The port is fully operational and performing as provisioned. • OOS-AU,AINS—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic. • OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Line Type	Defines the line framing type.	For DS1 mode • Unframed - default • J_ESF • ESF • D4 • Auto Frame For E1 mode • Auto Frame • Unframed • E1_MF • E1_CRCMF

Table 20-3 Line Options for the DS1/E1-56 Card (continued)

Parameter	Description	Options
Line Coding	Defines the transmission coding type that is used.	For DS1 mode • B8ZS • AMI For E1 mode • HDB3
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 131 (default) • 132 - 262 • 263 - 393 • 394 - 524 • 525 - 655
AINS Soak	Sets the automatic in-service soak period.	Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically. Value ranges from 0 to 48 hours in 15-minute increments.
FDL Mode	Sets the mode for far-end loopbacks and far-end performance monitoring.	• T1.403 • Bidirectional fiber data link (BFDL)
Send AIS-V for Ds1 AIS	Sends an Alarm Indication Signal VT (AIS-V) instead of DS1 AIS (from line side towards backplane/system side) when a line side trigger occurs.	• Off (unchecked, default) • On (checked)
Raise AIS for LOF	Sends AIS when a Loss of Frame (LOF) occurs.	• Off (unchecked, default) • On (checked)
ProvidesSync	The port is provisioned as a near-end timing reference.	• Off (unchecked, default) • On (checked)
SyncMsgIn	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.	• Off (unchecked, default) • On (checked)
SendDoNotUse	Sends a DUS (do not use) message on the S1 byte.	• Off (unchecked, default) • On (checked)
Enable Retiming	When checked, retimes the transmit clock to the clock reference of the NE, removing the asynchronous relationship between electrical line and SONET transport time domains for the electrical path. When not checked, leaves the port as “through-timed,” which means that the transmit clock is extracted from the DS1/E1 data from the SONET payload coming from the backplane.	• Off (unchecked, default) • On (checked)

Table 20-3 Line Options for the DS1/E1-56 Card (continued)

Parameter	Description	Options
Ds1 Mapping	Sets the mapping mode.	• Asynchronous: DS1 transport over SONET uses asynchronous mapping into VT1.5 (within a VT-structured STS-1 synchronous payload envelope [SPE]). • Byte Synchronous: DS1 transport over SONET uses byte-synchronous mapping into VT1.5 (within a VT-structured STS-1 SPE). • Japan Byte Synchronous: E1 transport over SONET uses asynchronous mapping into VT2 (within a VT-structured STS-1 SPE).
Admin SSM	Overrides the synchronization status message (SSM) synchronization traceability unknown (STU) value. If the node does not receive an SSM signal, it defaults to STU.	• PRS—Primary Reference Source (Stratum 1) • ST2—Stratum 2 • TNC—Transit node clock • ST3E—Stratum 3E • ST3—Stratum 3 • SMC—SONET minimum clock • ST4—Stratum 4 • DUS—Do not use for timing synchronization • RES—Reserved; quality level set by user

Table 20-4 describes the values on the Provisioning > Line Thresholds tabs for the DS1/E1-56 card.

Table 20-4 Line Threshold Options for DS1/E1-56 Card

Parameter	Description
Port	(Display only) Port number; 1 to 56.
CV	Coding violations. Available for Near End only.
ES	Errored seconds. Available for Near End only.
SES	Severely errored seconds. Available for Near End only.
LOSS	Loss of signal seconds; number of one-second intervals containing one or more LOS defects. Available for Near End only.
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 20-5 describes the values on the Provisioning > Elect Path Thresholds tabs for the DS1/E1-56 card.

Table 20-5 Electrical Path Threshold Options for the DS1/E1-56 Card

Parameter	Description
Port	(Display only) Port number; 1 to 56.
CV	Coding violations. Available for Near End and Far End.
ES	Errored seconds. Available for Near End and Far End.
SES	Severely errored seconds. Available for Near End and Far End.
SAS	Severely errored frame/alarm indication signal. Available for Near End only.
AISS	Alarm indication signal seconds. Available for Near End only.
UAS	Unavailable seconds. Available for Near End and Far End.
FC	Failure Count. Available for Near End only.
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 20-6 describes the values on the Provisioning > SONET Thresholds tabs for the DS1/E1-56 card.

Table 20-6 SONET Threshold Options for the DS1/E1-56 Card

Parameter	Description
Port	(Display only) DS-1 ports partitioned for STS Line 1, STS 1, Line 2, STS 1 Line 3, STS 1, Line 4 STS 1
CV	Coding violations. Available for Near End and Far End, STS termination only.
ES	Errored seconds. Available for Near End and Far End, STS termination only.
FC	Failure count. Available for Near End and Far End, STS termination only.
SES	Severely errored seconds. Available for Near End and Far End, STS termination only.
UAS	Unavailable seconds. Available for Near End and Far End, STS termination only.
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 20-7 describes the values on the Provisioning > Card tabs for the DS1/E1-56 card.

Table 20-7 Card Options for the DS1/E1-56 Card

Parameter	Description	Options
Transport Mode	Sets the encapsulation mode.	• SONET: (Default for DS1) Transports DS1s in VT1.5s and E1s in VT2s. In AU4 mode, only one STS-3c circuit shall be allowed. • AU4: (Default for E1) Transports DS1s and E1s in a structured VC4 payload (STS-3c). **Note** Switching from one transport mode to another is not allowed if a port is in a circuit, in service, or selected as a timing reference for the NE.
Operating Mode	Sets the port usage. The restrictions on switching between these selections is based on existing circuits, ports being in service, and port usage as an NE reference source.	• All DS1: (Default) All 56 ports are used as DS1 ports. Ports 1 to 28 have retiming capability. Any of the 56 ports can be selected to provide timing reference to the NE. • All E1: All 56 ports are used as E1 ports. Ports 1 to 21 have retiming capability. Any of the 56 ports can be selected to provide a timing reference to the NE.

Table 20-7 Card Options for the DS1/E1-56 Card (continued)

Parameter	Description	Options
Retiming Enabled	When checked, retimes the transmit clock to the clock reference of the NE, removing the asynchronous relationship between electrical line and SONET transport time domains for the electrical path. If the Operating Mode is All DS1, Retiming Enabled is checked and cannot be changed. When not checked for E1 mode, leaves the port as "through-timed," which means that the transmit clock is extracted from the DS1/E1 data from the SONET payload coming from the backplane.	• On (checked, default) • Off (unchecked)
Port to VT Mapping	Selects the sequence in which DS1 ports are mapped into the VT1.5s within an STS-1. This setting applies to a group of DS1 ports associated with the same STS-1.	• GR 253 interleaves the DS1 ports into the VT1.5 (DS1-14 compatible). In this mapping, sequential DS1 port numbers are mapped to interleave the 7 VT groups of VT1.5s. Interleaving by VT group essentially means that the DS1 ports follow the order of transmission of the VT1.5s, as indicated in Telcordia GR-253. • INDUSTRY maps sequential DS1 port numbers to fill each VT group in order. In this mapping, ports in sequential progression are packed into VTs filling an entire VT group before moving on to the next VT group.

Note The threshold value appears after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-A377 Provision Section DCC Terminations

Purpose	This task creates the SONET data communications channel (DCC) terminations required for alarms, administration data, signal control information, and messages. In this task, you can also set up the node so that it has direct IP access to a far-end non-ONS node over the DCC network. In addition, this task can create an OSI subnetwork point of attachment on the DCC to allow the node to be networked with third-party NEs that are based on the OSI protocol stack.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution If the ONS 15454 is configured as an OSI IS Level 1 or IS Level 1/Level 2 node and you are provisioning an OSI-only (LAP-D) SDCC to a third party NE, verify that the maximum area routing parameter on the vender NE is set to 3 before you start this task.

Note The SDCCs and LDCCs should not be provisioned between SONET (ANSI) and SDH (ETSI) nodes using CTC or TL1 because they cannot operate between SONET and SDH nodes. These communication channels should be provisioned on similar nodes, such as SONET-to-SONET or SDH-to-SDH. To establish communication channels between SONET and SDH nodes, create a DCC tunnel. See the "DLP-A313 Create a DCC Tunnel" task on page 20-7 to create a DCC tunnel.

Note When SDCC is provisioned, an LDCC termination is allowed on the same port, but is not recommended. Using SDCC and LDCC on the same port is only needed during a software upgrade if the software version does not support LDCC. You can provision SDCCs and LDCCs on different ports in the same node.

Step 1 In node view, click the **Provisioning > Comm Channels > SDCC** tabs.

Step 2 Click **Create.**

Step 3 In the Create SDCC Terminations dialog box, click the ports where you want to create the SDCC termination. To select more than one port, press the Shift key or the Ctrl key.

Note SDCC refers to the Section DCC, which is used for ONS 15454 DCC terminations. The SONET Line DCCs and the Section DCC (when not used as a DCC termination by the ONS 15454) can be provisioned as DCC tunnels. See the "DLP-A313 Create a DCC Tunnel" task on page 20-7.

Step 4 In the Port Admin State area, click **Set to IS** to put the port in service.

Step 5 Verify that the Disable OSPF on SDCC Link is unchecked.

Step 6 If the SDCC termination is to include a non-ONS node, check the **Far End is Foreign** check box. This automatically sets the far-end node IP address to 0.0.0.0, which means that any address can be specified by the far end. To change the default to a specific the IP address, see the "DLP-A374 Change a Section DCC Termination" task on page 20-60.

Step 7 In the Layer 3 box, perform one of the following:

- Check the IP box only—if the SDCC is between the ONS 15454 and another ONS node and only ONS nodes reside on the network. The SDCC will use PPP (point-to-point protocol).
- Check the IP and OSI boxes—if the SDCC is between the ONS 15454 and another ONS node and third party NEs that use the OSI protocol stack are on the same network. The SDCC will use PPP.
- Check OSI box only—if the SDCC is between an ONS node and a third party NE that uses the OSI protocol stack. The SDCC will use the LAP-D protocol.

Note If OSI is checked and IP is not checked (LAP-D), no network connections will appear in network view.

Step 8 If you checked OSI, complete the following steps. If you checked IP only, continue with Step 9.

a. Click **Next**.

b. Provision the following fields:

- Router—Choose the OSI router.
- ESH—Sets the End System Hello (ESH) propagation frequency. End system NEs transmit ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- ISH—Sets the Intermediate System Hello PDU propagation frequency. Intermediate system NEs send ISHs to other ESs and ISs to inform them about the IS NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- IIH—Sets the Intermediate System to Intermediate System Hello PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
- IS-IS Cost—Sets the cost for sending packets on the LAN subnet. The IS-IS protocol uses the cost to calculate the shortest routing path. The default metric cost for LAN subnets is 20. It normally should not be changed.

c. If the OSI and IP boxes are checked, continue with Step 9. If only the OSI is checked, click **Next** and provision the following fields:

- Mode

  AITS—(Default) Acknowledged Information Transfer Service. Does not exchange data until a logical connection between two LAP-D users is established. This service provides reliable data transfer, flow control, and error control mechanisms.

  UITS—Unacknowledged Information Transfer Service. Transfers frames containing user data with no acknowledgement. The service does not guarantee that the data presented by one user will be delivered to another user, nor does it inform the user if the delivery attempt fails. It does not provide any flow control or error control mechanisms.
- Role—Set to the opposite of the mode of the NE at the other end of the SDCC.
- MTU—Maximum transmission unit. Sets the maximum number of octets in a LAP-D information frame. The range is 512 to 1500 octets. The default is 512. You normally should not change it.

- T200—Sets the time between Set Asynchronous Balanced Mode (SABME) frame retransmissions. The default is 0.2 seconds. The range is 0.2 to 20 seconds.
- T203—Provisions the maximum time between frame exchanges, that is, the trigger for transmission of the LAP-D "keep-alive" Receive Ready (RR) frames. The default is 10 seconds. The range is 4 to 120 seconds.

Step 9 Click **Finish**.

Note EOC (DCC Termination Failure) and LOS (Loss of Signal) alarms appear until you create all network DCC terminations and put the DCC termination OC-N ports in service.

Step 10 Return to your originating procedure (NTP).

DLP-A378 Provision Line DCC Terminations

Purpose	This task creates the line data communications channel (LDCC) terminations required for alarms, administration data, signal control information, and messages. LDCCs are three-times larger than SDCCs. In this task, you can also set up the node so that it has direct IP access to a far-end non-ONS node over the DCC network. In addition, this task can create an OSI subnetwork point of attachment on the DCC to allow the node to be networked with third party NEs that are based on the OSI protocol stack.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The SDCCs and LDCCs should not be provisioned between SONET (ANSI) and SDH (ETSI) nodes using CTC or TL1 because they cannot operate between SONET and SDH nodes. These communication channels should be provisioned on similar nodes, such as SONET-to-SONET or SDH-to-SDH. To establish communication channels between SONET and SDH nodes, create a DCC tunnel. See the "DLP-A313 Create a DCC Tunnel" task on page 20-7 to create a DCC tunnel.

Note When LDCC is provisioned, an SDCC termination is allowed on the same port, but is not recommended. Using SDCC and LDCC on the same port is only needed during a software upgrade if the software version does not support LDCC. You can provision SDCCs and LDCCs on different ports in the same node.

Step 1 In node view, click the **Provisioning > Comm Channels > LDCC** tabs.

Step 2 Click **Create**.

Step 3 In the Create LDCC Terminations dialog box, click the ports where you want to create the LDCC termination. To select more than one port, press the Shift key or the Ctrl key.

Note LDCC refers to the Line DCC, which is used for ONS 15454 DCC terminations. The SONET Line DCCs and the Section DCC (when not used as a DCC termination by the ONS 15454) can be provisioned as DCC tunnels. See the "DLP-A313 Create a DCC Tunnel" task on page 20-7.

Step 4 In the Port Admin State area, click **Set to IS** to put the port in service.

Step 5 Verify that the Disable OSPF on DCC Link check box is unchecked.

Step 6 If the SDCC termination is to include a non-ONS node, check the **Far End is Foreign** check box. This automatically sets the far-end node IP address to 0.0.0.0, which means that any address can be specified by the far end. To change the default to a specific the IP address, see the "DLP-A375 Change a Line DCC Termination" task on page 20-60.

Step 7 In the Layer 3 box, perform one of the following:

- Check the IP box only—if the LDCC is between the ONS 15454 and another ONS node and only ONS nodes reside on the network. The LDCC will use PPP (point-to-point protocol).
- Check the IP and OSI boxes—if the LDCC is between the ONS 15454 and another ONS node and third party NEs that use the OSI protocol stack are on the same network. The LDCC will use PPP.

Note OSI-only (LAP-D) is not available for LDCCs.

Step 8 If you checked OSI, complete the following steps. If you checked IP only, continue with Step 9.

a. Click **Next**.

b. Provision the following fields:

- Router—Choose the OSI router
- ESH—Sets the End System Hello (ESH) propagation frequency. End system NEs transmit ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- ISH—Sets the Intermediate System Hello PDU propagation frequency. Intermediate system NEs send ISHs to other ESs and ISs to inform them about the IS NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- IIH—Sets the Intermediate System to Intermediate System Hello PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
- IS-IS Cost—Sets the cost for sending packets on the LAN subnet. The IS-IS protocol uses the cost to calculate the shortest routing path. The default metric cost for LAN subnets is 20. It normally should not be changed.

Step 9 Click **Finish**.

Note EOC-L (Line DCC Termination Failure) and LOS (Loss of Signal) alarms appear until you create all network DCC terminations and put the DCC termination OC-N ports in service.

Step 10 Return to your originating procedure (NTP).

DLP-A379 Change Line Transmission Settings for OC-N Cards

Purpose	This task changes the line transmission settings for OC-N cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 In node view, double-click the OC-N card where you want to change the line settings.

Step 2 Click the **Provisioning > Line** tabs.

Note If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 3 Modify the settings described in Table 20-8 by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value or select or deselect a check box.

Step 4 Click **Apply**.

Table 20-8 OC-N Card Line Settings

Parameter	Description	Options
Port	(Display only) Port number.	• 1 (OC-12, OC-48, OC-192) • 1 – 4 (OC-3, OC12-4) • 1 – 8 (OC3-8 • 1 – 12 (MRC_12)
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 20-8.
Port Rate	(Display only; MRC-12 and OC192-XFP cards only) Displays the port rate set for the pluggable port module (PPM). **Note** When the port rate is changed, the reach is not automatically updated and a PROV-MISMATCH alarm is raised.	• OC-3 • OC-12 • OC-48 • OC-192 (OC192-XFP only)

Table 20-8 OC-N Card Line Settings (continued)

Parameter	Description	Options
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
BLSR Ext. Byte	Allows you to remap the extended byte that carries information governing BLSR protection switches. The K3 byte should not be changed unless specifically required to run an ONS BLSR through third-party equipment.	• N/A • K3
Provides Synch	(Display only) If checked, the card is provisioned as a network element timing reference.	—
SyncMsgIn	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.	• Yes • No
Send Do Not Use	When checked, sends a DUS (do not use) message on the S1 byte.	• Yes • No
Send <FF> DoNotUse	When checked, sends a special DUS (0xff) message on the S1 byte.	• Yes • No
Admin SSM In	If the node does not receive a sync status message (SSM) signal, it defaults to STU. Admin SSM In allows you to override the STU value.	• PRS: Primary Reference Source (Stratum 1) • ST2: Stratum 2 • TNC: Transit node clock • ST3E: Stratum 3E • ST3: Stratum 3 • SMC: SONET minimum clock • ST4: Stratum 4
PJSTSMon #	Sets the STS that will be used for pointer justification. If set to 0, no STS is monitored. Only one STS can be monitored on each OC-N port.	• 0 - 3 (OC-3, per port) • 0 - 12 (OC-12) • 0 - 48 (OC-48) • 0 - 192 (OC-192)

Table 20-8 OC-N Card Line Settings (continued)

Parameter	Description	Options
Admin State	Sets the port administrative service state unless network conditions prevent the change.	• IS—Puts the port in-service. The port service state changes to IS-NR. • IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. • OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. • OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT. **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—The port is fully operational and performing as provisioned. • OOS-AU,AINS—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic. • OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments

Table 20-8 OC-N Card Line Settings (continued)

Parameter	Description	Options
Type	Defines the port as SONET or SDH. The Enable Sync Msg field and the Send Do Not Use field must be disabled before the port can be set to SDH.	• Sonet • SDH
ALS Mode	Sets the automatic laser shutdown function.	• Disabled • Auto Restart • Manual Restart • Manual Restart for Test
Reach	(Does not apply to all cards) Allows you to provision the reach value. You can also choose Auto Provision, which allows the system to automatically provision the reach from the PPM reach value on the hardware.	The options that appear in the drop-down list depend on the card: • SR (short reach, up to 2 km distance) • SR-1 (up to 2 km distance) • IR-1 (intermediate reach, up to 15 km distance) • IR-2 (up to 40 km distance) • LR-1 (long reach, up to 40 km distance) • LR-2 (up to 80 km distance) • LR-3 (up to 80 km distance)
Wavelength	(Does not apply to all cards) Allows you to provision the wavelength frequency.	• First Tunable Wavelength • 1310 nm • 1470 nm • 1490 nm • 1510 nm • 1530 nm • 1550 nm • 1570 nm • 1590 nm • 1610 nm ONS-XC-10G-C= Tunable XFP: • 1529.55 nm through 1561.83 nm, with ITU spacing.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

DLP-A380 Provision a Proxy Tunnel

Purpose	This task sets up a proxy tunnel to communicate with a non-ONS far-end node. Proxy tunnels are only necessary when the proxy server is enabled and a foreign DCC termination exists, or if static routes exist so that the DCC network is used to access remote networks or devices. You can provision a maximum of 12 proxy server tunnels.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 DLP-A377 Provision Section DCC Terminations, page 20-69
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note If the proxy server is disabled, you cannot set up a proxy tunnel.

Step 1 Click the **Provisioning > Network > Proxy** subtabs.

Step 2 Click **Create**.

Step 3 In the Create Tunnel dialog box, complete the following:

- Source Address—Type the IP address of the source node (32 bit length) or source subnet (any other length).
- Length—Choose the length of the source subnet mask.
- Destination Address—Type the IP address of the destination node (32 bit length) or destination subnet (any other length).
- Length—Choose the length of the destination subnet mask.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-A381 Provision a Firewall Tunnel

Purpose	This task provisions destinations that will not be blocked by the firewall. Firewall tunnels are only necessary when the proxy server is enabled and a foreign DCC termination exists, or if static routes exist so that the DCC network is used to access remote networks or devices. You can provision a maximum of 12 firewall tunnels.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 DLP-A377 Provision Section DCC Terminations, page 20-69
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note If the proxy server is configured as proxy-only or is disabled, you cannot set up a firewall tunnel.

Step 1 Click the **Provisioning > Network > Firewall** subtabs.

Step 2 Click **Create**.

Step 3 In the Create Tunnel dialog box, complete the following:

- Source Address—Type the IP address of the source node (32 bit length) or source subnet (any other length).
- Length—Choose the length of the source subnet mask.
- Destination Address—Type the IP address of the destination node (32 bit length) or destination subnet (any other length).
- Length—Choose the length of the destination subnet mask.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-A382 Delete a Proxy Tunnel

Purpose	This task removes a proxy tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Click the **Provisioning > Network > Proxy** subtabs.

Step 2 Click the proxy tunnel that you want to delete.

Step 3 Click **Delete**.

Step 4 Return to your originating procedure (NTP).

DLP-A383 Delete a Firewall Tunnel

Purpose	This task removes a firewall tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Click the **Provisioning > Network > Firewall** subtabs.

Step 2 Click the firewall tunnel that you want to delete.

Step 3 Click **Delete**.

Step 4 Return to your originating procedure (NTP).

DLP-A384 Add a Member to a VCAT Circuit

Purpose	This task adds a member to one of the following VCAT circuits: • Software link capacity adjustment scheme (SW-LCAS) VCAT circuits on FC_MR-4 (enhanced mode) or CE-1000-4 cards • Non-LCAS and LCAS circuits on CE-100T-8 cards Adding a member to a VCAT circuit changes the size of the circuit. The new members use the VCAT member source, destination, and routing preference (common fiber or split routing) specified during the VCAT circuit creation procedure.
Tools/Equipment	FC_MR-4 card (enhanced mode) or CE-Series card.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 VCAT circuits must exist on the network. See the "NTP-A264 Create an Automatically Routed VCAT Circuit" procedure on page 6-81 or the "NTP-A265 Create a Manually Routed VCAT Circuit" procedure on page 6-86.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This task optionally uses automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Note Adding a member to a non-LCAS VCAT circuit can be service affecting.

Note Adding a member to SW-LCAS or LCAS VCAT circuits in the IS-NR, OOS-AU,AINS, or OOS-MA,MT service state could be service affecting. Cisco recommends using the OOS-MA,OOG service state when adding new members. You can put the member in the desired state after adding the member.

Note You cannot add members to VCAT circuits that have a source or destination on an ML-Series or FC_MR-4 (line rate mode) card.

Step 1 In node or network view, click the **Circuits** tab.

Step 2 Click the VCAT circuit that you want to edit, then click **Edit**.

Step 3 Click the **Members** tab.

Step 4 If you want to add a member to a non-LCAS VCAT circuit, complete the following substeps. If you want to add a member to a SW-LCAS or LCAS VCAT circuit, skip this step and continue with Step 5.

- **a.** Select a member with a VCAT State of In Group. The In Group state indicates that a member has cross-connects in the IS-NR; OOS-MA,AINS; or OOS-MA,MT service states.
- **b.** Click **Edit Member**.
- **c.** In the Edit Member Circuit window, click the **State** tab.
- **d.** View the cross-connect service state in the CRS Service State column. You will need this information when choosing the new member state.

  Cross-connects of all In Group non-LCAS members must be in the same service state. If all existing members are in the Out of Group VCAT state, which for non-LCAS members is the OOS-MA,DSBLD service state, you can choose any service state for the new member.
- **e.** From the File menu, choose **Close** to return to the Edit Circuit window.

Step 5 Click **Add Member**. The Add Member button is enabled if the VCAT circuit has sufficient bandwidth for an added member.

Step 6 Define the number of members and member attributes:

- Number of members to add—Choose the number of members to add from the drop-down list. If the drop-down list does not show a number, the VCAT circuit has the maximum number of members allowed. The number of members allowed depends on the source and destination card and the existing size of the circuit. For more information on the number of members allowed for a card, refer to the "Circuits and Tunnels" chapter of the *Cisco ONS 15454 Reference Manual*.
- New Circuit Size—(Display only) Automatically updates based on the number of added members.

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit.
- State—To add a non-LCAS member to a VCAT with In Group members, choose the state you viewed in Step 4. To add a non-LCAS member to a VCAT with only Out of Group members, choose any of the following states. To add SW-LCAS or LCAS members, Cisco recommends the OOS,OOG state.
  - IS—Puts the member cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the member cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - IS,AINS—Puts the member cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the member cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-A437 Change a VCAT Member Service State" task on page 21-16.
  - OOS,OOG—(LCAS and SW-LCAS VCAT circuits only) Puts VCAT member cross-connects in the Out-of-Service and Management, Out-of-Group (OOS-MA,OOG) service state. This administrative state is used to put a member circuit out of the group and to stop sending traffic.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 7 Click **Next**.

Step 8 To route the member(s) automatically, check **Route Automatically**. To manually route the members, leave Route Automatically unchecked.

Step 9 If you want to set preferences for individual members, complete the following in the Member Preferences area. To set identical preferences for all added members, skip this step and continue with Step 10.

Note Common fiber or split routing cannot be changed.

- Number—Choose a number (between 1 and 256) from the drop-down list to identify the member.
- Name—Type a unique name to identify the member. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the circuit.
- Protection—Choose the member protection type:
  - Fully Protected—Routes the circuit on a protected path.
  - Unprotected—Creates an unprotected circuit.
  - PCA—Routes the member on a BLSR protection channel.
  - DRI—(Split routing only) Routes the member on a dual-ring interconnect circuit.
- Node-Diverse Path—(Split routing only) Available for each member when Fully Protected is chosen.

Step 10 To set preferences for all members, complete the following in the Set Preferences for All Members area:

- Protection—Choose the member protection type:
  - Fully Protected—Routes the circuit on a protected path.
  - Unprotected—Creates an unprotected circuit.
  - PCA—Routes the member on a BLSR protection channel.
  - DRI—(Split routing only) Routes the member on a dual-ring interconnect circuit.
- Node-Diverse Path—(Split routing only) Available when Fully Protected is chosen.

Step 11 If you left Route Automatically unchecked in Step 8, click **Next** and complete the following substeps. If you checked Route Automatically in Step 8, continue with Step 12.

a. In the Route Review/Edit area of the Circuit Creation wizard, choose the member to route from the Route Member number drop-down list.

b. Click the source node icon if it is not already selected.

c. Starting with a span on the source node, click the arrow of the span you want the member to travel. The arrow turns white. In the Selected Span area, the From and To fields provide span information.

d. If you want to change the source, adjust the Source STS field; otherwise, continue with Step e.

e. Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

f. Repeat Steps c through e until the member is provisioned from the source to the destination node through all intermediary nodes. If you selected Fully Protect Path, you must:

- Add two spans for all path protection ring or unprotected portions of the member route from the source to the destination
- Add one span for all BLSR or 1+1 portions of route from the source to the destination
- For members routed on path protection dual-ring interconnect topologies, provision the working and protect paths as well as spans between the DRI nodes

g. Repeat Steps a through f for each member.

Step 12 If you checked Route Automatically in Step 8 and checked Review Route Before Creation, complete the following substeps. If not, continue with Step 13.

a. Click **Next**.

b. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information.

Step 13 Click **Finish**.

Note Adding members to a VCAT circuit may take several minutes depending on the complexity of the network and the number of members to be added.

Step 14 If you added an LCAS member, complete the following substeps:

a. Click the Alarms tab and see if the VCAT Group Degraded (VCG-DEG) alarm appears. If it does appear, refer to the *Cisco ONS 15454 Troubleshooting Guide* for the procedure to clear the alarm. If it does not, continue with Step b.

b. Complete the "DLP-A437 Change a VCAT Member Service State" task on page 21-16 to put the member in the IS service state.

Step 15 Return to your originating procedure (NTP).

DLP-A385 Delete a Member from a VCAT Circuit

Purpose	This task removes a member from a VCAT circuit that was created with one of the following criteria: • SW-LCAS VCAT circuits on FC_MR-4 (enhanced mode) or CE-1000-4 cards • Non-LCAS and LCAS circuits on CE-100T-8 cards This task reduces the size of the VCAT circuit.
Tools/Equipment	FC_MR-4 card (enhanced mode) or CE-Series card.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 VCAT circuits must exist on the network. See the "NTP-A264 Create an Automatically Routed VCAT Circuit" procedure on page 6-81 or the "NTP-A265 Create a Manually Routed VCAT Circuit" procedure on page 6-86. As necessary, complete the "DLP-A437 Change a VCAT Member Service State" task on page 21-16 to change a SW-LCAS or LCAS member state to OOS-MA,OOG.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Whenever circuits are deleted in a VCAT group, make sure that the TL1 parameter, txcount in a VCAT group is updated with the number of existing circuits. TL1 and CTC will now show the correct number of VCAT circuits present.

Note Deleting a member from a non-LCAS circuit can be service-affecting.

Note Deleting SW-LCAS or LCAS members in the IS-NR or OOS-AU,AINS service state can be service affecting. Cisco recommends putting the member to be deleted in the OOS-MA,OOG service state before deleting. Non-LCAS members do not support the OOS-MA,OOG service state.

Note You cannot delete members that have a source or destination on an ML-Series or FC_MR-4 (line rate mode) card.

Step 1 In node or network view, click the **Circuits** tab.

Step 2 Click the VCAT circuit that you want to edit, then click **Edit**.

Step 3 Click the **Members** tab.

Step 4 Select the member that you want to delete. To select multiple members, press **Ctrl** and click the desired members.

Step 5 Click **Delete Member**.

Step 6 In the confirmation dialog box, click **Yes**.

Step 7 Return to your originating procedure (NTP).

DLP-A386 Install Electrical Cables on the UBIC-V EIAs

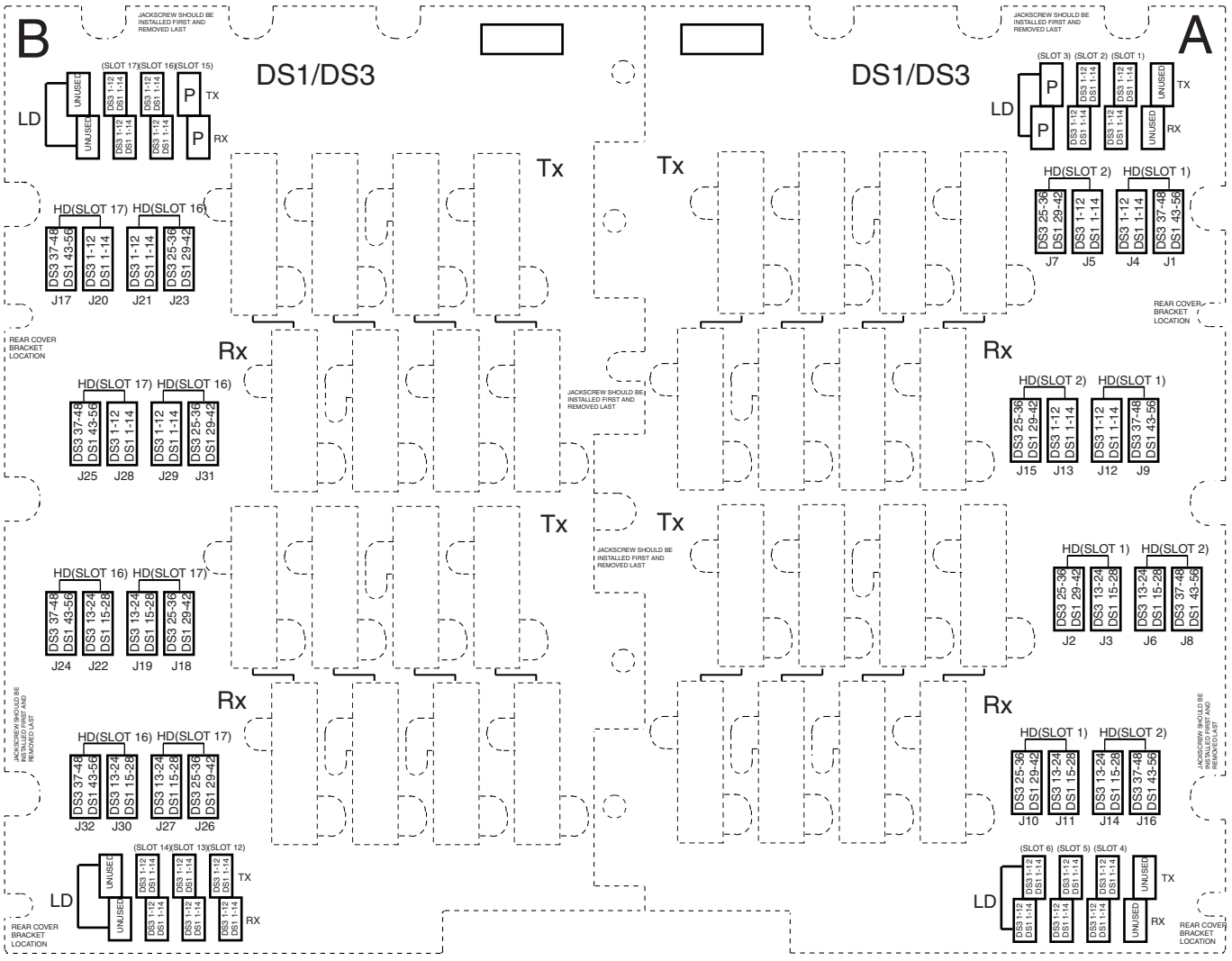
Purpose	This task installs DS-1 and DS-3/EC-1 cables on the UBIC-V EIAs.
Tools/Equipment	3/16-inch flat-head screwdriver DS-1 and DS-3/EC-1 cables, as needed: • DS-1 cable, 150 feet: 15454-CADS1-SD • DS-1 cable, 250 feet: 15454-CADS1-ID • DS-1 cable, 655 feet: 15454-CADS1-LD • DS-3/EC-1 cable, 75 feet: 15454-CADS3-SD • DS-3/EC-1 cable, 225 feet: 15454-CADS3-ID • DS-3/EC-1 cable, 450 feet: 15454-CADS3-LD
Prerequisite Procedures	DLP-A190 Install a UBIC-V EIA, page 18-59
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Cisco recommends that you plan for future slot utilization and fully cable all SCSI connectors you will use later.

Step 1 Starting at the lowest row where you want to install cables on the UBIC-V place a cable connector over the desired connection point on the UBIC-V EIA.

Figure 20-14 shows the UBIC-V slot designations.

Figure 20-14 UBIC-V Slot Designations



Step 2 With the alignment slots of the cable connector aligned with the alignment standoffs of the UBIC connector, carefully install the cable.

Step 3 Use the flat-head screwdriver to tighten the screw at the top left of the cable connector to 8 to 10 lbf-inch (9.2 to 11.5kgf-cm). Repeat this for the screw at the bottom right of the connector. Alternate between the two screws until both are tight.

Step 4 Repeat Steps 1 through 3 for each cable you want to install, moving from the bottom row to the top row. If you are installing a cable near cables that are already installed, you might need to gently hold back the surrounding cables. Make sure you install cables in pairs, Tx and Rx, each time.

Figure 20-15 shows a UBIC-V with cables installed in all connectors.

Figure 20-15 Fully Cabled UBIC-V; Front- and Side-View

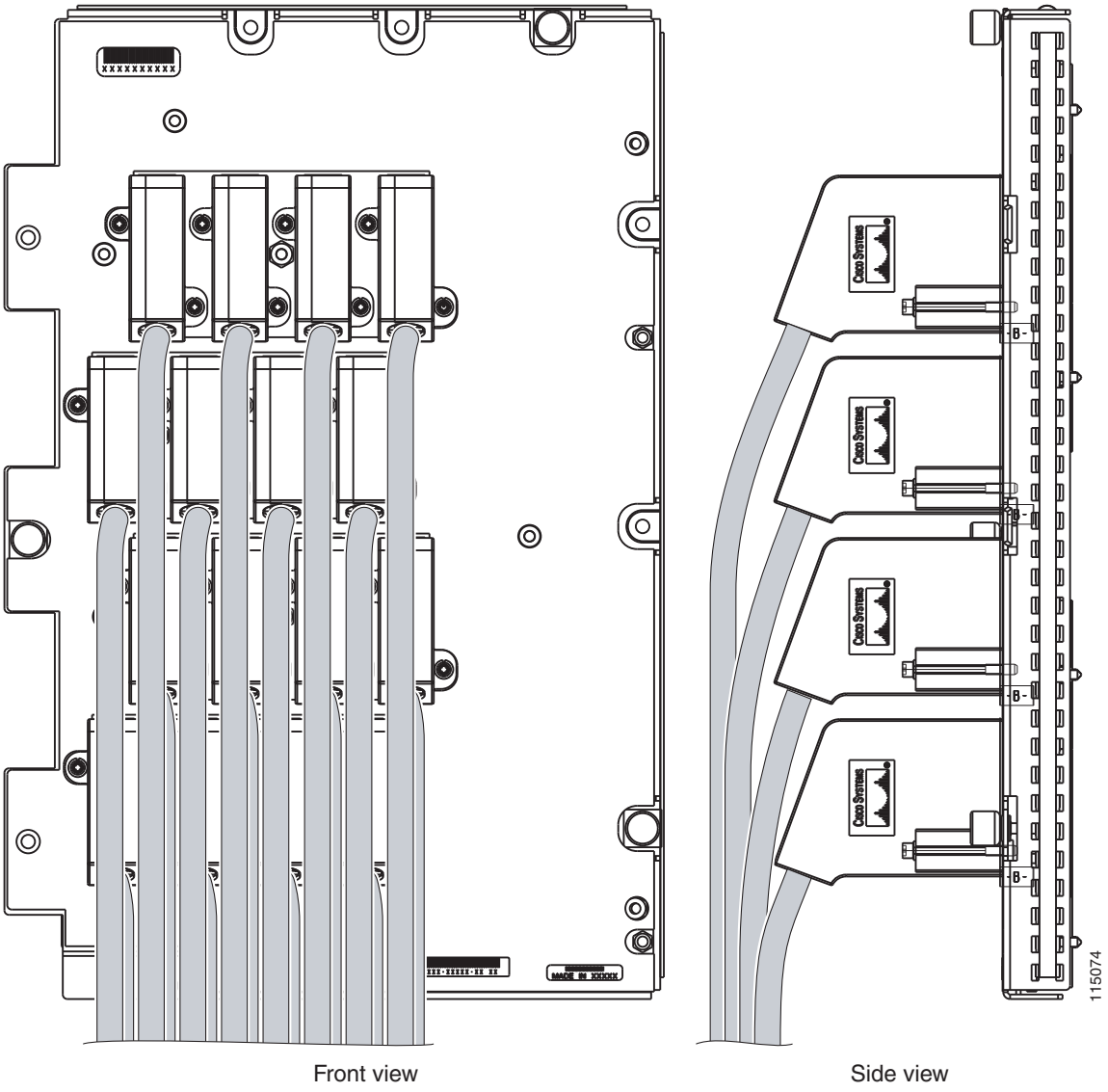
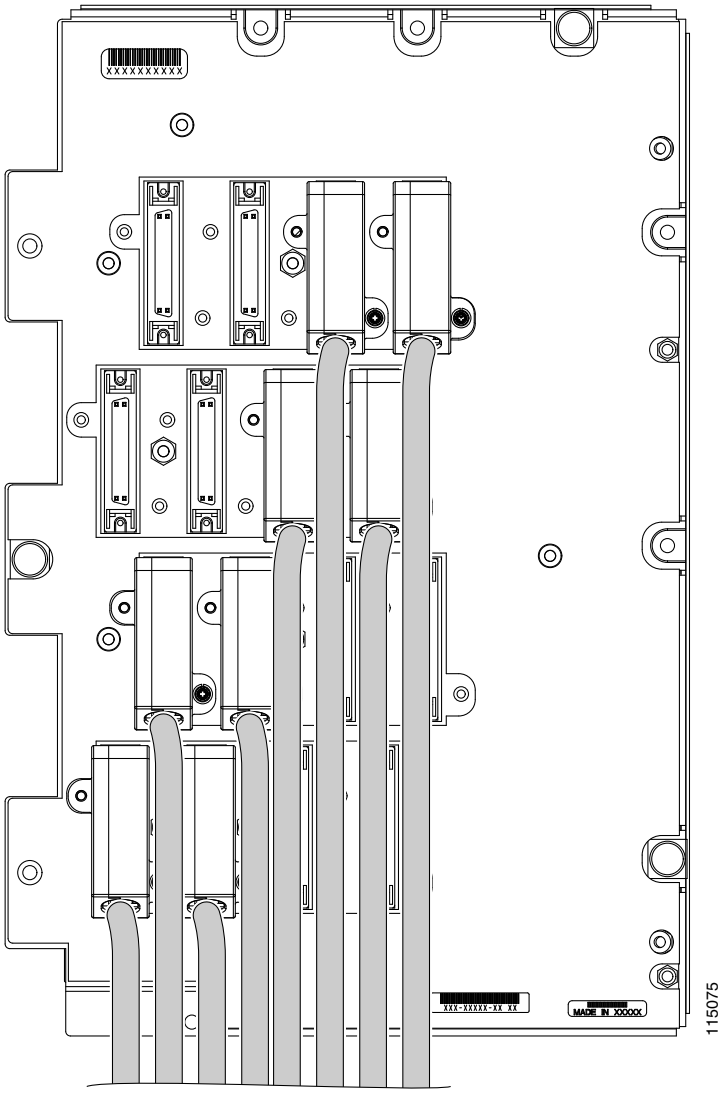


Figure 20-16 shows a partially populated UBIC-V.

Figure 20-16 Partially Cabled UBIC-V



Step 5 If available, tie wrap or lace the cables to the tie bar according to Telcordia standards (GR-1275-CORE) or local site practice.

Note When routing the electrical cables, be sure to leave enough room in front of the alarm and timing panel so that it is accessible for maintenance activity.

Step 6 Return to your originating procedure (NTP).

DLP-A387 Change Line and Threshold Settings for the DS3XM-12 Card

Purpose	This task changes the line and threshold settings for the DS3XM-12 card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The DS3XM-12 (transmux) card can accept up to 12 channelized DS-3 signals and convert each signal to 28 VT1.5 signals for a total of 336 VT1.5 conversions. Conversely, the card can take 28 VT1.5s and multiplex them into a channeled C-bit or M13 framed DS-3 signal for each of the 12 DS-3 ports.

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 In node view, double-click the DS3XM-12 card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line**, **DS1**, **Line Thresholds, Elect Path Thresholds,** or **SONET Thresholds** tab.

Note See Chapter 8, "Manage Alarms" for information about the Alarm Profiles tab.

Note If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 4 Modify the settings found under these subtabs by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

Step 7 For definitions of the line settings, see Table 20-9. For definitions of the DS1 settings, see Table 20-10 on page 20-90. For definitions of the line threshold settings, see Table 20-11 on page 20-91. For definitions of the electrical path threshold settings, see Table 20-12 on page 20-92. For definitions of the SONET threshold settings, see Table 20-13 on page 20-92.

Table 20-9 describes the values on the Provisioning > Line tabs for the DS3XM-12 cards.

Table 20-9 Line Options for the DS3XM-12 Parameters

Parameter	Description	Options
Port #	(Display only) Port number.	1 to 36
Port Name	Displays the port name.	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 20-8.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—The port is fully operational and performing as provisioned. • OOS-AU,AINS—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic. • OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Line Type	Defines the line framing type.	• M13 - default • C BIT

Table 20-9 Line Options for the DS3XM-12 Parameters (continued)

Parameter	Description	Options
Line Coding	Defines the DS-1 transmission coding type that is used.	B3ZS
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450
Admin State	Sets the port service state unless network conditions prevent the change.	• IS—Puts the port in-service. The port service state changes to IS-NR. • IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. • OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. • OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT. **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.

Table 20-10 describes the values on the Provisioning > DS1 tabs for the DS3XM-12 cards. Refer to the *Cisco ONS 15454 Reference Manual* for more information about "portless" protection on DS3XM-12 cards.

Table 20-10 DS1 Options for the DS3XM-12 Card

Parameter	Description	Options
Port	(Display only) Displays the port number by DS-3 and corresponding DS-1.	DS-3: 1–35 DS-1: 1–28
Port Name	Displays the port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 20-8.

Table 20-10 DS1 Options for the DS3XM-12 Card (continued)

Parameter	Description	Options
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—The port is fully operational and performing as provisioned. • OOS-AU,AINS—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic. • OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
Line Type	Defines the line framing type.	• AUTO FRAME • ESF - Extended Super Frame • D4 • UNFRAMED
FDL Mode	Defines the fiber data link (FDL) mode for the port.	• T1.403 • BFDL - Bidirectional FDL

Table 20-11 lists the line thresholds options for DS3XM-12 cards.

Table 20-11 Line Thresholds Options for the DS3XM-12 Card

Parameter	Description
Port	(Display only) Display the port number by DS-3 and corresponding DS-1. DS-3: 1 – 35 DS-1: 1 – 28
CV	Coding violations
ES	Errored seconds
SES	Severely errored seconds
LOSS	Loss of signal seconds
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 20-12 describes the values on the Provisioning > Elect Path Thresholds tabs for the DS3XM-12 cards.

Table 20-12 Electrical Path Threshold Options for the DS3XM-12 Card

Parameter	Description
Port	(Display only) Port number; 1 to 36
CV	Coding violations
ES	Errored seconds
SES	Severely errored seconds
SAS	Severely errored frame/alarm indication signal
AISS	Alarm indication signal seconds
UAS	Unavailable seconds
FC	Failure Count (available for STS only)
CSS	Controlled Slip Seconds
ESA	Errored Seconds (Type A)
ESB	Errored Seconds (Type B)
SEFS	Severely Errored Frame Seconds
ESNE	Errored seconds (Near End)
ESFE	Errored seconds (Far End)
SESNE	Severely errored seconds (Near End)
SESFE	Severely errored seconds (Far End)
UASNE	Unavailable seconds (Near End)
UASFE	Unavailable seconds (Far End)
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 20-13 describes the values on the Provisioning > SONET Thresholds tabs for the DS3XM-12 cards.

Table 20-13 SONET Threshold Options for the DS3XM-12 Card

Parameter	Description
CV	Coding violations
ES	Errored seconds
FC	Failure count
SES	Severely errored seconds
UAS	Unavailable seconds

Table 20-13 SONET Threshold Options for the DS3XM-12 Card (continued)

Parameter	Description
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Note The threshold value appears after the circuit is created.

Step 8 Return to your originating procedure (NTP).

DLP-A388 Change Line and Threshold Settings for the DS3/EC1-48 Cards

Purpose	This task changes the line and threshold settings for the DS3/EC1-48 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 Double-click the DS3/EC1-48 card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line**, **Line Thresholds**, **Elect Path Thresholds**, or **SONET Thresholds** tab.

Note See Chapter 8, "Manage Alarms" for information about the Alarm Profiles tab.

Note If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 4 Modify the settings found under these subtabs by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

For definitions of the line settings, see Table 20-14. For definitions of the line threshold settings, see Table 20-15 on page 20-95. For definitions of the electrical path threshold settings, see Table 20-16 on page 20-96. For definitions of the SONET threshold settings, see Table 20-17 on page 20-96.

Table 20-14 Line Options for the DS3/EC1-48 Card

Parameter	Description	Options
Port	(Display only) Port number.	1 to 48
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 20-8.
Admin State	Sets the port service state unless network conditions prevent the change.	• IS—Puts the port in-service. The port service state changes to IS-NR. • IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. • OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. • OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT. **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—The port is fully operational and performing as provisioned. • OOS-AU,AINS—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic. • OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.

Table 20-14 Line Options for the DS3/EC1-48 Card (continued)

Parameter	Description	Options
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Line Type	Defines the line framing type.	• Unframed - default • M13 • C BIT • Auto Provision Fmt
Detected Line Type	(Display only) Displays the detected line type.	• M13 • C Bit • Unframed • Unknown
Line Coding	Defines the DS-3 transmission coding type that is used.	B3ZS
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450
AINS Soak	Sets the automatic in-service soak period.	Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically. Value is between 0 and 48 hours, in 15-minute increments.

Table 20-15 describes the values on the Provisioning > Line Thresholds tabs for the DS3/EC1-48 card.

Table 20-15 Line Threshold Options for DS3/EC1-48 Card

Parameter	Description
Port	(Display only) Port number; 1 to 48.
CV	Coding violations.
ES	Errored seconds.
SES	Severely errored seconds.
LOSS	Loss of signal seconds; number of one-second intervals containing one or more LOS defects.

Table 20-15 Line Threshold Options for DS3/EC1-48 Card (continued)

Parameter	Description
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 20-16 describes the values on the Provisioning > Elect Path Thresholds tabs for the DS3/EC1-48 card.

Table 20-16 Electrical Path Threshold Options for the DS3/EC1-48 Card

Parameter	Description
Port	(Display only) Port number; 1 to 48.
CV	Coding violations
ES	Errored seconds
SES	Severely errored seconds
SAS	Severely errored frame/alarm indication signal
AISS	Alarm indication signal seconds
UAS	Unavailable seconds
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 20-17 describes the values on the Provisioning > SONET Thresholds tabs for the DS3/EC1-48 card.

Table 20-17 SONET Threshold Options for the DS3/EC1-48 Card

Parameter	Description
Port	(Display only) DS-3 ports partitioned for STS Line 1, STS 1, Line 2, STS 1 Line 3, STS 1, Line 4 STS 1
CV	Coding violations. Available for Near and Far End, STS termination only.
ES	Errored seconds. Available for Near and Far End, STS termination only.
FC	Failure count. Available for Near and Far End, STS termination only.
SES	Severely errored seconds. Available for Near and Far End, STS termination only.
UAS	Unavailable seconds. Available for Near and Far End, STS termination only.

Table 20-17 SONET Threshold Options for the DS3/EC1-48 Card (continued)

Parameter	Description
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Note The threshold value appears after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-A390 View Alarms

Purpose	Use this task to view current alarms on a card, node, or network.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the card, node, or network view, click the **Alarms** tab to view the alarms for that card, node, or network.

Table 20-18 Alarm Column Descriptions

Column	Information Recorded
Num	Sequence number of the original alarm
Ref	Reference number of the original alarm
New	Indicates a new alarm; to change this status, click either the Synchronize button or the Delete Cleared Alarms button.
Date	Date and time of the alarm.
Node	The name of the node where the alarm is located. (In dense wavelength-division multiplexing [DWDM] configurations, one node can contain multiple shelves.) Visible in network view.
Object	TL1 access identifier (AID) for the alarmed object; for an STSmon or VTmon, this is the monitored STS or VT.
Eqpt Type	If an alarm is raised on a card, the card type in this slot.
Slot	If an alarm is raised on a card, the slot where the alarm occurred (appears only in network and node view).

Table 20-18 Alarm Column Descriptions (continued)

Column	Information Recorded
Port	If an alarm is raised on a card, the port where the alarm is raised; for STSTerm and VTTerm, the port refers to the upstream card it is partnered with.
Path Width	Indicates how many STSs are contained in the alarmed path. This information complements the alarm object notation, which is described in the *Cisco ONS 15454 Troubleshooting Guide*.
Sev	Severity level: CR (Critical), MJ (Major), MN (minor), NA (Not Alarmed), NR (Not Reported).
ST	Status: R (raised), C (clear), or T (transient).
SA	When checked, indicates a service-affecting alarm.
Cond	The error message/alarm name; these names are alphabetically defined in the *Cisco ONS 15454 Troubleshooting Guide.*
Description	Description of the alarm.
Shelf	For DWDM configurations, the shelf where the alarmed object is located. Visible in network view.

Table 20-19 lists the color codes for alarm and condition severities.

Table 20-19 Color Codes for Alarms and Condition Severities

Color	Description
Red	Raised Critical (CR) alarm
Orange	Raised Major (MJ) alarm
Yellow	Raised Minor (MN) alarm
Magenta (pink)	Raised Not Alarmed (NA) condition
Blue	Raised Not Reported (NR) condition
White	Cleared (C) alarm or condition

Step 2 If alarms are present, refer to the *Cisco ONS 15454 Troubleshooting Guide* for information and troubleshooting procedures.

Step 3 Return to your originating procedure (NTP).

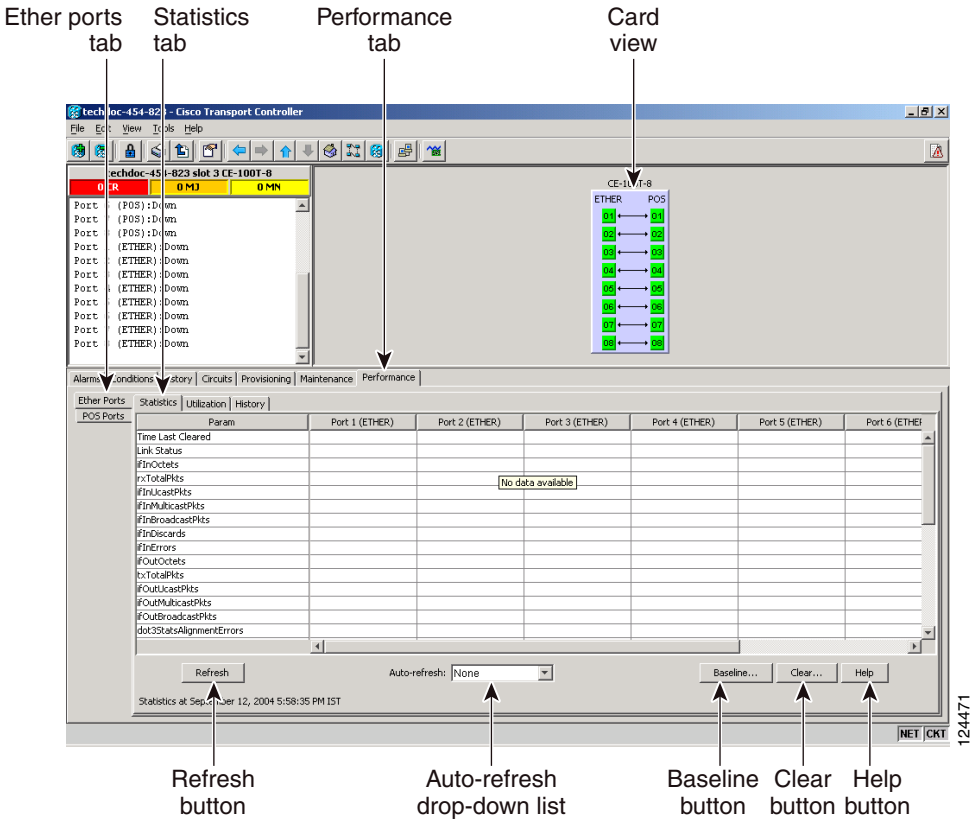
DLP-A391 View CE-Series Ether Ports and POS Ports Statistics PM Parameters

Purpose	This task enables you to view CE-Series Ethernet port Statistics PM counts at selected time intervals to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the CE-Series Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Ether Ports** > **Statistics** (Figure 20-17) or **Performance** > **POS Ports** > **Statistics** tabs.

Figure 20-17 Ether Ports Statistics on the CE-Series Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Port # columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 9-2.

Step 5 Return to your originating procedure (NTP).

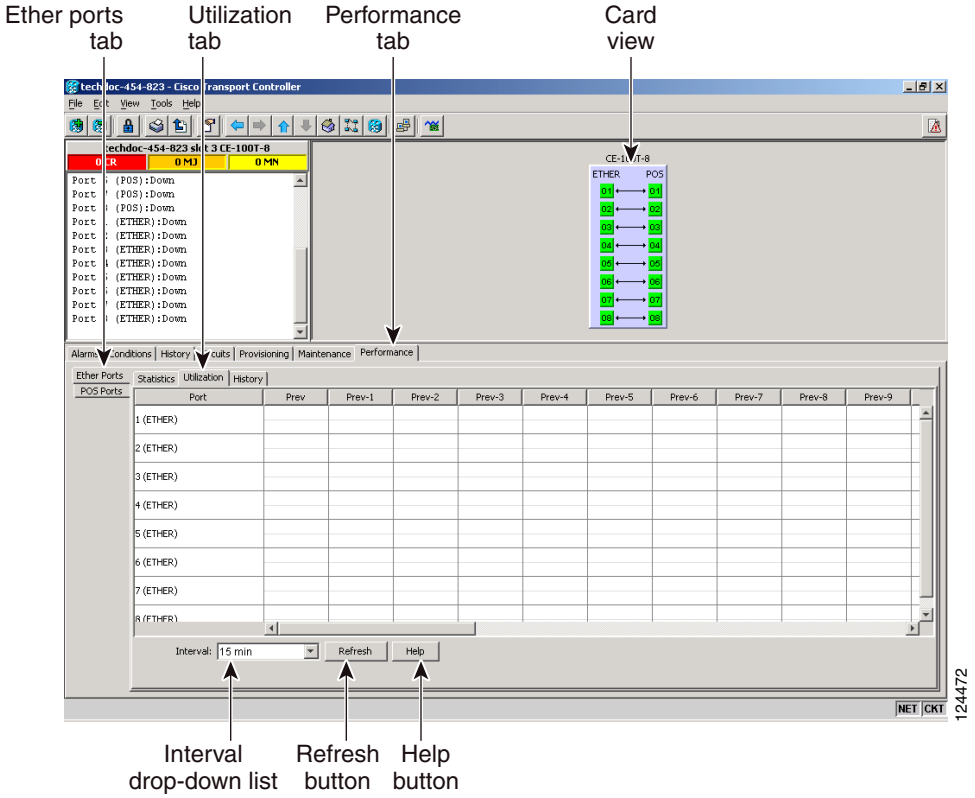
DLP-A392 View CE-Series Ether Ports and POS Ports Utilization PM Parameters

Purpose	This task enables you to view CE-Series Ethernet port Utilization PM counts at selected time intervals to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the CE-Series Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance > Ether Ports > Utilization** (Figure 20-18) or **Performance > POS Ports > Utilization** tabs.

Figure 20-18 Ether Ports Utilization on the CE-Series Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the Port # column to find the port you want to monitor.

Step 5 The transmit (Tx) and receive (Rx) bandwidth utilization values for the previous time intervals appear in the Prev-*n* columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 9-2.

Step 6 Return to your originating procedure (NTP).

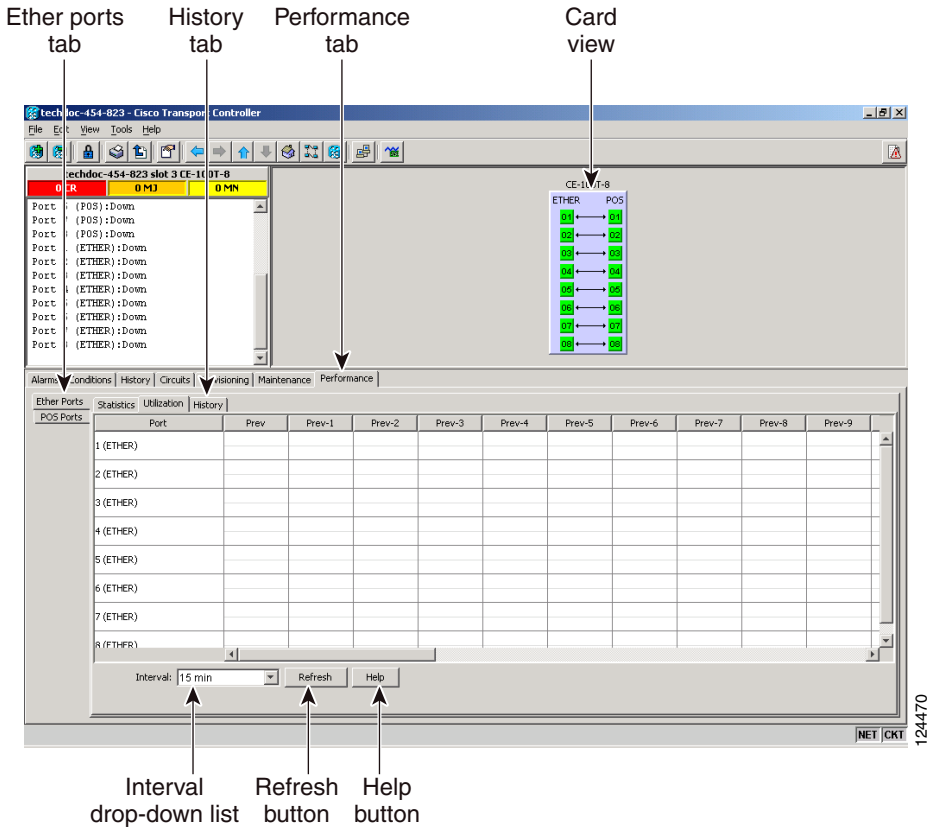
DLP-A393 View CE-Series Ether Ports and POS Ports History PM Parameters

Purpose	This task enables you to view CE-Series Ethernet port History PM counts at selected time intervals to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the CE-Series Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Ether Ports** > **History** tabs (Figure 20-19) **Performance** > **POS Ports** > **History** tabs.

Figure 20-19 Ether Ports History on the CE-Series Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Prev-n columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 9-2.

Step 5 Return to your originating procedure (NTP).

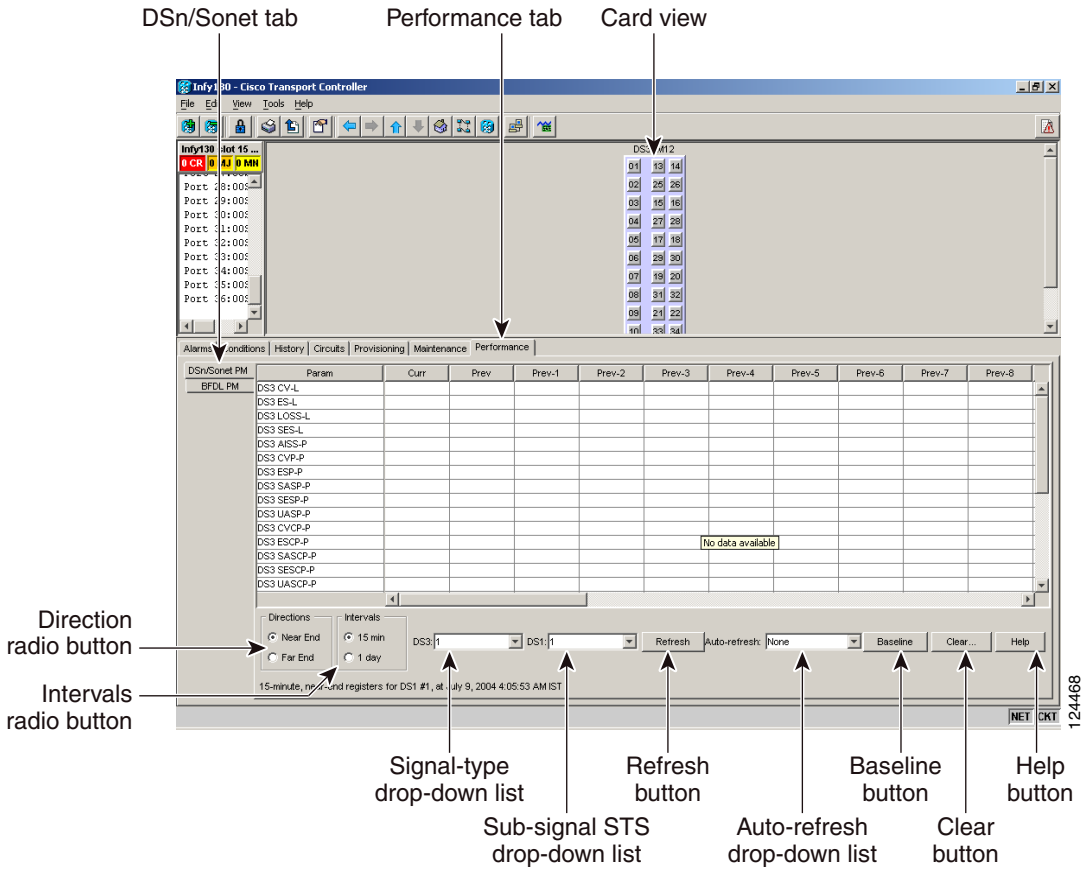
DLP-A394 View DS-N/SONET PM Parameters for the DS3XM-12 Card

Purpose	This task enables you to view DS-N/SONET PM parameters for near-end or far-end performance during selected time intervals on an DS3XM-12 electrical card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits and VT Tunnels" and Chapter 10, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the DS3XM-12 electric card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance > DSn/SONET PM** tabs to view the DS-N/SONET Performance parameters (Figure 20-20).

Figure 20-20 Viewing DS3XM-12 Card DSn/SONET Performance Monitoring Information



Note Different port and signal-type drop-down lists appear depending on the card type and the circuit type. The appropriate types (DS1, DS3, VT path, STS path) appear based on the card. For example, the DS3XM cards list DS3, DS1, VT path, and STS path PM parameters as signal types. This enables you to select both the DS-3 port and the DS-1 within the specified DS-3.

Step 3 In the signal type drop-down lists, choose the DS-3 port and the DS-1 port within the specified DS-3.

Step 4 Click **Refresh**.

Step 5 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 9-2.

Step 6 Return to your originating procedure (NTP).

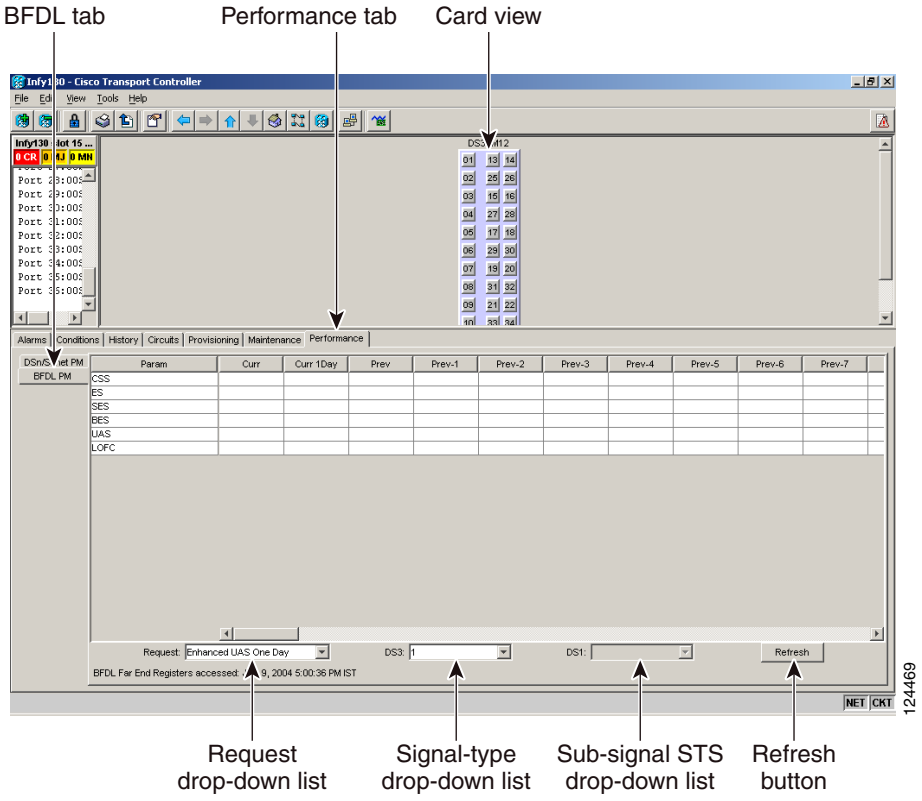
DLP-A395 View BFDL PM Parameters for the DS3XM-12 Card

Purpose	This task enables you to view bidirectional fiber data link (BFDL) PM parameters for near-end or far-end performance during selected time intervals on an DS3XM-12 electrical card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits and VT Tunnels" and Chapter 10, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the DS3XM-12 card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance > BFDL PM** tabs to view the BFDL performance parameters (Figure 20-21).

Figure 20-21 Viewing DS3XM-12 Card BFDL Performance Monitoring Information



Note Different port and signal-type drop-down lists appear depending on the card type and the circuit type. The appropriate types (DS1, DS3, VT path, STS path) appear based on the card. For example, the DS3XM cards list DS3, DS1, VT path, and STS path PM parameters as signal types. This enables you to select both the DS-3 port and the DS-1 within the specified DS-3.

Step 3 From the Request drop-down list choose one of the following:

- Enhanced ES One Day
- Enhanced BES One day
- Enhanced SES One Day
- Enhanced UAS One Day
- Enhanced CSS/LOFC One day

Step 4 In the signal type drop-down lists, choose the DS-3 port and the DS-1 port within the specified DS-3.

Step 5 Click **Refresh**.

Step 6 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 9-2.

Step 7 Return to your originating procedure (NTP).

DLP-A397 Manually Route a Path Protection Circuit for a Topology Upgrade

Purpose	This task creates a manually routed USPR circuit during a conversion from an unprotected point-to-point or linear ADM system to a path protection configuration.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 NTP-A342 Convert a Point-to-Point or Linear ADM to a Path Protection Configuration Automatically, page 13-11
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the Circuit Routing Preferences area of the Unprotected to Path Protection page, uncheck **Route Automatically**.

Step 2 Click **Next**. In the Route Review and Edit area, node icons appear for you to route the circuit. The circuit source node is selected. Green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit.

Step 3 Click **Finish**.

Step 4 Return to your originating procedure (NTP).

DLP-A398 Automatically Route a Path Protection Circuit for a Topology Upgrade

Purpose	This task creates an automatically routed USPR circuit during a conversion from an unprotected point-to-point or linear ADM system to a path protection configuration.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 NTP-A342 Convert a Point-to-Point or Linear ADM to a Path Protection Configuration Automatically, page 13-11
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This task requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 In the Circuit Routing Preferences area of the Unprotected to Path Protection page, check **Route Automatically**.

Step 2 Two options are available; choose either, both, or none based on your preferences.

- Review Route Before Creation—Check this check box if you want to review and edit the circuit route before the circuit is created.
- VT-DS3 Mapped Conversion—(STS circuits only) Check this check box to create a circuit using the portless transmultiplexing interface of the DS3XM-12 card.

Step 3 Choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 4 If you selected VT-DS3 Mapped Conversion in Step 2, complete the following substeps; otherwise, continue with Step 5:

a. Click **Next**.

b. In the Conversion Circuit Route Constraints area, complete the following:

- Node—Choose a node with a DS3XM-12 card installed.
- Slot—Choose the slot where a DS3XM-12 card is installed.

- DS3 Mapped STS—If applicable, choose **Circuit Dest** to indicate that the STS is the circuit destination, or **Circuit Source** to indicate that the STS is the circuit source.

Step 5 If you selected Review Route Before Creation in Step 2, complete the following substeps. If not, continue with Step 6.

a. Click **Next**.

b. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the "NTP-A182 Create a Manually Routed DS-1 Circuit" procedure on page 6-12.

Step 6 Click **Finish**.

Step 7 Return to your originating procedure (NTP).

DLP-A399 Install a UBIC-H EIA

Purpose	This task installs a Universal Backplane Interface Connector—Horizontal (UBIC-H) EIA.
Tools/Equipment	#2 Phillips screwdriver Small slot-head screwdriver 6 perimeter screws, 6-32 x 0.375-inch Phillips head (P/N 48-0422-01) UBIC-H, A side (15454-EIA-UBICH-A) EIA panel and/ or UBIC-H, B side (15454-EIA-UBICH-B) EIA panel
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution Always use an electrostatic discharge (ESD) wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Note UBIC EIAs can only be installed on shelf assembly 15454-SA-HD. 15454-SA-HD shelf assemblies are differentiated from other shelf assemblies by the blue hexagon symbol, which indicates the available high-density slots, found under Slots 1 through 3 and 15 through 17.

Note UBIC-V or UBIC-H EIAs are required when using high-density (48-port DS-3 and 12-port DS3XM) electrical cards.

Step 1 Locate the correct UBIC-H EIA for the side you want to install and remove the UBIC-H EIA from the packaging.

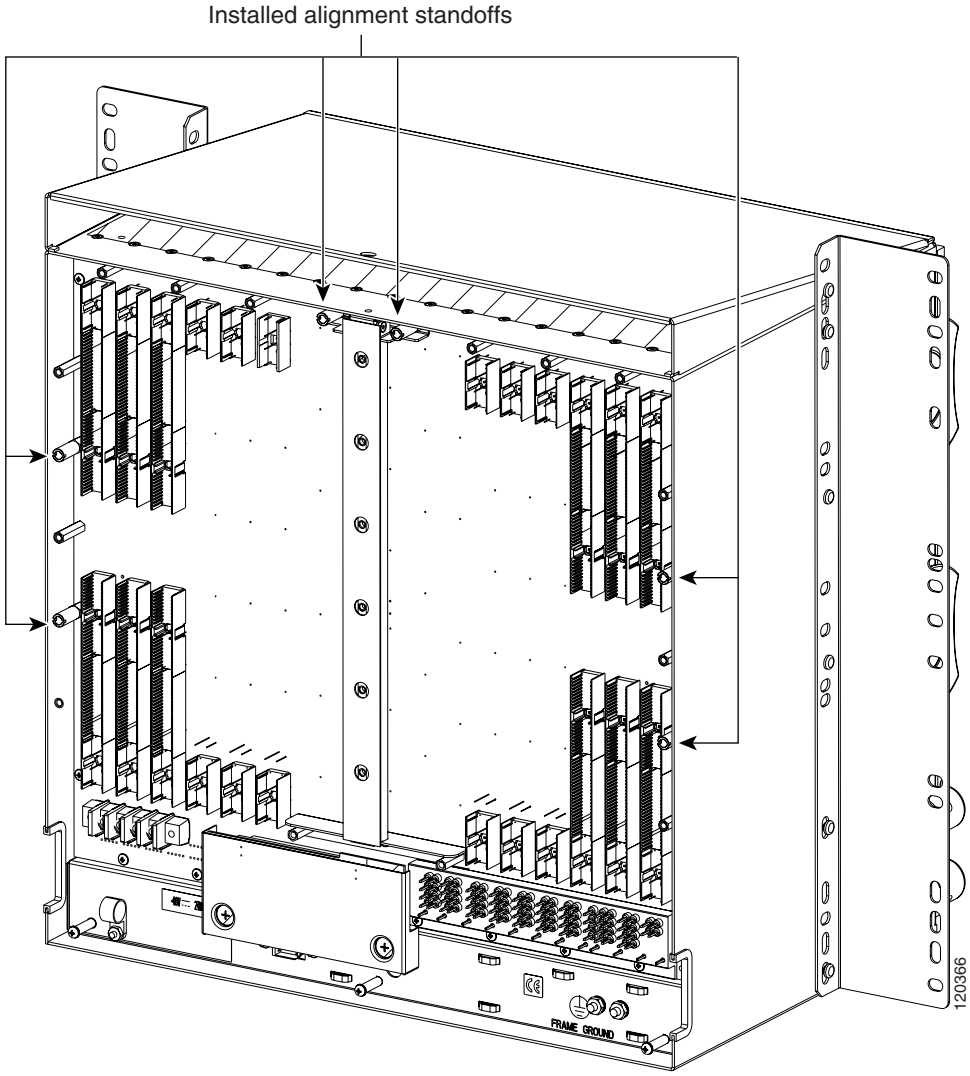
Step 2 Verify that none of the pins on the UBIC-H EIA are bent.

Step 3 If present, remove the yellow connector protectors.

Step 4 If screws are present in the alignment standoff holes, use a Phillips screwdriver to remove them.

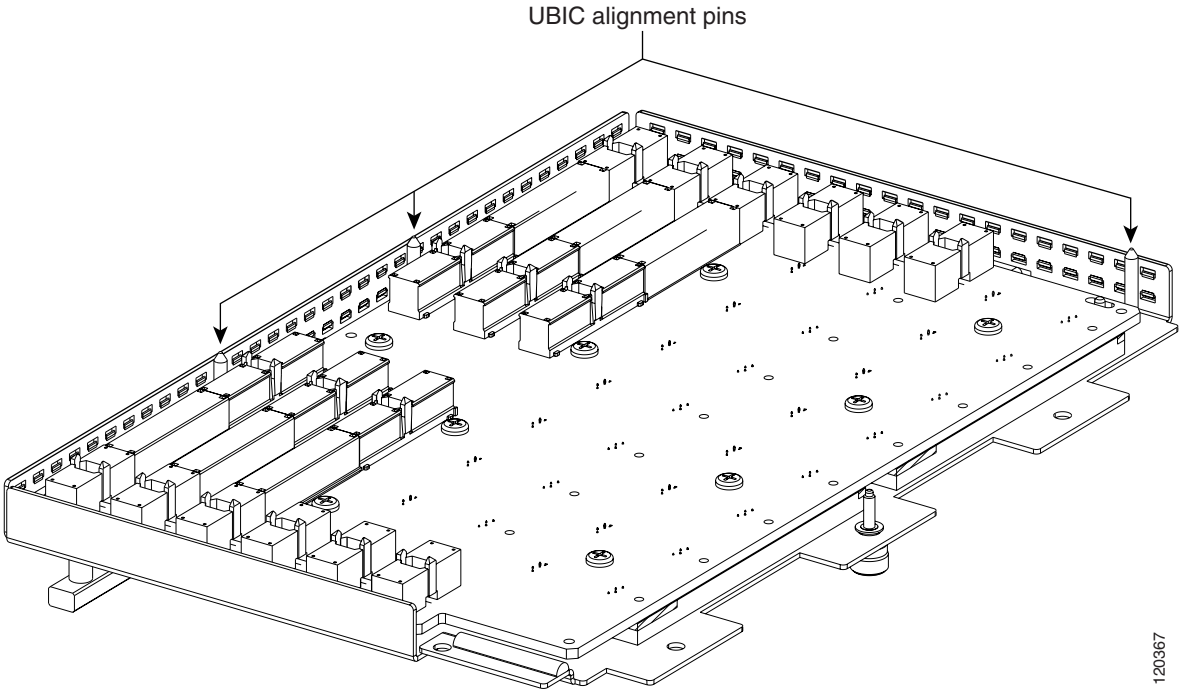
Step 5 Use a flathead screwdriver or 5/16-inch deep socket wrench to tighten the standoffs at 8 to 10 inch pound-force (lbf-in) (9.2 to 11.5 centimeter kilogram-force[kgf-cm]). Figure 20-22 shows the alignment standoffs installed on the shelf.

Figure 20-22 Installed Alignment Standoffs



Step 6 Line up the alignment pins on the UBIC-H EIA (Figure 20-23) with the alignment standoffs on the shelf and push the UBIC-H EIA with consistent pressure until the pins and standoffs fit together firmly.

Figure 20-23 UBIC-H Alignment Pins

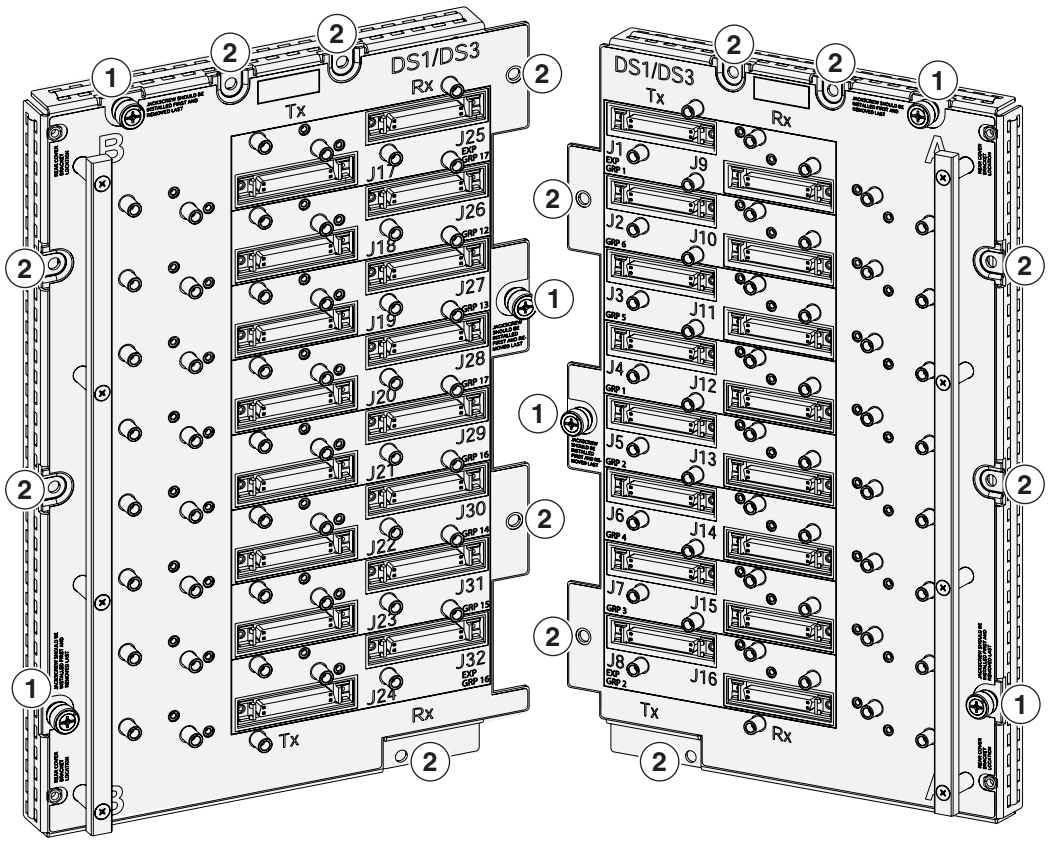


Caution Do not force the UBIC-H EIA onto the shelf if you feel strong resistance.

Step 7 Locate the three jack screws on the UBIC-H (Figure 20-24). Starting with any jack screw, tighten the thumb screw a few turns and move to the next one, turning each thumb screw a few turns at a time until all three screws are hand tight (Figure 20-25).

Caution Tightening the jack screws unevenly could cause damage to the UBIC-H connectors.

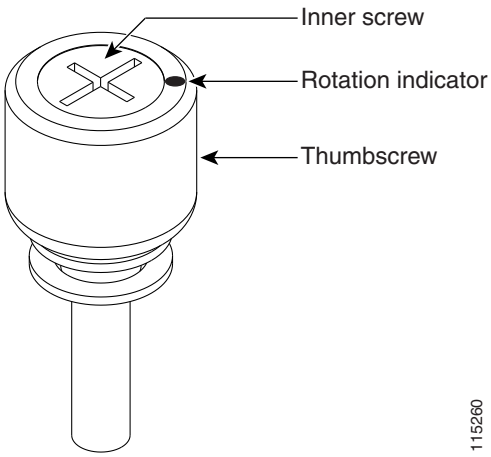
Figure 20-24 UBIC-H EIA Screw Locations



(1) Jack screws (3)

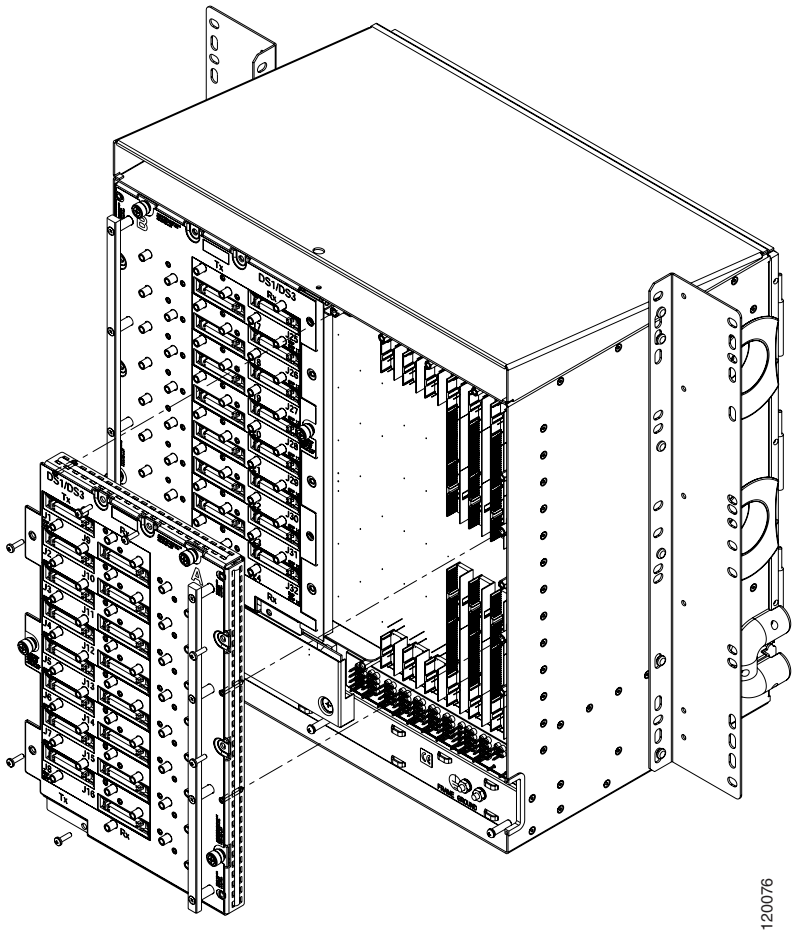
(2) Perimeter screws, 6-32 x 0.375-inch Phillips head (7)

Figure 20-25 UBIC-H EIA Jack Screw



Step 8 Use a Phillips screwdriver to install five of the six perimeter screws (Figure 20-26), leaving the lower perimeter screw out, and torque to 8 to 10 lbf-inch (9.2 to 11.5 kgf-cm) to secure the cover panel to the backplane.

Figure 20-26 Installing the UBIC-H EIA



Step 9 Reinstall the lower backplane cover using a Phillips screwdriver, inserting five screws and tightening until seated.

Step 10 Return to your originating procedure (NTP).

CHAPTER 21

DLPs A400 to A499

Note The terms “Unidirectional Path Switched Ring” and “UPSR” may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as “Path Protected Mesh Network” and “PPMN,” refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

DLP-A412 Install the DCU Shelf Assembly

Purpose	If you are installing dispersion compensation modules, use this task to install the dispersion compensation unit (DCU) chassis.
Tools/Equipment	#2 Phillips screwdriver Crimping tool #14 AWG wire and lug
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Step 1 The DCU chassis requires 1 RU in a standard 19-inch (482.6-mm) or 23-inch (584.2-mm) rack. Locate the RMU space specified in your site plan.

Step 2 Two sets of mounting brackets are included with the DCU mounting kit, one set each, for 19-inch (482.6-mm) or 23-inch (584.2-mm) racks. Verify that your chassis is equipped with the correct set of brackets for your rack. Change the brackets as required.

Step 3 Align the chassis with the rack mounting screw holes; one at a time, insert and tighten the four screws.

Step 4 Connect a frame ground to the ground terminal provided on either side of the chassis. Use minimum #14 AWG wire.

Step 5 Return to your originating procedure (NTP).

DLP-A416 View Circuit Information

Purpose	This task enables you to view information about circuits, such as name, type, size, and direction.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate Cisco Transport Controller (CTC) view:

- To view circuits for an entire network, from the View menu, choose **Go to Network View**.
- To view circuits that originate, terminate, or pass through a specific node, from the View menu, choose **Go to Other Node**, then choose the node you want to search and click **OK**.
- To view circuits that originate, terminate, or pass through a specific card, in node view, double-click the card containing the circuits you want to view.

Note In node or card view, you can change the scope of the circuits that appear by choosing Card (in card view), Node, or Network from the Scope drop-down list in the bottom right corner of the Circuits window.

Step 2 Click the **Circuits** tab. The Circuits tab shows the following information:

- Name—Name of the circuit. The circuit name can be manually assigned or automatically generated.
- Type—Circuit types are STS (STS circuit), VT (VT circuit), VTT (VT tunnel), VAP (VT aggregation point), OCHNC (dense wavelength division multiplexing [DWDM] optical channel network connection [OCHNC]), STS-v (STS virtual concatenated [VCAT] circuit), and VT-v (VT VCAT circuit).
- Size—Circuit size. VT circuit size is VT1.5 or VT2. STS circuit sizes are 1, 3c, 6c, 9c, 12c,18c, 24c, 36c, 48c, and 192c. OCHNC circuit sizes are Equipped not specific, Multi-rate, 2.5 Gbps No FEC (forward error correction), 2.5 Gbps FEC, 10 Gbps No FEC, and 10 Gbps FEC (DWDM only; refer to the *Cisco ONS 15454 DWDM Procedure Guide*). VCAT circuit sizes are VT1.5-*n*v, STS-1-*n*v, STS-3c-*n*v, and STS-12c-*n*v, where *n* is the number of members.
- OCHNC Wlen—(DWDM only) For OCHNCs, the provisioned wavelength. For more information, refer to the *Cisco ONS 15454 DWDM Procedure Guide*.
- Direction—The circuit direction, either two-way or one-way.
- OCHNC Dir—(DWDM only) For OCHNCs, the direction of the OCHNC, either East to West or West to East. For more information, refer to the *Cisco ONS 15454 DWDM Procedure Guide*.
- Protection—The type of circuit protection. See Table 21-1 for a list of protection types.

Table 21-1 Circuit Protection Types

Protection Type	Description
1+1	The circuit is protected by a 1+1 protection group.
2F BLSR	The circuit is protected by a two-fiber bidirectional line switched ring (BLSR).
4F BLSR	The circuit is protected by a four-fiber BLSR.
2F-PCA	The circuit is routed on a protection channel access (PCA) path on a two-fiber BLSR. PCA circuits are unprotected.
4F-PCA	The circuit is routed on a PCA path on a four-fiber BLSR. PCA circuits are unprotected.
BLSR	The circuit is protected by a both a two-fiber and a four-fiber BLSR.
DRI	The circuit is protected by a dual-ring interconnect (both path protection and BLSR).
N/A	A circuit with connections on the same node is not protected.
PCA	The circuit is routed on a PCA path on both two-fiber and four-fiber BLSRs. PCA circuits are unprotected.
Protected	The circuit is protected by diverse SONET topologies, for example, a BLSR and a path protection configuration, or a path protection and 1+1 configuration.
Splitter	The circuit is protected by the protect transponder (TXPP_MR_2.5G) splitter protection. Refer to the *Cisco ONS 15454 DWDM Procedure Guide*.
Unknown	A circuit has a source and destination on different nodes and communication is down between the nodes. This protection type appears if not all circuit components are known.
Unprot (black)	A circuit with a source and destination on different nodes is not protected.
Unprot (red)	A circuit created as a fully protected circuit is no longer protected due to a system change, such as removal of a BLSR or 1+1 protection group.
Path Protection	The circuit is protected by a path protection configuration.
Y-Cable	The circuit is protected by a transponder or muxponder card Y-cable protection group. Refer to the *Cisco ONS 15454 DWDM Procedure Guide*.

- Status—The circuit status. Table 21-2 lists the circuit statuses that can appear.

Table 21-2 Cisco ONS 15454 Circuit Status

Status	Definition/Activity
CREATING	CTC is creating a circuit.
DISCOVERED	CTC created a circuit. All components are in place and a complete path exists from the circuit source to the circuit destination.
DELETING	CTC is deleting a circuit.

Table 21-2 Cisco ONS 15454 Circuit Status (continued)

Status	Definition/Activity
PARTIAL	A CTC-created circuit is missing a cross-connect or network span, a complete path from source to destination(s) does not exist, or an alarm interface panel (AIP) change occurred on one of the circuit nodes and the circuit is in need of repair. (AIPs store the node MAC address.) In CTC, circuits are represented using cross-connects and network spans. If a network span is missing from a circuit, the circuit status is PARTIAL. However, an PARTIAL status does not necessarily mean a circuit traffic failure has occurred, because traffic might flow on a protect path. Network spans are in one of two states: up or down. On CTC circuit and network maps, up spans are shown as green lines, and down spans are shown as gray lines. If a failure occurs on a network span during a CTC session, the span remains on the network map but its color changes to gray to indicate the span is down. If you restart your CTC session while the failure is active, the new CTC session cannot discover the span and its span line will not appear on the network map. Subsequently, circuits routed on a network span that goes down will appear as DISCOVERED during the current CTC session, but they will appear as PARTIAL to users who log in after the span failure.
DISCOVERED_TL1	A TL1-created circuit or a TL1-like CTC-created circuit is complete. A complete path from source to destination(s) exists.
PARTIAL_TL1	A TL1-created circuit or a TL1-like CTC-created circuit is missing a cross-connect, and a complete path from source to destination(s) does not exist.
CONVERSION_PENDING	An existing circuit in a topology upgrade is set to this state. The circuit returns to the DISCOVERED state once the topology upgrade is complete. For more information about topology upgrades, refer to the “SONET Topologies and Upgrades” chapter in the *Cisco ONS 15454 Reference Manual*.
PENDING_MERGE	Any new circuits created to represent an alternate path in a topology upgrade are set to this status to indicate that it is a temporary circuit. These circuits can be deleted if a topology upgrade fails.For more information about topology upgrades, refer to the “SONET Topologies and Upgrades” chapter in the *Cisco ONS 15454 Reference Manual*.
DROP_PENDING	A circuit is set to this status when a new circuit drop is being added.
ROLL_PENDING	A circuit roll is awaiting completion or cancellation.

- Source—The circuit source in the format: *node/slot(card type)/port "port name"/STS/VT*. (The port name will appear in quotes.) Node and slot will always appear; *port "port name"/STS/VT* might appear, depending on the source card, circuit type, and whether a name is assigned to the port. If the port is on a MRC-12 or MRC-2.5G-4 card, the port format is *PPM-port_number*. If the circuit size is a concatenated size (3c, 6c, 12c, etc.), synchronous transport signals (STSs) used in the circuit are indicated by an ellipsis, for example, "S7..9," (STSs 7, 8, and 9) or S10..12 (STS 10, 11, and 12).
- Destination—The circuit destination in same format (*node/slot[card type]/port "port name"/STS/VT*) as the circuit source.
- # of VLANS—The number of VLANs used by an Ethernet circuit.
- # of Spans—The number of internode links that constitute the circuit. Right-clicking the column shows a shortcut menu from which you can choose Span Details to show or hide circuit span detail. For each node in the span, the span detail shows the *node/slot (card type)/port/STS/VT*.
- State—The circuit service state, IS, OOS, or OOS-PARTIAL. The circuit service state is an aggregate of the service states of its cross-connects:
  - IS—All cross-connects are in the In-Service and Normal (IS-NR) service state.
  - OOS—All cross-connects are in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) and/or Out-of-Service and Management, Maintenance (OOS-MA,MT) service state.
  - OOS-PARTIAL—At least one cross-connect is IS-NR and others are OOS-MA,DSBLD and/or OOS-MA,MT.

Step 3 Return to your originating procedure (NTP).

DLP-A418 Install Public-Key Security Certificate

Purpose	This task installs the ITU Recommendation X.509 public-key security certificate. The public-key certificate is required to run Software Release 4.1 or later.
Tools/Equipment	None
Prerequisite Procedures	This task is performed during the "DLP-A60 Log into CTC" task on page 17-60. You cannot perform it outside of this task.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 If the Java Plug-in Security Warning dialog box appears, choose one of the following options:

- Yes (Grant This Session)—Installs the public-key certificate to your PC only for the current session. After the session is ended, the certificate is deleted. This dialog box will appear the next time you log into the ONS 15454.
- No (Deny)—Denies permission to install certificate. If you choose this option, you cannot log into the ONS 15454.
- Always (Grant Always)—Installs the public-key certificate and does not delete it after the session is over. Cisco recommends this option.

- More Details (View Certificate)—Allows you to view the public-key security certificate.

Step 2 If the Login dialog box appears, continue with Step 3. If the Change Java Policy File dialog box appears, complete this step. The Change Java Policy File dialog box appears if CTC finds a modified Java policy file (.java.policy) on your PC. In Software Release 4.0 and earlier, the Java policy file was modified to allow CTC software files to be downloaded to your PC. The modified Java policy file is not needed in Software R4.1 and later, so you can remove it unless you will log into ONS 15454s running software earlier than R4.1. Choose one of the following options:

- Yes—Removes the modified Java policy file from your PC. Choose this option only if you will log into ONS 15454s running Software R4.1 software or later.
- No—Does not remove the modified Java policy file from your PC. Choose this option if you will log into ONS 15454s running Software R4.0 or earlier. If you choose No, this dialog box will appear every time you log into the ONS 15454. If you do not want it to appear, check the **Do not show the message again** check box.

Caution If you delete the Java policy file, you cannot log into nodes running Software R4.0 and earlier. If you delete the file and want to log into an ONS 15454 running an earlier release, insert the software CD for the release into your PC CD-ROM and run the CTC setup wizard to reinstall the Java policy file.

Step 3 Return to your originating procedure (NTP).

DLP-A421 Provision G-Series and CE-1000-4 Flow Control Watermarks

Purpose	This task provisions the buffer memory levels for flow control on G-Series and CE-1000-4 Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, double-click the G-Series or CE-1000-4 card graphic to open the card.

Step 2 Click the **Provisioning** > **Port** tabs.

Step 3 In the Water Marks column, click the cell in the row for the appropriate port.

Step 4 To provision the Low Latency flow control watermark:

a. Choose **Low Latency** from the drop-down list.

The Flow Ctrl Lo and Flow Ctrl Hi values change.

b. Click **Apply**.

Step 5 To provision a Custom flow control watermark:

a. Choose **Custom** from the drop-down list.

b. In the Flow Ctrl Lo column, click the cell in the row for the appropriate port.

c. Enter a value in the cell. The Flow Ctrl Lo value has a valid range from 1 to 510 and must be lower than the Flow Ctrl Hi value.

   This value sets the flow control threshold for sending the signal to the attached Ethernet device to resume transmission.

d. In the Flow Ctrl Hi column, click the cell in the row for the appropriate port.

e. Enter a value in the cell. The Flow Ctrl Hi value has a valid range from 2 to 511 and must be higher than the Flow Ctrl Lo value.

   This value sets the flow control threshold for sending the signal to the attached Ethernet device to pause transmission.

f. Click **Apply**.

Note Low watermarks are optimum for low latency subrate applications, such as voice-over-IP (VoIP) using an STS-1. High watermarks are optimum when the attached Ethernet device has insufficient buffering, best effort traffic, or long access line lengths.

Step 6 Return to your originating procedure (NTP).

DLP-A422 Verify BLSR Extension Byte Mapping

Purpose	This task verifies that the extension byte mapping is the same on BLSR trunk (span) cards that will be connected after a node is removed from a BLSR.
Tools/Equipment	OC-48 AS cards must be installed at one or both ends of the BLSR span that will be connected.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In network view, double-click a BLSR node with OC-48 AS trunk (span) cards that will be reconnected after a BLSR node removal.

Step 2 Double-click one OC-48 AS BLSR trunk card.

Step 3 Click the **Provisioning > Line** tabs.

Step 4 Record on paper the byte in the BLSR Ext Byte column.

Step 5 Repeat Steps 2 through 4 for the second OC-48 AS trunk card.

Step 6 If the node at the other end of the new span contains OC-48 AS trunk cards, repeat Steps 1 through 5 at the node. If it does not have OC-48 AS cards, their trunk cards are mapped to the K3 extension byte. Continue with Step 7.

Step 7 If the trunk cards on each end of the new span are mapped to the same BLSR extension byte, continue with Step 8. If they are not the same, remap the extension byte of the trunk cards at one of the nodes. See the "DLP-A89 Remap the K3 Byte" task on page 17-82.

Step 8 Return to your originating procedure (NTP).

DLP-A428 Install Fiber-Optic Cables in a 1+1 Configuration

Purpose	This task installs fiber-optic cables on optical (OC-N) cards in a 1+1 linear configuration.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors, page 15-15
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note The Cisco OC-3 IR/STM-1 SH, OC-12 IR/STM-4 SH, and OC-48 IR/STM-16 SH interface optics, all working at 1310 nm, are optimized for the most widely used SMF-28 fiber-optic cable, available from many suppliers.

Note Corning MetroCor fiber-optic cable is optimized for optical interfaces that transmit at 1550 nm or in the C and L DWDM windows. This fiber-optic cable targets interfaces with higher dispersion tolerances than those found in OC-3 IR/STM-1 SH, OC-12 IR/STM-4 SH, and OC-48 IR/STM-16 SH interface optics. If you are using Corning MetroCor fiber-optic cable, OC-3 IR/STM-1 SH, OC-12 IR/STM-4 SH, and OC-48 IR/STM-16 SH interface optics will become dispersion limited before they will become attenuation limited. In this case, consider using OC-3 LR/STM-1 LH, OC-12 LR/STM-4 LH, and OC-48 LR/STM-16 LH cards instead of OC-3 IR/STM-1 SH, OC-12 IR/STM-4 SH, and OC-48 IR/STM-16 SH cards.

Note With all fiber types, network planners/engineers should review the relative fiber type and optics specifications to determine attenuation, dispersion, and other characteristics to ensure appropriate deployment.

Step 1 Plan your fiber connections. Use the same plan for all 1+1 nodes.

Step 2 Align the keyed ridge of the cable connector with the transmit (Tx) connector of a working OC-N card at one node and plug the other end of the fiber-optic cable into the receive (Rx) connector of a working OC-N card at the adjacent node. The card displays an SF LED if the transmit and receive fiber-optic cables are mismatched (one fiber-optic cable connects a receive port on one card to a receive port on another card, or the same situation with transmit ports). Figure 19-1 on page 19-5 shows the cable location.

Step 3 Repeat Steps 1 and 2 for the corresponding protect ports on the two nodes and for all other working/protect port pairs that you want to place in a 1+1 configuration.

Step 4 Return to your originating procedure (NTP).

DLP-A430 View Spanning Tree Information

Purpose	This task allows you to view E-Series Ethernet circuits and the Ethernet front ports operating with the Spanning Tree Protocol (STP). The E-Series card supports up to eight STPs per node. For more information about STP, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, click the **Maintenance > Ether Bridge > Circuits** tabs.

Step 2 In the EtherBridge Circuits window, you can view the following information:

- Type—Identifies the type of Ethernet circuit mapped to the spanning tree, such as EtherSwitch point-to-point.
- Circuit Name/Port—Identifies the circuit name for the circuit in the spanning tree. This column also lists the Ethernet slots and ports mapped to the spanning tree for the node.
- STP ID—Shows the Spanning Tree Protocol ID number.
- VLANS—Lists the VLANs associated with the circuit or port.

Step 3 Return to your originating procedure (NTP).

DLP-A431 Change the JRE Version

Purpose	This task changes the JRE version, which is useful if you would like to upgrade to a later JRE version from earlier one without using the software CD. This does not affect the browser default version. After selecting the desired JRE version, you must exit CTC. The next time you log into a node, the new JRE version will be used.
Tools	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu, choose **Preferences**.

Step 2 Click the **JRE** tab. The JRE tab shows the current JRE version and the recommended version.

Step 3 Click the **Browse** button and navigate to the JRE directory on your computer.

Step 4 Choose the JRE version.

Step 5 Click **OK**.

Step 6 From the File menu, choose **Exit**.

Step 7 In the confirmation dialog box, click **Yes**.

Step 8 Complete the "DLP-A60 Log into CTC" task on page 17-60.

Step 9 Return to your originating procedure (NTP).

DLP-A433 Enable Node Secure Mode

Purpose	This task enables secure mode on the ONS 15454. When secure mode is enabled, two IPv4 addresses are assigned to the node: one address is assigned to the backplane LAN port and the other is assigned to the TCC2P RJ-45 TCP/IP (LAN) port.
Tools/Equipment	TCC2P cards must be installed.
Prerequisite Procedures	NTP-A108 Back Up the Database, page 15-5 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution The IPv4 address assigned to the TCC2P TCP/IP (LAN) port must reside on a different subnet from the backplane LAN port and the ONS 15454 default router. Verify that the new TCC2P IP address meets this requirement and is compatible with the ONS 15454 network IP4v addresses.

Note The node will reboot after you complete this task, causing a temporary disconnection between the CTC computer and the node.

Step 1 In node view, click the **Provisioning > Security > Data Comm** tabs.

Step 2 Click **Change Mode**.

Step 3 Review the information on the Change Secure Mode wizard page, then click **Next**.

Step 4 On the TCC Ethernet Port page, enter the IP address and subnet mask for the TCC2P LAN (TCP/IP) port. The IPv4 address cannot reside on the same subnet as the backplane LAN port or the ONS 15454 default router.

Step 5 Click **Next**.

Step 6 On the Backplane Ethernet Port page, modify the backplane IPv4 address, subnet mask, and default router, if needed. (Normally, you do not need to modify these fields if no ONS 15454 network changes have occurred.)

Step 7 Click **Next**.

Step 8 On the SOCKS Proxy Server Settings page, choose one of the following options:

- External Network Element (ENE)—If selected, the CTC computer is only visible to the ONS 15454 where the CTC computer is connected. The computer is not visible to the data communications channel (DCC)-connected nodes. By default, SOCKS proxy is not enabled for an ENE. If SOCKS proxy is disabled, the NE cannot communicate with other secure mode NEs behind the firewall.
- Gateway Network Element (GNE)—If selected, the CTC computer is visible to other DCC-connected nodes. The node prevents IP traffic from being routed between the DCC and the LAN port. By default, configuring the secure node as a GNE also enables SOCKS proxy for communication with other secure NEs.

Step 9 Click **Finish**.

Within the next 30 to 40 seconds, the TCC2P cards reboot. CTC switches to network view, and the CTC Alerts dialog box appears. In network view, the node changes to gray and a DISCONNECTED condition appears.

Step 10 In the CTC Alerts dialog box, click **Close**. Wait for the reboot to finish. (This might take several minutes.)

Step 11 After the DISCONNECTED condition clears, complete the following steps to suppress the backplane IP address from display in CTC and the LCD. If you do not want to suppress the backplane IP address display, continue with Step 12.

a. Display the node in node view.

b. Click the **Provisioning > Security > Data Comm** tabs.

c. If you do not want the IPv4 address to appear on the LCD, in the LCD IP Setting field, choose **Suppress Display**.

d. If you do not want the IPv4 address to appear in CTC, check the **Suppress CTC IP Address** check box. This removes the IPv4 address from display in the CTC information area and from the Provisioning > Security > Data Comm tab.

e. Click **Apply**.

Note After you turn on secure mode, the TCC2P IP (LAN) port address becomes the node's IP address. The backplane LAN port has a different IPv4 address.

Step 12 Return to your originating procedure (NTP).

DLP-A434 Lock Node Security

Purpose	This task locks the secure mode configuration on an ONS 15454. When secure mode is locked, two IP addresses must always be provisioned on the ONS 15454: one for the TCC2P TCP/IP (LAN) port and one for the backplane LAN port.
Tools/Equipment	TCC2P cards must be installed.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 DLP-A433 Enable Node Secure Mode, page 21-10
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution When a node is locked, it cannot be unlocked by any user or action. It can only be changed by Cisco Technical Support. Even if the node's database is deleted and another unlocked database is loaded, the node will remain locked. Do not proceed unless you want the node to permanently retain the current secure configuration including dual IP addresses.

Note For more information about secure mode, refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 1 Click the **Provisioning > Security > Data Comm** tabs.

Step 2 Click **Lock**.

Step 3 In the Confirm Lock Secure Mode dialog box, click **Yes**.

Step 4 Return to your originating procedure (NTP).

DLP-A435 Modify Backplane Port IP Settings in Secure Mode

Purpose	This task modifies the ONS 15454 backplane IPv4 address, subnet mask, default router. In addition, if IPv6 is enabled, this task modifies the IPv6 Configuration like IPv6 Address, Prefix Length and IPv6 Default Router. It also modifies settings that control backplane IP address visibility in CTC and the ONS 15454 LCD. To perform this task, secure mode must be enabled.
Tools/Equipment	TCC2P cards must be installed.
Prerequisite Procedures	NTP-A108 Back Up the Database, page 15-5 DLP-A60 Log into CTC, page 17-60 DLP-A433 Enable Node Secure Mode, page 21-10
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution Provisioning an IP address that is incompatible with the ONS 15454 network might be service affecting.

Caution This task cannot be performed on a secure mode NE that has been locked.

Step 1 Click the **Provisioning > Security > Data Comm** tabs.

Step 2 Modify the following fields, as necessary:

- IP Address
- Subnet Mask
- Default Router
- LCD IP Setting—choose one of the following:
  - **Allow Configuration**—Displays the backplane IP address on the LCD and allows the IP address to be changed using the LCD buttons.
  - **Display only—**Displays the backplane IP address on the LCD but does not allow the IP address to be changed using the LCD buttons.
  - **Suppress Display**—Suppresses the display of the IP address on the LCD.
- Suppress CTC IP Address—If checked, displays node IP information only to Superusers (that is, not to Provisioning, Maintenance, or Retrieve-level users) in the CTC Provisioning > General > Network tab; the Provisioning > Security > Data Comm tab, and the CTC node view information area.
- IPv6 Configuration—Allows provisioning of IPv6 addresses. After you provision an IPv6 address, you can access the device using the IPv6 address. Configure these settings only if you want to enable IPv6 on the node. IPv6 cannot be configured using the LCD push buttons.
  - **Enable IPv6**—Select this check box to assign an IPv6 address to the node. The IPv6 Address, Prefix Length, and IPv6 Default Router fields are enabled only if this check box is selected. The check box is disabled by default. The valid range for Prefix Length is 0 - 128.

Note IPv6 can be enabled only when 'Enable SOCKS Proxy on Port' check box is enabled. For IPv6 connectivity, once the SOCKS Proxy is enabled, the ONS 15454 node can be configured as 'External Network Element (ENE)', 'Gateway Network Element (GNE)', or 'SOCKS proxy only' by enabling the suitable radio button.

Note By default, when IPv6 is enabled, the node processes both IPv4 and IPv6 packets on the LAN interface. If you want the node to process only IPv6 packets, you need to disable IPv4 on the node. For more information, see DLP-A512 Change Node Access and PM Clearing Privilege, page 22-5

- **IPv6 Address**—Enter the IPv6 address that you want to assign to the node. This IP address is the global unicast IPv6 address. This field is disabled if the **Enable IPv6** check box is not selected.
- **Prefix Length**—Enter the prefix length of the IPv6 address. This field is disabled if the **Enable IPv6** check box is not selected. The valid range for Prefix Length is 0 - 128.
- **IPv6 Default Router**—Enter the IPv6 address of the default router of the IPv6 NE. This field is disabled if the **Enable IPv6** check box is not selected. This field can be set to 0 or 0::0 or 0:0:0:0:0:0:0:0 if any of the following are true:

  The ONS 15454 is not connected to a LAN.

  The ONS 15454 is provisioned as an end network element (ENE).

Note The ONS 15454 uses NAT-PT internally to support native IPv6. NAT-PT uses the IPv4 address range 128.x.x.x for packet translation. Do not use this address range when you enable IPv6 feature.

Caution Ensure that the IPv6 address assigned to the node is unique in the network. Duplicate IP addresses in the same network cause loss of visibility.

Step 3 Click **Apply**.

If you changed the IPv4 address, subnet mask, or default router, the node will reboot. This will take 5 to 10 minutes.

Step 4 Return to your originating procedure (NTP).

DLP-A436 Disable Node Security Mode

Purpose	This task disables the ONS 15454 secure mode, meaning dual-IP addresses are no longer supported.With secure mode disabled, only one IP address can be provisioned for both the backplane LAN port and the TCC2P TCP/IP (LAN) port. If secure mode is disabled for a node, that node cannot identify other network nodes that are in secure mode.
Tools/Equipment	TCC2P cards must be installed.
Prerequisite Procedures	NTP-A108 Back Up the Database, page 15-5 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note The node will reboot after you complete this task, causing a temporary disconnection between the CTC computer and the node.

Note If you change an NE from secure mode to the default (repeater) mode, the backplane IP address becomes the node IP address.

Note This task cannot be performed if the NE's security mode configuration is locked. If secure mode is locked, you must contact Cisco Technical Support to change the node configuration.

Step 1 Click the **Provisioning > Security > Data Comm** tabs.

Step 2 Click **Change Mode**.

Step 3 Review the information on the Change Secure Mode wizard page, then click **Next**.

Step 4 On the Node IP Address page, choose the address you want to assign to the node:

- Backplane Ethernet (LAN) Port—Assigns the backplane IP address as the node IP address.
- TCC Ethernet (LAN) Port—Assigns the TCC2P port IP address as the node IP address.
- New IP Address—Allows you to define a new IP address. If you choose this option, enter the new IP address, subnet mask, and default router IP address.

Step 5 Click **Next**.

Step 6 On the SOCKS Proxy Server Settings page, choose one of the following:

- **External Network Element (ENE)**—If selected, SOCKS proxy is disabled by default, and the CTC computer is only visible to the ONS 15454 where the CTC computer is connected. The computer is not visible to the secure mode, DCC-connected nodes. Firewall is enabled, which means that the node prevents IP traffic from being routed between the DCC and the LAN port.
- **Gateway Network Element (GNE)**—If selected, the CTC computer is visible to other DCC-connected nodes, and SOCKS proxy remains enabled. However, the node prevents IP traffic from being routed between the DCC and the LAN port.

- **Proxy-only**—If selected, the ONS 15454 responds to CTC requests with a list of DCC-connected nodes within the firewall for which the node serves as a proxy. The CTC computer is visible to other DCC-connected nodes. The node does not prevent traffic from being routed between the DCC and LAN port.

Step 7 Click **Finish**.

Within the next 30 to 40 seconds, the TCC2P cards reboot. CTC switches to network view, and the CTC Alerts dialog box appears. In network view, the node changes to gray and a DISCONNECTED condition appears.

Step 8 In the CTC Alerts dialog box, click **Close**. Wait for the reboot to finish. (This might take several minutes.)

Step 9 Return to your originating procedure (NTP).

DLP-A437 Change a VCAT Member Service State

Purpose	This task displays the Edit Circuit window for VCAT members, where you can change the service state.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 VCAT circuits must exist on the network. See the "NTP-A264 Create an Automatically Routed VCAT Circuit" procedure on page 6-81 or the "NTP-A265 Create a Manually Routed VCAT Circuit" procedure on page 6-86.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note CTC only permits you to change the state of a member that does not use the link capacity adjustment scheme (LCAS) if the new state matches the In Group VCAT state of the other members, or the new state is an Out of Group VCAT state. The In Group VCAT state indicates that a member has cross-connects in the IS-NR; OOS-MA,AINS; or OOS-AU,MT service states. For non-LCAS VCAT members, the Out of Group VCAT state is the OOS-MA,DSBLD service state.

Step 1 In node or network view, click the **Circuits** tab.

Step 2 Click the VCAT circuit that you want to edit, then click **Edit**.

Step 3 Click the **Members** tab.

Step 4 Select the member that you want to change. To choose multiple members, press **Ctrl** and click each member.

Step 5 From the Tools menu, choose **Set Circuit State**.

Note You can also change the state for all members listed in the Edit Circuit window using the State tab. Another alternative is to click the Edit Member button to access the Edit Member Circuit window for the selected member, and click the State tab.

Step 6 From the Target Circuit Admin State drop-down list, choose the administrative state:

- IS—Puts the member cross-connects in the IS-NR service state.
- OOS,DSBLD—Puts the member cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
- IS,AINS—Puts the member cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
- OOS,MT—Puts the member cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete.
- OOS,OOG—(LCAS and Sw-LCAS VCAT only) Puts VCAT member cross-connects in the Out-of-Service and Management, Out-of-Group (OOS-MA,OOG) service state. This administrative state is used to put a member circuit out of the group and to stop sending traffic.

Note the following behavior of the two VCAT members on ML-Series cards (both SW-LCAS and non-LCAS members):

- When changing a member from the IS-NR to the OOS-MT, MT or the OOS-MA,DSBLD service state, changing the service state of the first member causes both members to change service state autonomously.
- When changing a member from the OOS-MA,DSBLD to the OOS-MT, MT or the IS-NR service state, you must begin with the second VCAT member. For example, change the service state of the second member first, and then the first member. You cannot change the service state of the first member if the second member is in another service state.

Step 7 Click **Apply**.

Step 8 To close the Edit Circuit window, choose **Close** from the File menu.

Step 9 Return to your originating procedure (NTP).

DLP-A438 Change General Port Settings for the FC_MR-4 Card

Purpose	This task changes the general port settings for FC_MR-4 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the “Network Element Defaults” appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 In node view, double-click the FC_MR-4 card where you want to change the port settings.

Step 2 Click the **Provisioning > Port > General** tabs.

Step 3 Modify any of the settings described in Table 21-3 by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value or select or deselect a check box.

Step 4 Click **Apply**.

Table 21-3 FC_MR-4 Card General Port Settings

Parameter	Description	Options
Port	(Display only) Port number.	1 through 4
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 20-8. **Note** If this port's Fibre Channel or FICON link will be discovered by the Cisco MDS Fabric Manager for use with a Cisco MDS 9000 switch, you must provision the Fiber Channel/FICON port name to the following string: FC: <switch> <interface> Where <switch> is the DNS name or IPv4/v6 address of the Cisco MDS 9000 switch, and <interface> is the card slot/port of the FC_MR-4 port you are assigning a name. Example: FC: 10.0.0.1 fc2/4
Admin State	Changes the port administrative service state unless network conditions prevent the change.	• IS—Puts the port in-service. The port service state changes to IS-NR. • IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. • OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. • OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT. **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—The port is fully operational and performing as provisioned. • OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic. • OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
Port Rate	Selects the fiber channel interface.	• 1 Gbps • 2 Gbps

Table 21-3 FC_MR-4 Card General Port Settings (continued)

Parameter	Description	Options
Link Rate	(Display only) Shows the actual rate of the port.	—
Max GBIC Rate	(Display only) Shows the maximum Gigabit Interface Converter (GBIC) rate. Cisco supports two GBICs for the FC_MR-4 card (ONS-GX-2FC-SML and ONS-GX-2FC-MMI). If used with another GBIC, "Contact GBIC vendor" is displayed.	—
Link Recovery	Enables or disables link recovery if a local port is inoperable. If enabled, a link reset occurs when there is a loss of transport from a cross-connect switch, protection switch, or an upgrade.	• Yes • No
Media Type	Sets the proper payload value for the Transparent Generic Framing Protocol (GFP-T) frames.	• Fibre Channel - 1 Gbps • Fibre Channel - 2 Gbps • FICON 1 Gbps • FICON 2 Gbps • Unknown

Step 5 Return to your originating procedure (NTP).

DLP-A439 Change Distance Extension Port Settings for the FC_MR-4 Card

Purpose	This task changes the distance extension parameters for FC_MR-4 ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 In node view, double-click the FC_MR-4 card where you want to change the port settings.

Step 2 Click the **Provisioning > Port > Distance Extension** tabs.

Step 3 Modify any of the settings described in Table 21-4 by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value or select or deselect a check box.

Step 4 Click **Apply**.

Table 21-4 FC_MR-4 Card Distance Extension Port Settings

Parameter	Description	Options
Port	(Display only) Port number.	1 through 4
Enable Distance Extension	If checked, allows additional distance by providing a GFP-T based flow control scheme. It enables the node to be a part of a storage area network (SAN) with long-distance, remote nodes. If left unchecked, the remaining options are not available for editing. If Distance Extension is enabled, set the connected Fibre Channel switches to Interop or Open Fabric mode, depending on the Fibre Channel switch. By default, the FC_MR card will interoperate with the Cisco MDS storage products.	—
Auto Detect Credits	If checked, enables the node to detect the transmit credits from a remote node. Credits are used for link flow control and for Extended Link Protocol (ELP) login frames between Fibre Channel/fiber connectivity (FICON) Switch E ports.	—
Credits Available	Sets the number of credits if an ELP login frame setting is missing or if the ELP login frame cannot be detected. Credits Available is editable only if Auto Detect Credits is unchecked. **Note** Longer distances between connected devices need more credits to compensate for the latency introduced by the long-distance link. The value should never be greater than the number of credits supported by the Fibre Channel/FICON port.	Numeric. 2 through 256, multiples of 2 only
Autoadjust GFP Buffer Threshold	If checked, guarantees the best utilization of the SONET/SDH transport in terms of bandwidth and latency.	—
GFP Buffers Available	Sets the GFP buffer depth. GFP Buffers Available is editable if Autoadjust GFP Buffer Threshold is unchecked. For shorter SONET transport distances, Cisco recommends lower values to decrease latency. For longer SONET transport distances, Cisco recommends higher values to provide higher bandwidth.	Numeric. 16 through 1200, multiples of 16 only

Step 5 Return to your originating procedure (NTP).

DLP-A440 Change Enhanced FC/FICON Port Settings for the FC_MR-4 Card

Purpose	This task changes the enhanced FC/FICON parameters for FC_MR-4 ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 In node view, double-click the FC_MR-4 card where you want to change the port settings.

Step 2 Click the **Provisioning > Port > Enhanced FC/FICON** tabs.

Step 3 Modify any of the settings described in Table 21-5 by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value or select or deselect a check box.

Step 4 Click **Apply**.

Table 21-5 FC_MR-4 Card Distance Extension Port Settings

Parameter	Description	Options
Port	(Display only) Port number.	1 through 4

Table 21-5 FC_MR-4 Card Distance Extension Port Settings (continued)

Parameter	Description	Options
Ingress Idle Filtering	If checked, prevents removal of excess Fibre Channel/FICON IDLE codes from SONET transport. IDLEs are 8b10b control words that are sent between frames or appear when there is no data to send. Ingress idle filtering applies only to SONET circuit bandwidth sizes that allow full line rate Fibre Channel/FICON transport. It can be used for interoperability with remote Fibre Channel/FICON over third-party SONET equipment.	—
Maximum Frame Size	Sets the maximum size of a valid frame. This setting prevents oversized performance monitoring accumulation for frame sizes that are above the Fibre Channel maximum. This can occur for Fibre Channel frames with added virtual SAN (VSAN) tags that are generated by the Cisco MDS 9000 switches.	Numeric; 2148 through 2172

Step 5 Return to your originating procedure (NTP).

DLP-A441 Install Electrical Cables on the UBIC-H EIAs

Purpose	This task installs DS-1 and DS-3/EC-1 cables on the UBIC-H EIAs.
Tools/Equipment	3/16-inch flat-head screwdriver DS-1 and DS-3/EC-1 cables, as needed: • 15454-CADS1-H-25 • 15454-CADS1-H-50 • 15454-CADS1-H-75 • 15454-CADS1-H-100 • 15454-CADS1-H-150 • 15454-CADS1-H-200 • 15454-CADS1-H-250 • 15454-CADS1-H-350 • 15454-CADS1-H-450 • 15454-CADS1-H-550 • 15454-CADS1-H-655 • 15454-CADS3-SD • 15454-CADS3-ID • 15454-CADS3-LD
Prerequisite Procedures	DLP-A399 Install a UBIC-H EIA, page 20-108
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Cisco recommends that you plan for future slot utilization and fully cable all SCSI connectors you will use later.

Step 1 Place a cable connector over the desired connection point on the backplane, making sure the cable runs toward the outside of the shelf.

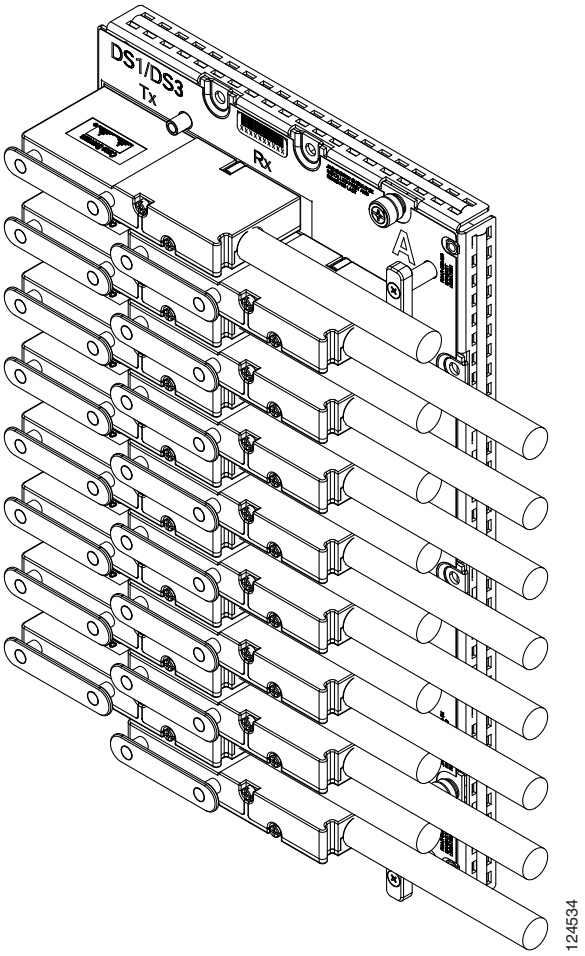
Step 2 Carefully push the connector into the backplane until the pin on the cable connector slides into the notch on the UBIC-H. Make sure the standoffs on the UBIC-H align properly with the notches on the cable.

Step 3 Use the flathead screwdriver to tighten the screws at the top and bottom of the end of cable connector two to three turns at 8 to 10 lbf-inch (9.2 to 11.5kgf-cm). Alternate between the two screws until both are tight.

Step 4 Repeat Steps 1 through 3 for each cable you want to install.

Figure 21-1 shows a UBIC-H with cables installed in all connectors.

Figure 21-1 Fully Cabled UBIC-H (A-Side)



Step 5 If available, tie wrap or lace the cables according to Telcordia standards (GR-1275-CORE) or local site practice.

Note When routing the electrical cables be sure to leave enough room in front of the alarm and timing panel so that it is accessible for maintenance activity.

Step 6 Return to your originating procedure (NTP).

DLP-A442 Verify Pass-Through Circuits

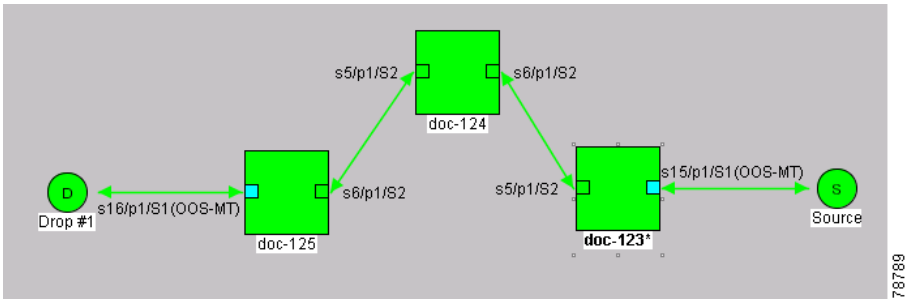
Purpose	This task verifies that circuits passing through a node enter and exit the node on the same STS and/or VT.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the CTC Circuits window, choose a circuit that passes through the node that will be removed and click **Edit**.

Step 2 In the Edit Circuits window, check **Show Detailed Map**.

Step 3 Verify that the STS and VT mapping on the node's east and west ports are the same. For example, if the circuit mapping on the west port is s5/p1/S1 (Slot 5, Port 1, STS 1), verify that the mapping is STS 1 on the east port. If the circuit displays different STSs and/or VTs on the east and west ports, record the name of the circuit. Figure 21-2 shows a circuit passing through a node (doc-124) on the same STS (STS 2).

Figure 21-2 Verifying Pass-Through STSs



Step 4 Repeat Steps 1 to 3 for each circuit in the Circuits tab.

Step 5 Delete and recreate each circuit recorded in Step 3. To delete the circuit, see the "DLP-A333 Delete Circuits" task on page 20-21. To create the circuit, see Chapter 6, "Create Circuits and VT Tunnels."

Step 6 Return to your originating procedure (NTP).

DLP-A443 Install the Fiber Clip on 15454_MRC-12 Cards

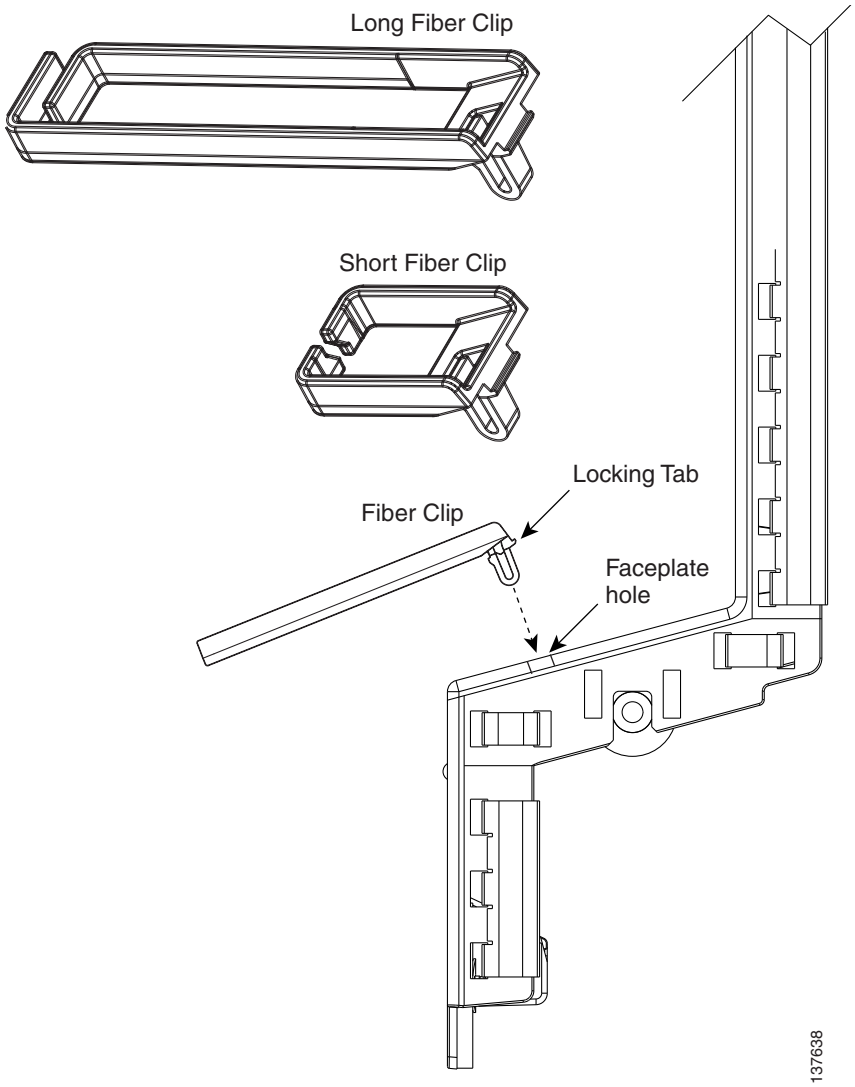
Purpose	This task installs a fiber clip, which allows proper routing of the fiber. Required for 15454_MRC-12 cards (known as the MRC-12 in CTC).
Tools/Equipment	Short or long fiber clip, as needed. Short clip: 52-0629-01 Long clip: 52-0628-01
Prerequisite Procedures	NTP-A16 Install Optical Cards and Connectors, page 2-8
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note You can install the fiber clip before or after the fibers are attached to the 15454_MRC-12 card.

Step 1 Determine the correct clip to use. Use the short clip with a standard cabinet door and a long clip with an extended door.

Step 2 Insert the prong of the fiber clip into the rectangular cutout on the sloped face of the faceplate (Figure 21-3).

Figure 21-3 Installing the Fiber Clip



Step 3 Push the clip into the hole until the locking tab snaps the clip securely into place. To remove a fiber clip, push on the locking tab to release the clip while rotating the clip forward and up.

Step 4 Return to your originating procedure (NTP).

DLP-A448 Convert DS3XM-6 or DS3XM-12 Cards From 1:1 to 1:N Protection

Purpose	This task converts DS3XM-6 or DS3XM-12 cards in 1:1 protection to 1:N protection. A 1:N protection group can protect a maximum of five working cards.
Tools/Equipment	DS3XM-12 card(s) Protection groups with either DS3XM-6 or DS3XM-12 cards
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This procedure assumes that either DS3XM-6 or DS3XM-12 cards are installed in Slots 1 to 6 and/or Slots 12 to 17. If there are DS3XM-6 cards in Slots 3 or 15, which are the protection slots, they will be replaced with a DS3XM-12 cards.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 Click the protection group containing Slot 3 or Slot 15. If the 1:1 protect card in Slot 3 or Slot 15 is a DS3XM-6 card, continue with Step 3. If the 1:1 protect card in Slot 3 or Slot 15 is a DS3XM-12 card, continue with Step 5.

Step 3 Make sure the slot that you are upgrading is not carrying working traffic. In the Selected Group list, the protect slot must say Protect/Standby, and not Protect/Active. If the protect slot status is Protect/Active, switch traffic to the working card:

a. Under Selected Group, click the protect card.

b. Next to Switch Commands, click **Switch**.

The working slot should change to Working/Active and the protect slot should change to Protect/Standby. If they fail to change, do not continue. Troubleshoot the working card and slot to determine why the card cannot carry working traffic.

Step 4 Repeat Steps 2 and 3 for each protection group that you need to convert.

Step 5 Click the **Alarms** tab to verify that no standing alarms exist for any of the DS3-12 cards you are converting. If alarms exist and you have difficulty clearing them, contact your next level of support.

Step 6 Click the **Provisioning > Protection** tabs.

Step 7 Click the 1:1 protection group that contains the cards that you will move into the new protection group.

Step 8 Click **Delete**.

Step 9 When the confirmation dialog box appears, click **Yes**.

Note Deleting 1:1 protection groups will not disrupt service. However, no protection bandwidth exists for the working circuits until the 1:N protection procedure is completed. Therefore, complete this procedure as soon as possible.

Step 10 If you are deleting more than one DS-3 1:1 protection group, repeat Steps 7 through 9 for each group that you want to include in a 1:N group.

Step 11 If the 1:1 protect card in Slot 3 or Slot 15 is a DS3XM-6 card, physically remove the protect DS3XM-6 card from Slot 3 or Slot 15. This raises an improper removal (IMPROPRMVL) alarm. If the 1:1 protect card in Slot 3 or Slot 15 is a DS3XM-12 card, continue with Step 16.

Step 12 In node view, right-click the slot that held the removed card and choose **Delete** from the shortcut menu. Wait for the card to disappear from the node view.

Step 13 Physically insert a DS3XM-12 card into the same slot.

Step 14 Verify that the card boots up properly.

Step 15 Click the **Inventory** tab and verify that the new card appears as a DS3XM-12 card.

Step 16 Click the **Provisioning > Protection** tabs.

Step 17 Click **Create**.

Step 18 Type a name for the protection group in the Name field (optional).

Step 19 Click **Type** and choose **1:N (card)** from the drop-down list.

Step 20 Verify that the DS3XM-12 card appears in the Protect Card field.

Step 21 In the Available Cards list, highlight the cards that you want in the protection group. Click the arrow (**>>**) tab to move the cards to the Working Cards list.

Step 22 Click **OK**.

The protection group should appear in the Protection Groups list on the Protection subtab.

Step 23 Return to your originating procedure (NTP).

DLP-A449 Set Up SNMP for a GNE

Purpose	This procedure provisions simple network management protocol (SNMP) parameters so that you can use SNMP network management software with the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP** tabs.

Step 2 In the Trap Destinations area, click **Create**.

Step 3 In the Create SNMP Trap Destination dialog box, complete the following fields:

- Destination IP Address—Enter the IP address of your network management system (NMS).
- Community—Enter the SNMP community name. (For more information refer to the “SNMP” chapter in the *Cisco ONS 15454 Reference Manual*.)

Note The community name is a form of authentication and access control. The community name assigned to the ONS 15454 is case-sensitive and must match the community name of the NMS.

- UDP Port—The default User Datagram Protocol (UDP) port for SNMP traps is 162.
- Trap Version—Choose either SNMPv1 or SNMPv2. Refer to your NMS documentation to determine whether to use SNMPv1 or SNMPv2.

Step 4 Click **OK**. The node IP address of the node where you provisioned the new trap destination appears in the Trap Destinations area.

Step 5 Click the node IP address in the Trap Destinations area. Verify the SNMP information that appears in the Selected Destination list.

Step 6 If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If the box is not checked, SET requests are rejected.

Step 7 If you want to set up the SNMP proxy feature to allow network management, message reporting, and performance statistic retrieval across ONS firewalls, click the **Enable SNMP Proxy** check box on the SNMP tab.

Step 8 If you want to use a generic SNMP MIB, check the **Use Generic MIB** check box.

Note In ONS 15454 Software R9.0 and later, you can configure IPv6 addresses for SNMPv1/v2 on a GNE, in addition to IPv4 addresses.

For more information about the SNMP proxy feature, refer to the "SNMP" chapter of the *Cisco ONS 15454 Reference Manual*.

Step 9 Click **Apply**.

Step 10 Return to your originating procedure (NTP).

DLP-A450 Set Up SNMP for an ENE

Purpose	This procedure provisions the SNMP parameters for an ONS 15454 configured to be an ENE if you use SNMP proxy on the GNE.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP** tabs.

Step 2 In the Trap Destinations area, click **Create**.

Step 3 On the Create SNMP Trap Destination dialog box, complete the following fields:

- Destination IP Address—Enter the IP address of your NMS.

- Community—Enter the SNMP community name. (For more information, refer to the "SNMP" chapter in the *Cisco ONS 15454 Reference Manual*.)

Note The community name is a form of authentication and access control. The community name assigned to the ONS 15454 is case-sensitive and must match the community name of the NMS.

- UDP Port—The default UDP port for SNMP traps is 162.
- Trap Version—Choose either SNMPv1 or SNMPv2. Refer to your NMS documentation to determine whether to use SNMPv1 or SNMPv2.

Step 4 Click **OK**. The node IP address of the node where you provisioned the new trap destination appears in the Trap Destinations area.

Step 5 Click the node IP address in the Trap Destinations area. Verify the SNMP information that appears in the Selected Destination list.

Step 6 If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If the box is not checked, SET requests are rejected.

Step 7 If you want to set up the SNMP proxy feature to allow network management, message reporting, and performance statistic retrieval across ONS firewalls, click the **Enable SNMP Proxy** check box on the SNMP tab.

Step 8 If you want to use a generic SNMP MIB, check the **Use Generic MIB** check box.

Note The ONS firewall proxy feature only operates on nodes running releases 4.6 and later. Using this information effectively breaches the ONS firewall to exchange management information.

For more information about the SNMP proxy feature, refer to the "SNMP" chapter of the *Cisco ONS 15454 Reference Manual*.

Step 9 Click **Apply**.

Step 10 If you are setting up SNMP proxies, you can set up to three relays for each trap address to convey SNMP traps from the NE to the NMS. To do this, complete the following substeps:

a. Click the first trap destination IP address. The address and its community name appear in the Destination fields.

b. If the node you are logged into is an ENE, set the Relay A address to the GNE and type its community name in the community field. If there are NEs between the GNE and ENE, you can enter up to two SNMP proxy relay addresses and community names in the fields for Relay B and Relay C. When doing this, consult the following guidelines:

- If the NE is directly connected to the GNE, enter the address and community name of the GNE for Relay A.
- If this NE is connected to the GNE through other NEs, enter the address and community name of the GNE for Relay A and the address and community name of NE 1 for Relay B and NE 2 for Relay C.

The SNMP proxy directs SNMP traps in the following general order:
ENE > RELAY C > RELAY B > RELAY A > NMS. The following parameters also apply:

- If there is 1 intermediate relay, the order is ENE > RELAY B (NE1) > RELAY A(GNE) > NMS
- If there is are 2 intermediate relays, the order is ENE > RELAY C (NE2) > RELAY B (NE 1) > RELAY A (GNE) > NMS.

Step 11 Click **Apply**.

Step 12 Repeat Step 2 through Step 11 for all NEs between the GNE and ENE.

Step 13 Return to your originating procedure (NTP).

Note In ONS 15454 Software R9.0 and later, you can configure IPv6 addresses for SNMPv1/v2 on an ENE if you use SNMP proxy on the GNE, in addition to IPv4 addresses.

DLP-A451 Format and Enter NMS Community String for SNMP Command or Operation

Purpose	This procedure describes how to format a network management system (NMS) community string to execute the following SNMP commands for GNEs and ENEs: Get, GetBulk, GetNext, and Set.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 If the SNMP "Get" (or other operation) is enabled on the ONS 15454 configured as a GNE, enter the community name assigned to the GNE in community name field on the MIB browser.

Note The community name is a form of authentication and access control. The community name of the NMS must match the community name assigned to the ONS 15454.

Step 2 If the SNMP "Get" (or other operation) is enabled for the ENE through a SOCKS proxy-enabled GNE, create a formatted string to enter in the MIB browser community name field. Refer to the following examples when constructing this string for your browser:

- Formatted community string input example 1:

  ```
  allviews{192.168.7.4,,,net7node4}
  ```

  If "allviews" is a valid community name value at the proxy-enabled SNMP agent (the GNE), the GNE is expected to forward the PDU to 192.168.7.4 at Port 161. The outgoing PDU will have "net7node4" as the community name. This is the valid community name for the ENE with address 192.168.7.4.

- Formatted community string input example 2:

  ```
  allviews{192.168.7.99,,,enter7{192.168.9.6,161,,net9node6}}
  ```

  If "allviews" is a valid community name value at the proxy-enabled GNE, the GNE is expected to forward the PDU to 192.168.7.99 at the default port (Port 161) with a community name of "enter7{192.168.9.6,161,,net9node6}". The system with the address 192.168.7.99 (the NE between

the GNE and ENE) forwards this PDU to 192.168.9.6 at Port 161 (at the ENE) with a community name of “net9node6”. The community name “enter7” is valid for the NE between the GNE and the ENE and “net9node6” is a valid community name for the ENE.

Step 3 Log into the NMS where the browser is installed to retrieve the network information from the ONS 15454.

Step 4 On the same computer, go to Start and click the SNMP MIB browser application.

Step 5 In the Host and Community areas, enter the IP address of the GNE through which the ONS 15454 with the information to be retrieved can be reached.

Step 6 In the Community area, enter the community string as explained in Step 2.

Step 7 Return to your originating procedure (NTP).

DLP-A452 Create a VLAN

Purpose	This task creates a new VLAN.
Tools/Equipment	None
Prerequisite Procedures	See Chapter 6, “Create Circuits and VT Tunnels” for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 From the Tools menu, choose **Manage VLANS**.

Step 3 In the All VLANs dialog box, click **Create**.

Step 4 In the Define New VLAN dialog box, complete the following:

- VLAN Name—Assign an easily identifiable name to your VLAN.
- VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.
- Topology Host—Choose the node to serve as the topology host from the drop-down list. The topology host is used to discover the VLAN topology. The login node is the default.

Step 5 Click **OK**.

Step 6 Click **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-A453 Delete a Server Trail

Purpose	This task deletes a server trail.
Tools/Equipment	None
Prerequisite Procedures	NTP-A326 Create a Server Trail, page 6-93 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Deleting server trails do not impact the circuits provisioned over it as server trail is a logical link. Deleting a server trail is recommended when migrating from IPv4 to IPv6 because the server trails created on a IPv4 network will not work in an IPv6 network. You can recreate server trails after migrating to IPv6 network without deleting the circuits. When you delete a server trail, the circuit state becomes PARTIAL.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > Server Trails** tabs.

Step 3 Click the server trail that you want to delete.

Step 4 Click **Delete**.

Step 5 In the confirmation dialog box, click **Yes**.

Note You can use the server trail audit log to recreate a server trail that you may have accidentally deleted. The server trail audit log includes the following parameters:

- Server trail ID
- Peer IP address
- Circuit size
- Protection type
- Number of trails
- Starting STS/VT
- SRLG value

You can look at the audit log of the source or destination node and find the entry for the delete call. This log entry has the STS/VT path definitions on the node, peer IP address, and server trail ID. You can then look at the audit log of the peer IP address, locate the delete call for the specific server trail ID, and find the STS/VT path definitions on the node. This would provide you with the required information to recreate the server trail.

Note It is recommended that you delete one server trail at a time as the deletion of multiple trails together may cause CTC to hang and is a time consuming task.

Step 6 Return to your originating procedure (NTP).

DLP-A454 View the BLSR STS Squelch Table

Purpose	This task allows you to view the BLSR STS squelch table for an ONS 15454 BLSR node. For example, if a fiber cut occurs, the BLSR STS squelch tables show STSs that will be squelched for every isolated node. Squelching replaces traffic by inserting the appropriate alarm indication signal path (AIS-P); it prevents traffic misconnections. For an STS with a VT-access check mark, the AIS-P will be removed after 100 ms. For more information about BLSR squelching, refer to Telcordia GR-1230.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 To open the squelch table in node view:

a. In node view, click the **Provisioning > BLSR** tabs.

b. Click the BLSR whose squelch table you want to view.

c. Click **Squelch Table**.

Step 2 To open the squelch table in network view:

a. In network view, click the **Provisioning > BLSR** tabs.

b. Click the BLSR whose squelch table you want to view.

c. Click **Edit**.

d. Right-click a node in the **Edit** window.

e. Click **Squelch Table** from the drop-down list.

Step 3 In the BLSR Squelch Table window you can view the following information:

- STS Number—Shows the BLSR STS numbers. For two-fiber BLSRs, the number of STSs is half the BLSR OC-N, for example, an OC-48 BLSR squelch table will show 24 STSs. For four-fiber BLSRs, the number of STSs in the table is the same as the BLSR OC-N.
- West Source—If traffic is received by the node on its west span, the BLSR node ID of the source appears. (To view the BLSR node IDs for all nodes in the ring, click the **Ring Map** button.)
- West VT (from the West Source)—A check mark indicates that the STS carries incoming VT traffic. The traffic source is coming from the west side.
- West VT (from the West Destination)—A check mark indicates that the STS carries outgoing VT traffic. The traffic is dropped on the west side.
- West Dest—If traffic is sent on the node's west span, the BLSR node ID of the destination appears.
- East Source—If traffic is received by the node on its east span, the BLSR node ID of the source appears.

- East VT (from the East Source)—A check mark indicates that the STS carries incoming VT traffic. The traffic source is coming from the east side.
- East VT (from the East Destination)—A check mark indicates that the STS carries outgoing VT traffic. The traffic is dropped on the east side.
- East Dest—If traffic is sent on the node's east span, the BLSR node ID of the destination appears.

Note BLSR squelching is performed on STSs that carry STS circuits only. Squelch table entries will not appear for STSs carrying VT circuits or Ethernet circuits to or from E-Series Ethernet cards provisioned in a multicard Ethergroup.

Step 4 Return to your originating procedure (NTP).

DLP-A455 View the BLSR VT Squelch Table

Purpose	BLSR VT squelch tables only appear on the node dropping VTs from a BLSR and are used to perform VT-level squelching when a node is isolated. VT squelching is supported on the ONS 15454 and the ONS 15327 platforms. The ONS 15600 platform does not support VT squelching; however, when an ONS 15454 and an ONS 15600 are in the same network, the ONS 15600 node allows the ONS 15454 node to carry VT circuits in a VT tunnel. The ONS 15600 performs 100-ms STS-level squelching for each VT-access STS at the switching node in case of a node failure. For more information about BLSR squelching, refer to Telcordia GR-1230.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 To open the squelch table in node view:

a. In node view, click the **Provisioning > BLSR** tabs.

b. Click the BLSR whose squelch table you want to view.

c. Click **Squelch Table**.

Step 2 To open the squelch table in network view:

a. In network view, click the **Provisioning > BLSR** tabs.

b. Click the BLSR whose squelch table you want to view.

c. Click **Edit**.

d. Right-click a node in the **Edit** window.

e. Choose **Squelch Table** from the drop-down list.

Step 3 In the BLSR STS Squelch Table window, double-click the VT check mark. In the BLSR VT Squelch Table window you can view the following information:

Note The check mark appears on every VT-access STS; however, the VT squelch table appears only by double-clicking the check mark on the node dropping the VT. The intermediate node of the VT does not maintain the VT-squelch table.

- VT Number—Shows the BLSR VT numbers. The VT number includes VT group and channel (VT group 2 and channel 1 are displayed as 2-1.)
- West Source—If traffic is received by the node on its west span, the BLSR node ID of the source appears. (To view the BLSR node IDs for all nodes in the ring, click the **Ring Map** button.)
- East Source—If traffic is received by the node on its east span, the BLSR node ID of the source appears.

Step 4 Return to your originating procedure (NTP).

DLP-A456 Configure the Node for RADIUS Authentication

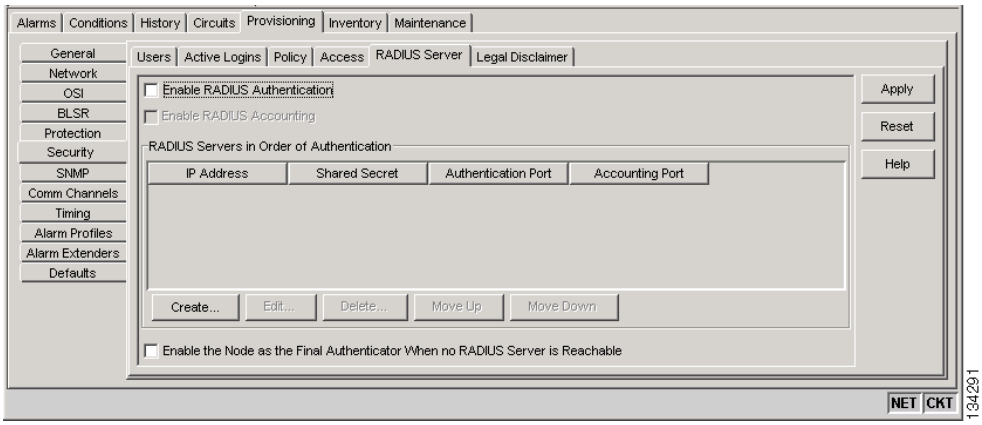
Purpose	This task allows you to configure a node for Remote Authentication Dial In User Service (RADIUS) authentication. RADIUS validates remote users who are attempting to connect to the network.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60 Before configuring the node for RADIUS authentication, you must first add the node as a network device on the RADIUS server. Refer to the *User Guide for Cisco Secure ACS for Windows Server* for more information about configuring a RADIUS server.
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution Do not configure a node for RADIUS authentication until after you have added that node to the RADIUS server and added the RADIUS server to the list of authenticators. If you do not add the node to a RADIUS server prior to activating RADIUS authentication, no user will be able to access the node. Refer to the *User Guide for Cisco Secure ACS for Windows Server* for more information about adding a node to a RADIUS server.

Note The following Cisco vendor-specific attribute (VSA) needs to be specified when adding users to the RADIUS server:
shell:priv-lvl=N, where N is:
0 for Retrieve User
1 for Maintenance User
2 for Provisioning User
3 for Super User
4 for Security User
5 for Security Super User
6 for Root User

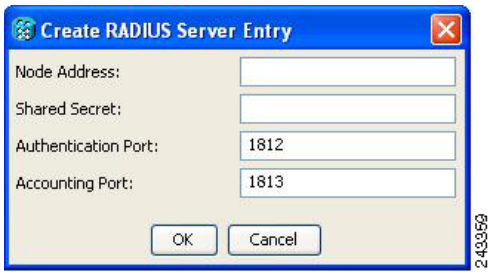
Step 1 In node view, click the **Provisioning > Security > RADIUS Server** tabs (Figure 21-4).

Figure 21-4 RADIUS Server Tab



Step 2 Click **Create** to add a RADIUS server to the list of authenticators. The Create RADIUS Server Entry window appears (Figure 21-5).

Figure 21-5 Create RADIUS Server Entry Window



Step 3 Enter the RADIUS server IP address in the Node Address field. If the node is an end network element (ENE), enter the IP address of the gateway network element (GNE) in this field.

The GNE passes authentication requests from the ENEs in its network to the RADIUS server, which grants authentication if the GNE is listed as a client on the server.

The RADIUS port numbers used for the ENE RADIUS configuration map to the RADIUS configuration entries in the GNE. For example, the first RADIUS authentication port number configured in ENE (1860) maps to the first RADIUS authentication entry in the GNE. The port number 1863 maps to the fourth entry in the GNE and so on.

The above logic applies to the configuration of the RADIUS accounting ports starting with port number 1870 for the first entry.

Note In ONS 15454 Software Release 9.0 and later, you can configure IPv6 addresses for RADIUS servers, in addition to IPv4 addresses.

Caution Because the ENE nodes use the GNE to pass authentication requests to the RADIUS server, you must add the ENEs to the RADIUS server individually for authentication. If you do not add the ENE node to a RADIUS server prior to activating RADIUS authentication, no user will be able to access the node. Refer to the *User Guide for Cisco Secure ACS for Windows Server* for more information about adding a node to a RADIUS server.

Step 4 Enter the shared secret in the Shared Secret field. A shared secret is a text string that serves as a password between a RADIUS client and RADIUS server.

Step 5 Enter the RADIUS authentication port number in the Authentication Port field. The default port is 1812. If the node is an ENE, set the authentication port to a number within the range of 1860 to 1869.

Step 6 Enter the RADIUS accounting port in the Accounting Port field. The default port is 1813. If the node is an ENE, set the accounting port to a number within the range of 1870 to 1879.

Step 7 Click **OK**. The RADIUS server is added to the list of RADIUS authenticators.

Note You can add up to 10 RADIUS servers to a node's list of authenticators.

Step 8 Click **Edit** to make changes to an existing RADIUS server. You can change the IP address, the shared secret, the authentication port, and the accounting port.

Step 9 Click **Delete** to delete the selected RADIUS server.

Step 10 Click **Move Up** or **Move Down** to reorder the list of RADIUS authenticators. The node requests authentication from the servers sequentially from top to bottom. If one server is unreachable, the node will request authentication from the next RADIUS server on the list.

Step 11 Click the **Enable RADIUS Authentication** check box to activate remote-server authentication for the node.

Step 12 Click the **Enable RADIUS Accounting** check box if you want to show RADIUS authentication information in the audit trail.

Step 13 Click the **Enable the Node as the Final Authenticator** check box if you want the node to be the final autheticator. This means that if every RADIUS authenticator is unavailable, the node will authenticate the login rather than locking the user out.

Step 14 Click **Apply** to save all changes or **Reset** to clear all changes.

Step 15 Return to your originating procedure (NTP).

DLP-A457 Grant Superuser Privileges to a Provisioning User

Purpose	This task enables a provisioning user to perform tasks such as retrieve an audit log, restore a database, and activate and revert a software load.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning** > **Defaults** tabs.

Step 2 In the Defaults Selector area, choose NODE > security > grantPermission.

Step 3 Click in the Default Value column for the default property you are changing and choose **Provisioning** from the drop-down list.

Note If you click **Reset** before you click **Apply**, all values will return to their original settings.

Step 4 Click **Apply**.

A pencil icon will appear next to the default name that will be changed as a result of editing the defaults file.

Note You must close your current CTC session and restart a new CTC session for the changes to take effect.

Step 5 Return to your originating procedure (NTP).

DLP-A458 Clear All PM Thresholds

Purpose	This task clears and resets all PM thresholds to the default values.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution Pressing the Reset button can mask problems if used incorrectly. This button is commonly used for testing purposes.

Step 1 In node view, double-click the card where you want to view PM thresholds. The card view appears.

Step 2 Click the **Provisioning > Threshold** tab. The subtab names vary depending on the card selected.

Step 3 Click **Reset to Default**.

Step 4 Click **Yes** in the Reset to Default dialog box.

Step 5 Verify that the PM thresholds have been reset.

Step 6 Return to your originating procedure (NTP).

DLP-A459 Change Optics Thresholds Settings for OC-192, MRC-12, and MRC-2.5G-4 Cards

Purpose	This task changes the optics thresholds settings for OC-192, MRC-12, and MRC-2.5G-4 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual.*

Step 1 In node view, double-click the card where you want to change the optics settings.

Step 2 Click the **Provisioning > Optics Thresholds** tabs.

Note If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 3 Modify any of the settings described in Table 21-6 by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value or select or deselect a check box.

Step 4 Click **Apply**.

Table 21-6 Optics Thresholds Settings

Parameter	Description	Options
Port	(Display only) Port number.	• 1 (OC-192, OC192-XFP) • 1-12 (MRC_12) • 1-4 (MRC-2.5G-4)
LBC-LOW	Laser bias current–minimum.	Default (15 min/1 day): 50 percent

Table 21-6 Optics Thresholds Settings (continued)

Parameter	Description	Options
LBC-HIGH	Laser bias current–maximum.	Default (15 min/1 day): 150 percent
OPT-LOW	Optical power transmitted–minimum.	Default (15 min/1 day): 80 percent
OPT-HIGH	Optical power transmitted–maximum.	Default (15 min/1 day): 120 percent
OPR-LOW	Optical power received–minimum.	Default (15 min/1 day): 50 percent
OPR-HIGH	Optical power received–maximum.	Default (15 min/1 day): 200 percent
Set OPR	Setting the optical power received establishes the received power level as 100 percent. If the receiver power decreases, then the OPR percentage decreases to reflect the loss in receiver power. For example, if the receiver power decreases by 3 dBm, the OPR decreases 50 percent.	Click **SET**.
Types	Sets the threshold values of alerts that trigger an alarm or TCA response. To view the provisionable thresholds that generate an Alarm or TCA, choose the type and click **Refresh**.	• TCA (threshold cross alert) • Alarm
Intervals	Sets the time interval for collecting parameter counts. To change the time interval, choose the desired interval and click **Refresh**.	• 15 Min • 1 Day

Step 5 Return to your originating procedure (NTP).

DLP-A460 Reset a Traffic Card Using CTC

Purpose	This task resets an optical, electrical, E-Series Ethernet, G-Series Ethernet, ML-Series Ethernet, or CE-1000-4 Ethernet card in CTC. The CE100T-8 Ethernet card has unique reset tasks; see the "DLP-A54 Hard-Reset a CE-100T-8 Card Using CTC" task on page 17-57 or the "DLP-A224 Soft-Reset a CE-100T-8 Card Using CTC" task on page 19-17 for more information.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note To reset transponder (TXP) or muxponder (MXP) cards, refer to the *Cisco ONS 15454 DWDM Procedure Guide*.

Caution If you soft reset a working electrical card that is part of a protection group, while the card is rebooting do not unlock that card or the protect card that protects the reset working electrical card. If you do so, a traffic loss will result. Wait until the working electrical card fully reboots before reversing a lock-out on protect on the protect card or reversing a lock-on on the working card. This applies to all electrical cards except the E1-42 card.

Step 1 In node view, position the cursor over the traffic card slot.

Step 2 Right-click the card and choose **Reset Card** from the shortcut menu.

Step 3 Click **Yes** in the Resetting Card dialog box.

Step 4 Return to your originating procedure (NTP).

DLP-A461 Preprovision an SFP or XFP Device

Purpose	This task preprovisions SFPs/XFPs on the MRC-12, MRC-2.5G-4, and OC192-XFP cards. Cisco-approved OC-3, OC-12, OC-48, OC-192 and multirate SFPs/XFPs are compatible with the ONS 15454. Refer to the *Cisco ONS 15454 Reference Manual* for a list of card and SFP/XFP compatibility. The SFPs/XFPs are referred to as pluggable port modules (PPMs) in CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Note Before you install SFPs on the MRC-12 or MRC-2.5G-4 card, refer to the MRC-12 or MRC-2.5G-4 section in the "Optical Cards" chapter of the *Cisco ONS 15454 Reference Manual* for bandwidth restrictions based on the port where you install the SFP and the cross-connect card being used.

Note If you preprovision a multirate SFP, you must next select the line rate using the "DLP-A574 Provision a PPM on the MRC-12 or MRC-2.5G-4 Card" task on page 22-88.

Step 1 In node view, click the **Alarms** tab:

- **a.** Verify that the alarm filter is not turned on. See the "DLP-A227 Disable Alarm Filtering" task on page 19-18 as necessary.
- **b.** Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.
- **c.** Complete the "DLP-A532 Export CTC Data" task on page 22-34 to export alarm and condition information.

Step 2 In node view, double-click the card where you want to provision PPM settings.

Step 3 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 4 In the Pluggable Port Modules pane, click **Create**. The Create PPM dialog box appears.

Step 5 In the Create PPM dialog box, complete the following:

- PPM—Choose the slot number where you want to preprovision the SFP/XFP from the drop-down list.
- PPM Type—Choose the number of ports supported by your SFP/XFP from the drop-down list. If only one port is supported, **PPM (1 port)** is the only option.

Step 6 Click **OK**. The newly created port appears on the Pluggable Port Modules pane. The row on the Pluggable Port Modules pane turns light blue and the Actual Equipment Type column lists the preprovisioned PPM as unknown until the actual SFP/XFP is installed. After the SFP/XFP is installed, the row on the pane turns white and the column lists the equipment name.

Step 7 Verify that the PPM appears in the list on the Pluggable Port Modules pane. If it does not, repeat Steps 4 through 6.

Step 8 On the Provisioning tab, click the **Line** subtab. If applicable for the PPM you are preprovisioning, use the **Reach** and **Wavelength** columns to configure these parameters as needed.

Note Only the parameters that are editable for the PPMs on a particular platform type are provisionable. For example, some platforms may not have PPMs with configurable wavelengths or reaches. In that case, wavelength md reach ares not provisionable.

Step 9 Repeat the task to create a second PPM.

Step 10 Click **OK**.

Step 11 When you are ready to install the SFP/XFP, complete the "DLP-A469 Install a GBIC or SFP/XFP Device" task on page 21-60.

Step 12 Return to your originating procedure (NTP).

DLP-A462 View and Terminate Active Logins

Purpose	This task allows you to view active CTC logins, retrieve the last activity time, and terminate all current logins.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher for viewing; Superuser for session termination

Step 1 In node view, click the **Provisioning > Security > Active Logins** tab. The Active Logins tab displays the following information:

- User ID
- User IP address
- Current node the user is logged into

- Session Type (EMS, TL1, FTP, telnet, or SSH)
- Login time
- Last activity time

Step 2 Click **Logout** to end the session of every logged-in user. This will log out all current users, excluding the initiating Superuser.

Step 3 Click **Retrieve Last Activity Time** to display the most recent activity date and time for users in the Last Activity Time field.

Step 4 Return to your originating procedure (NTP).

DLP-A463 Roll the Source or Destination of One Optical Circuit

Purpose	This task reroutes traffic from one source or destination to another on the same circuit, thus changing the original source or destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Circuits** tab.

Step 3 Click the circuit that you want to roll. The circuit must have a DISCOVERED status for you to begin a roll.

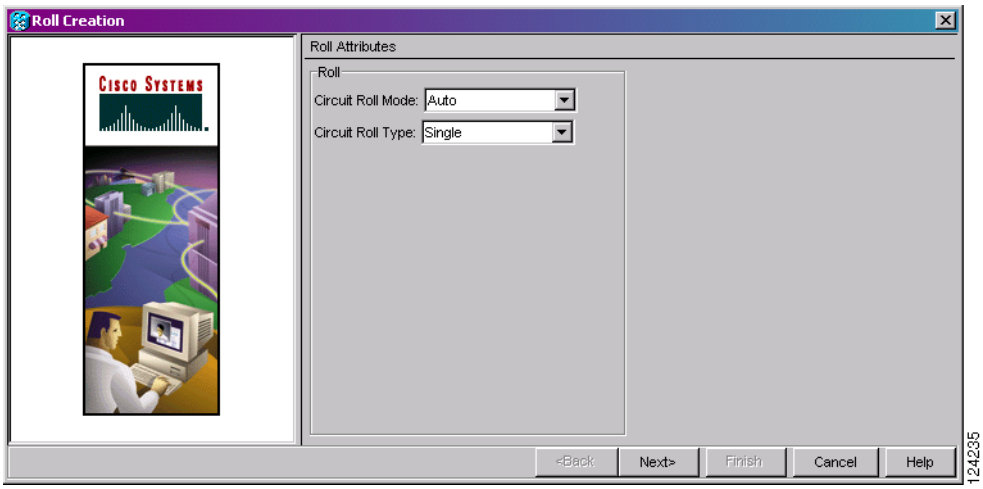
Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

Step 5 In the Roll Attributes area, complete the following (Figure 21-6):

a. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll (required for a 1-way source roll) or **Manual** to create a manual roll (required for a 1-way destination roll).

b. From the Circuit Roll Type drop-down list, choose **Single** to indicate that you want to roll one cross-connect on the chosen circuit.

Figure 21-6 Selecting Single Roll Attributes

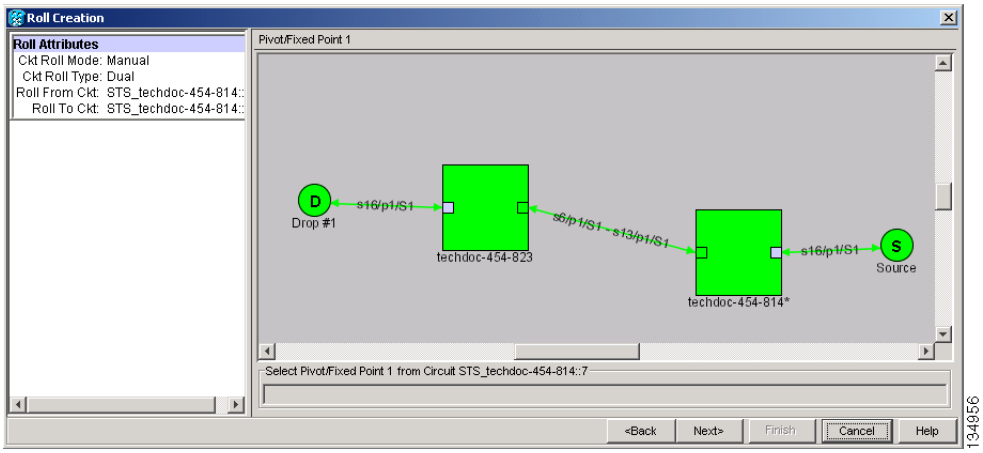


Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square in the graphic image that represents the facility that you want to keep (Figure 21-7).

This facility is the fixed location in the cross-connect involved in the roll process. The identifier appears in the text box below the graphic image. The facility that is not selected is the Roll From path. The Roll From path is deleted after the roll is completed.

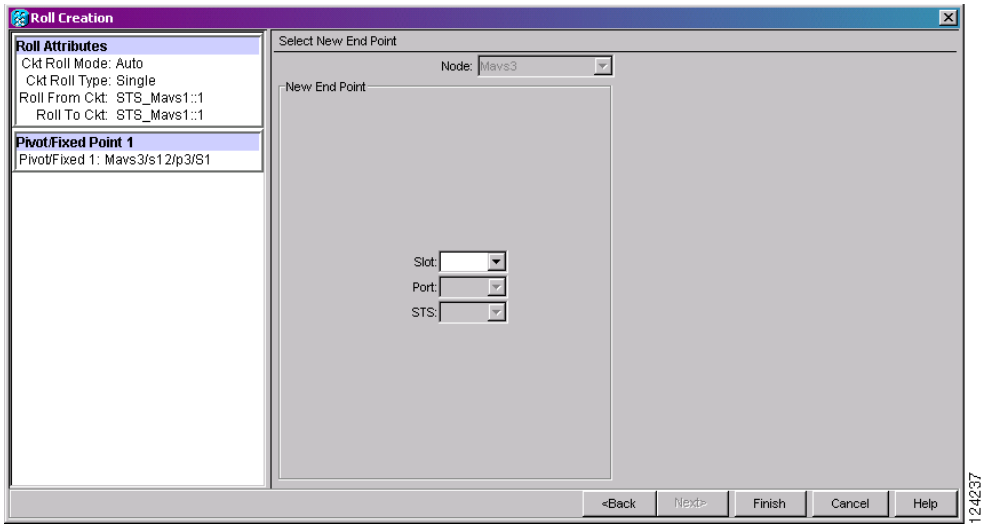
Figure 21-7 Selecting a Path



Step 8 Click **Next**.

Step 9 In the Select New End Point area, choose the **Slot**, **Port**, and **STS** from the drop-down lists to select the Roll To facility (Figure 21-8).

Figure 21-8 Selecting a New Endpoint



Step 10 Click **Finish**. On the Circuits tab, the circuit status for the Roll From port changes from DISCOVERED to ROLL_PENDING.

Step 11 Click the **Rolls** tab (Figure 21-9). For the pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with Step 12.

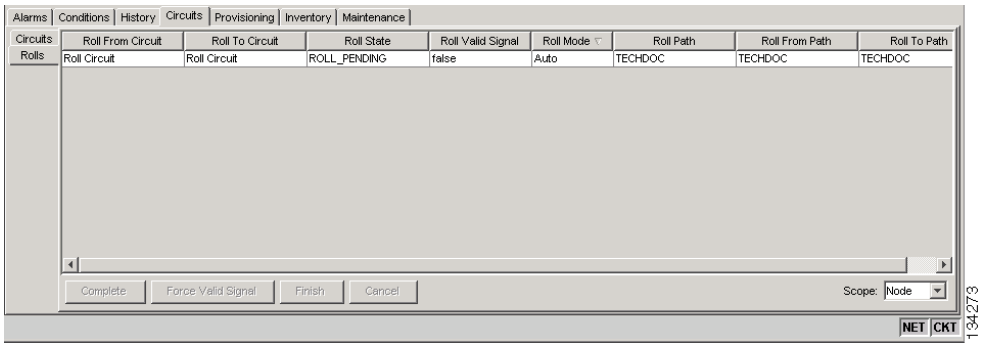
- If the Roll Valid Signal status is true, a valid signal was found on the new port. On either the Automatic or the Manual roll, the physical change of the cross-connect to the Roll To path occurs after running the roll command.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If the signal is not found, refer to the Circuits and Timing section of the *Cisco ONS 15454 Troubleshooting Guide*. To cancel the roll, see the "DLP-A489 Cancel a Roll" task on page 21-63.
- The roll is a one-way destination roll and the Roll Valid Signal is false. It is not possible to get a Roll Valid Signal status of true for a one-way destination roll.

Note You cannot cancel an automatic roll after a valid signal is found.

- You can force a signal onto the Roll To circuit by using the Force Valid Signal button. If you choose Force Valid Signal, traffic on the circuit that is involved in the roll might drop depending on conditions at the other end of the circuit when the roll is completed. You must force a signal if the circuits do not have a signal or have a bad signal and you want to complete the roll.

Note For a one-way destination roll in manual mode, you do not need to force the valid signal.

Figure 21-9 Viewing the Rolls Tab



Step 12 If you selected Manual in Step 5, click the rolled facility on the Rolls tab and then click **Complete**. If you selected Auto, continue with Step 13.

Step 13 For both Manual and Auto rolls, click **Finish** to complete the circuit roll process. The roll clears from the Rolls tab and the rolled circuit now appears on the Circuits tab in the DISCOVERED status.

Step 14 Return to your originating procedure (NTP).

DLP-A464 Roll One Cross-Connect from an Optical Circuit to a Second Optical Circuit

Purpose	This task reroutes a cross-connect on one circuit onto another circuit, resulting in a new destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 DLP-A156 Delete a Section DCC Termination, page 18-24 for the ports involved in the roll
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Circuits** tab.

Step 3 Press **Ctrl** and click the two circuits that you want to use in the roll process.

The circuits must have a DISCOVERED status; in addition, they must be the same size and direction for you to begin a roll. The planned Roll To circuit must not carry traffic. The Roll To facility should be DCC connected to the source node of the Roll To circuit.

Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

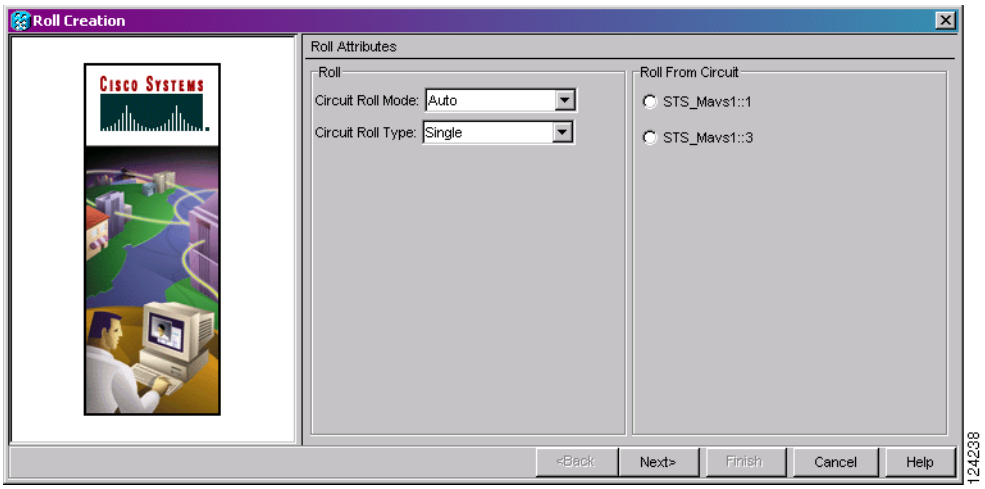
Step 5 In the Roll Attributes area, complete the following (Figure 21-10):

a. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll (required for a 1-way source roll) or **Manual** to create a manual roll (required for 1-way destination roll).

b. From the Circuit Roll Type drop-down list, choose **Single** to indicate that you want to roll a single connection from the Roll From circuit to the Roll To circuit.

c. In the Roll From Circuit area, click the circuit that contains the Roll From connection.

Figure 21-10 Selecting Roll Attributes for a Single Roll onto a Second Circuit



Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square representing the facility that you want to keep (Figure 21-7 on page 21-47).

This facility is the fixed location in the cross-connect involved in the roll process. The identifier appears in the text box below the graphic image. The facility that is not selected is the Roll From path. The Roll From path is deleted after the roll is completed.

Step 8 Click **Next**.

Step 9 In the Select New End Point area, choose the **Slot**, **Port**, and **STS** from the drop-down lists to identify the Roll To facility on the connection being rolled.

Step 10 Click **Finish.**

The statuses of the Roll From and Roll To circuits change from DISCOVERED to ROLL_PENDING in the Circuits tab.

Step 11 Click the **Rolls** tab. For the pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with Step 12.

- If the Roll Valid Signal status is true, a valid signal was found on the new port. On either the Automatic or the Manual roll, the physical change of the cross-connect to the Roll To path occurs after running the roll command.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If the signal is not found, refer to the Circuits and Timing section of the *Cisco ONS 15454 Troubleshooting Guide*. To cancel the roll, see the "DLP-A489 Cancel a Roll" task on page 21-63.
- The roll is a one-way destination roll and the Roll Valid Signal is false. It is not possible to get a "true" Roll Valid Signal status for a one-way destination roll.

Note You cannot cancel an automatic roll after a valid signal is found.

- A roll can be forced onto the Roll To Circuit destination without a valid signal by using the Force Valid Signal button. If you choose Force Valid Signal, traffic on the circuit that is involved in the roll will be dropped when the roll is completed.

Step 12 If you selected Manual in Step 5, click the roll on the Rolls tab and click **Complete** to lock the change of the route to the ROLLTO into the database. If you selected Auto, continue with Step 13.

Step 13 For both manual and automatic rolls, click **Finish** to complete the circuit roll process.

The roll is cleared from the Rolls tab and the new rolled circuit on Circuits tab returns to the DISCOVERED status.

Step 14 Return to your originating procedure (NTP).

DLP-A465 Roll Two Cross-Connects on One Optical Circuit Using Automatic Routing

Purpose	This task reroutes the network path while maintaining the same source and destination. This task allows CTC to automatically select a Roll To path.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This task optionally uses automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Circuits tab**.

Step 3 Click the circuit that has the connections that you want to roll. The circuit must have a DISCOVERED status for you to begin a roll.

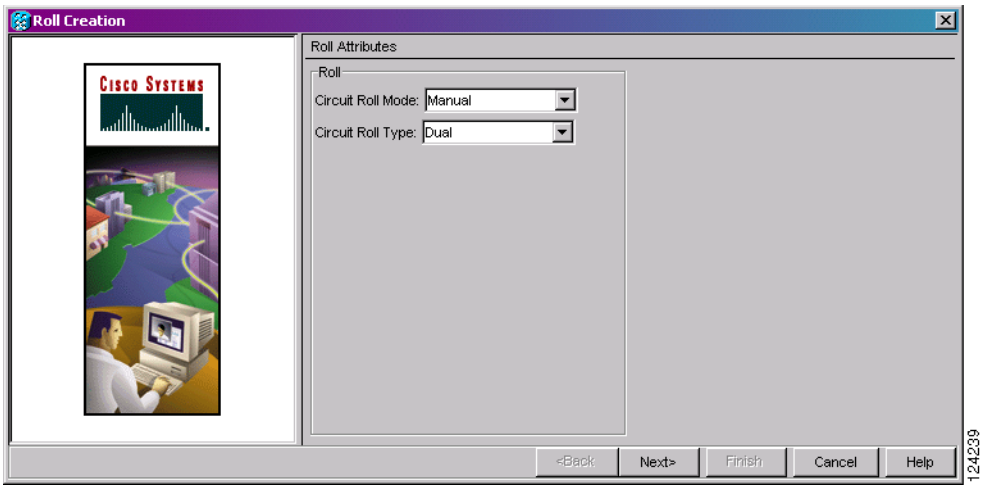
Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

Step 5 In the Roll Attributes area, complete the following (Figure 21-11):

a. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll or **Manual** to create a manual roll.

b. From the Circuit Type drop-down list, choose **Dual** to indicate that you want to roll two connections on the chosen circuit.

Figure 21-11 Selecting Dual Roll Attributes



Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square representing the fixed path of the first connection to be rolled (Figure 21-7 on page 21-47).

This path is a fixed point in the cross connection involved in the roll process. The path identifier appears in the text box below the graphic image. The path that is not selected contains the Roll From path. The Roll From path is deleted after the roll is completed.

Step 8 Click **Next**.

Step 9 Complete one of the following:

- If multiple Roll From paths exist, the Select Roll From dialog box appears. Select the path from which you want to roll traffic and click **OK**.
- If multiple Roll From paths do not exist, continue with Step 10. The circuit status for the Roll To path changes states from DISCOVERED to ROLL_PENDING.

Step 10 In the Pivot/Fixed Point 2 window, click the square that represents the fixed path of the second connection to be rolled.

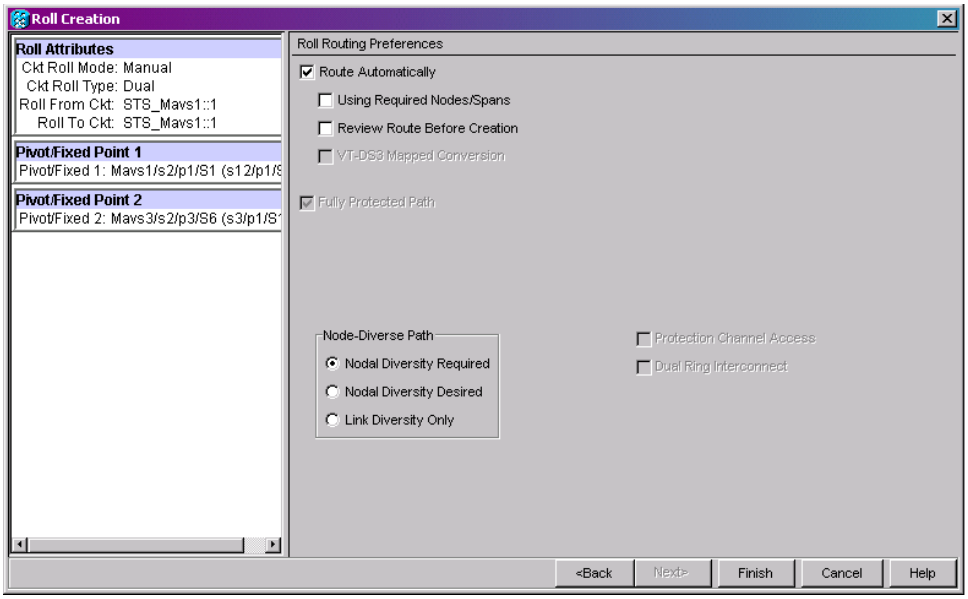
The path that is not selected is the Roll From path. The Roll From path is deleted after the roll is completed. The path identifier appears in the text box below the graphic image.

Step 11 Click **Next**.

Step 12 In the Circuit Routing Preferences area, check **Route Automatically** to allow CTC to find the route (Figure 21-12). If you check Route Automatically, the following options are available:

- Using Required Nodes/Spans—If checked, you can specify nodes and spans to include or exclude in the CTC-generated circuit route in Step 15.
- Review Route Before Creation—If checked, you can review and edit the circuit route before the circuit is created.

Figure 21-12 Setting Roll Routing Preferences



Step 13 To route the circuit over a protected path, check **Fully Protected Path**. (If you do not want to route the circuit on a protected path, continue with Step 14.) CTC creates a primary and alternate circuit route (virtual path protection) based on the following nodal diversity options. Select one of the following choices and follow subsequent window prompts to complete the routing:

- Nodal Diversity Required—Ensures that the primary and alternate paths within path-protected mesh network (PPMN) portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity should be attempted, but if node diversity is not possible, CTC creates link diverse paths for the PPMN portion of the complete circuit path.
- Link Diversity Only—Specifies that only link-diverse primary and alternate paths for PPMN portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you checked Route Automatically in Step 12:

- If you checked Using Required Nodes/Spans, continue with Step 15.
- If you checked only Review Route Before Creation, continue with Step 16.
- If you did not check Using Required Nodes/Spans or Review Route Before Creation, continue with Step 17.

Step 15 If you checked Using Required Nodes/Spans in Step 12:

a. In the Roll Route Constraints area, click a node or span on the circuit map.

b. Click **Include** to include the node or span in the circuit. Click **Exclude** to exclude the node/span from the circuit. The order in which you select included nodes and spans sets the circuit sequence. Click spans twice to change the circuit direction.

c. Repeat Step b for each node or span you wish to include or exclude.

d. Review the circuit route. To change the circuit routing order, select a node in the Required Nodes/Lines or Excluded Nodes Links lists, then click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 16 If you checked Review Route Before Creation in Step 12:

a. In the Roll Route Review and Edit area, review the circuit route. To add or delete a circuit span, select a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

b. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information.

Caution The following is only seen with DUAL roll mode when both ends of the circuit use the card(s) mentioned in this statement. If the termination card is a DS1/E1-56, DS1-14, DS1-N-14, DS3XM-6, or DS3XM-12 card, a roll will occur even if a valid signal is not detected on the Roll To port. The absence of path payload defect indication (PDI-P) downstream for loss of signal (LOS), loss of frame alignment (LOF), and AIS line defects causes the roll to continue without a valid signal. On the DS1/E1-56, DS1-14, and DS1-N-14 cards, it is possible to check the Send AIS-V For Ds1 AIS check box to properly generate PDI-P downstream for the LOS and LOF AIS line defects. This check box is selected from the card view Provisioning > Line tab. On the DS1-14 and DS1-N-14 cards, Send AIS-V for Ds1 AIS only works for VT circuits. On DS1/E1-56 cards, Send AIS-V for Ds1 AIS works for both STS and VT circuits.

Step 17 Click **Finish**.

In the Circuits tab, verify that a new circuit appears. This circuit is the Roll To circuit. It is designated with the Roll From circuit name appended with ROLL**.

Step 18 Click the **Rolls** tab. Two new rolls now appear. For each pending roll, view the Roll Valid Signal status. When one of the following requirements is met, continue with Step 19.

- If the Roll Valid Signal status is true, a valid signal was found on the new port. On either the Automatic or the Manual roll, the physical change of the cross-connect to the Roll To path occurs after running the roll command.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If a valid signal is not found, refer to the *Cisco ONS 15454 Troubleshooting Guide*. To cancel the roll, see the "DLP-A489 Cancel a Roll" task on page 21-63.
- The roll is a one-way destination roll and the Roll Valid signal status is false. It is not possible to get a Roll Valid Signal status of true for a one-way destination roll.

Note If you have completed a roll, you cannot cancel the sibling roll. You must cancel the two rolls together.

Note You cannot cancel an automatic roll after a valid signal is found.

- A roll can be forced onto the Roll To Circuit destination without a valid signal by using the Force Valid Signal button. If you choose Force Valid Signal, traffic on the circuit that is involved in the roll will be dropped when the roll is completed.

Step 19 If you selected Manual in Step 5, click both rolls on the Rolls tab and click **Complete** to lock the change of the route to the ROLLTO into the database. If you selected Auto, continue with Step 20.

Note You cannot complete a roll if you cancelled the sibling roll. You must complete the two rolls together.

Step 20 For both manual and automatic rolls, click **Finish** to complete circuit roll process.

Step 21 Return to your originating procedure (NTP).

DLP-A466 Roll Two Cross-Connects on One Optical Circuit Using Manual Routing

Purpose	This task reroutes a network path of an optical circuit using manual routing.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Circuits tab.**

Step 3 Click the circuit that you want to roll to a new path. The circuit must have a DISCOVERED status for you to begin a roll.

Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

Step 5 In the Roll Attributes area, complete the following (Figure 21-11 on page 21-52):

a. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll or **Manual** to create a manual roll.

b. From the Circuit Type drop-down list, choose **Dual** to indicate that you want to roll two connections on the chosen circuit.

Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square representing the fixed path of the first cross-connect to be rolled (Figure 21-7 on page 21-47).

This path is a fixed point in the cross-connect involved in the roll process. The path identifier appears in the text box below the graphic image. The path that is not selected contains the Roll From path. The Roll From path is deleted after the roll is completed.

Step 8 Click **Next**.

Step 9 Complete one of the following:

- If multiple Roll From paths exist, the Select Roll From dialog box appears. Select the path from which you want to roll traffic and click **OK**, then click **Next** (Figure 21-12 on page 21-53).
- If multiple Roll From paths do not exist, click **Next** and continue with Step 10. The circuit status for the Roll From path changes from DISCOVERED to ROLL_PENDING.

Step 10 In the Pivot/Fixed Point 2 window, click the square that represents the fixed path of the second connection to be rolled.

The path that is not selected is the Roll From path. The Roll From path is deleted after the roll is complete. The path identifier appears in the text box below the graphic image.

Step 11 Click **Next**.

Step 12 In the Circuit Routing Preferences area, uncheck **Route Automatically**.

Step 13 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 14.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.

Step 14 If you checked Fully Protected Path, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 15 Click **Next**. Beneath Route Review and Edit, node icons appear for you to route the circuit manually.

The green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit.

Step 16 Complete the "DLP-A369 Provision an OC-N Circuit Route" task on page 20-53.

Caution The following is only seen with DUAL roll mode when both ends of the circuit use the card(s) mentioned in this statement. If the termination card is a DS1/E1-56, DS1-14, DS1-N-14, DS3XM-6, or DS3XM-12 card, a roll will occur even if a valid signal is not detected on the Roll To port. The absence of PDI-P downstream for LOS, LOF, and AIS line defects causes the roll to continue without a valid signal. On the DS1/E1-56, DS1-14, and DS1-N-14 cards, it is possible to check the Send AIS-V For Ds1 AIS check box to properly generate PDI-P downstream for the LOS and LOF AIS line defects. This check box is selected from the card view Provisioning > Line tab. On the DS1-14 and DS1-N-14 cards, Send AIS-V for Ds1 AIS only works for VT circuits. On DS1/E1-56 cards, Send AIS-V for Ds1 AIS works for both STS and VT circuits.

Step 17 Click **Finish**. In the Circuits tab, verify that a new circuit appears.

This circuit is the Roll To circuit. It is designated with the Roll From circuit name appended with ROLL**.

Step 18 Click the **Rolls** tab. Two new rolls now appear on the Rolls tab. For each pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with Step 19.

- If the Roll Valid Signal status is true, a valid signal was found on the new port. On either the Automatic or the Manual roll, the physical change of the cross-connect to the Roll To path occurs after running the roll command.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If the signal is not found, refer to the Circuits and Timing section of the *Cisco ONS 15454 Troubleshooting Guide*. To cancel the roll, see the "DLP-A489 Cancel a Roll" task on page 21-63.
- The roll is a one-way destination roll and the Roll Valid signal status is false. It is not possible to get a Roll Valid Signal status of true for a one-way destination roll.

Note You cannot cancel an automatic roll after a valid signal is found.

- A roll can be forced onto the Roll To Circuit destination without a valid signal by using the Force Valid Signal button. If you choose Force Valid Signal, traffic on the circuit that is involved in the roll will be dropped when the roll is completed.

Step 19 If you selected Manual in Step 5, click each roll and click **Complete** to lock the change of the route to the ROLLTO into the database. If you selected Auto, continue with Step 20.

Note You cannot complete a roll if you cancelled the sibling roll. You must complete the two rolls together.

Step 20 For both manual and automatic rolls, click **Finish** to complete the circuit roll process.

Step 21 Return to your originating procedure (NTP).

DLP-A467 Roll Two Cross-Connects from One Optical Circuit to a Second Optical Circuit

Purpose	This task reroutes a network path using two optical circuits by allowing CTC to select the Roll To path on the second circuit automatically.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Circuits** tab.

Step 3 Press **Ctrl** and click the two circuits that you want to use in the roll process.

The Roll From path will be on one circuit and the Roll To path will be on the other circuit. The circuits must have a DISCOVERED status and must be the same size and direction for you to begin a roll. The planned Roll To circuit must not carry traffic. The first Roll To path must be DCC-connected to the source node of the Roll To circuit, and the second Roll To path must be DCC-connected to the destination node of the Roll To circuit.

Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

Step 5 In the Roll Attributes area, complete the following:

a. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll (required for a 1-way source roll) or **Manual** to create a manual roll (required for 1-way destination roll).

b. From the Circuit Roll Type drop-down list, choose **Dual.**

c. In the Roll From Circuit area, click the circuit that contains the Roll From path.

Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square representing the fixed path of the first cross-connect to be rolled (Figure 21-7 on page 21-47).

This path is a fixed point in the cross-connect involved in the roll process. The path identifier appears in the text box below the graphic image. The path that is not selected contains the Roll From path. The Roll From path is deleted after the roll is completed.

Step 8 Click **Next**.

Step 9 Complete one of the following:

- If multiple Roll From paths exist, the Select Roll From dialog box appears. Select the path from which you want to roll traffic and click **OK** (Figure 21-12 on page 21-53).
- If multiple Roll From paths do not exist, continue with Step 10.

The circuit status for the Roll From path changes from DISCOVERED to ROLL PENDING.

Step 10 In the Pivot/Fixed Point 2 window, click the square that represents the fixed path of the second connection to be rolled.

The path that is not selected is the Roll From path. The Roll From path is deleted after the roll is completed. The path identifier appears in the text box below the graphic image.

Step 11 Click **Next**.

Caution The following is only seen with DUAL roll mode when both ends of the circuit use the card(s) mentioned in this statement. If the termination card is a DS1/E1-56, DS1-14, DS1-N-14, DS3XM-6, or DS3XM-12 card, a roll will occur even if a valid signal is not detected on the Roll To port. The absence of PDI-P downstream for LOS, LOF, and AIS line defects causes the roll to continue without a valid signal. On the DS1/E1-56, DS1-14, and DS1-N-14 cards, it is possible to check the Send AIS-V For Ds1 AIS check box to properly generate PDI-P downstream for the LOS and LOF AIS line defects. This check box is selected from the card view Provisioning > Line tab. On the DS1-14 and DS1-N-14 cards, Send AIS-V for Ds1 AIS only works for VT circuits. On DS1/E1-56 cards, Send AIS-V for Ds1 AIS works for both STS and VT circuits.

Step 12 Click **Finish**. In the Circuits tab, the Roll From and Roll To circuits change from the DISCOVERED status to ROLL PENDING.

Step 13 Click the **Rolls** tab. Two new rolls now appear on the Rolls tab. For each pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with Step 14.

- If the Roll Valid Signal status is true, a valid signal was found on the new port. On either the Automatic or the Manual roll, the physical change of the cross-connect to the Roll To path occurs after running the roll command.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If the signal is not found, refer to the *Cisco ONS 15454 Troubleshooting Guide*. To cancel the roll, see the "DLP-A489 Cancel a Roll" task on page 21-63.
- The roll is a one-way destination roll and the Roll Valid signal status is false. It is not possible to get a Roll Valid Signal status of true for a one-way destination roll.

Note You cannot cancel an automatic roll after a valid signal is found.

- A roll can be forced onto the Roll To Circuit destination without a valid signal by using the Force Valid Signal button. If you choose Force Valid Signal, traffic on the circuit that is involved in the roll will be dropped when the roll is completed.

Step 14 If you selected Manual in Step 5, click both rolls on the Rolls tab and click **Complete** to lock the change of the route to the ROLLTO into the database. If you selected Auto, continue with Step 15.

Note You cannot complete a roll if you cancelled the sibling roll. You must complete the two rolls together.

Step 15 For both manual and automatic rolls, click **Finish** to complete the circuit roll process.

Step 16 Return to your originating procedure (NTP).

DLP-A468 Delete a Roll

Purpose	This task deletes a roll. Use caution when selecting this option, traffic might be affected. Delete a roll only if it cannot be completed or cancelled in normal ways. Circuits might have a PARTIAL status when this option is selected. See Table 21-2 on page 21-3 for a description of circuit statuses.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 NTP-A334 Bridge and Roll Traffic, page 7-11
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Circuits > Rolls** tabs.

Step 3 Click the rolled circuit that you want to delete.

Step 4 From the Tools menu, choose **Circuits > Delete Rolls.**

Step 5 In the confirmation dialog box, click **Yes**.

Step 6 Return to your originating procedure (NTP).

DLP-A469 Install a GBIC or SFP/XFP Device

Purpose	This task installs GBICs (required for E-Series Ethernet, G-Series Ethernet, CE-1000-4, E1000-4, and FC_MR-4 cards) and SFPs/XFPs (required for CE-MR-10, ML1000-2, ML100X-8, ML-MR-10, MXP, MRC-12, MRC-2.5G-4, and OC192-XFP cards) and attaches fiber to the devices. GBICs, SFPs, and XFPs are hot-swappable input/output devices that plug into a traffic card port to link the port with the fiber-optic network. For a description of SFP/XFP devices on transponder or muxponder cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.
Tools/Equipment	To determine which cards are compatible with which GBICs, SFPs, and XFPs, refer to the "Optical Cards" or "Ethernet Cards" chapters in the *Cisco ONS 15454 Reference Manual*.
Prerequisite Procedures	One or more of the following, depending on the card where you will install the GBIC or SFP/XFP device: • NTP-A16 Install Optical Cards and Connectors, page 2-8 • DLP-A39 Install Ethernet Cards, page 17-41 • NTP-A274 Install the FC_MR-4 Card, page 2-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **Class 1 laser product.** Statement 1008

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Note G-Series cards manufactured before August 2003 do not support DWDM GBICs. G1K-4 cards compatible with DWDM GBICs have a Common Language Equipment Identification (CLEI) code of WM5IRWPCAA.

Note All versions of G1K-4 cards support coarse wavelength division multiplexing (CWDM) GBICs.

Note GBICs, SFPs, and XFPs are hot-swappable and can therefore be installed/removed while the card/shelf assembly is powered and running.

Step 1 Remove the GBIC, SFP, or XFP from its protective packaging.

Step 2 Check the label to verify that the GBIC, SFP, or XFP is the correct type for your network. Refer to the "Optical Cards" chapter in the *Cisco ONS 15454 Reference Manual* for a list of card and SFP/XFP compatibility.

Note The GBICs are very similar in appearance. Check the GBIC label carefully before installing it.

Note Before you install SFPs on the MRC-12 or MRC-2.5G-4 card, refer to the MRC-12 or MRC-2.5G-4 card information in the *Cisco ONS 15454 Reference Manual* for bandwidth restrictions based on the port where you install the SFP and the cross-connect card being used.

Step 3 Verify the type of GBIC, SFP, or XFP you are using:

- If you are using a GBIC with clips, go to Step 4.
- If you are using a GBIC with a handle, go to Step 5.
- If you are using an SFP or XFP, go to Step 6.

Step 4 For GBICs with clips:

a. Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the card.

Note GBICs are keyed to prevent incorrect installation.

b. Slide the GBIC through the flap that covers the opening until you hear a click. The click indicates the GBIC is locked into the slot.

c. When you are ready to attach the network fiber-optic cable, remove the protective plug from the GBIC, save the plug for future use, then plug the fiber connector into the GBIC.

d. Continue with Step 7.

Step 5 For GBICs with a handle:

a. Remove the protective plug from the SC-type connector.

b. Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the card.

c. Lock the GBIC into place by closing the handle down. The handle is in the correct closed position when it does not obstruct access to an SC-type connector.

d. Slide the GBIC through the cover flap until you hear a click.

The click indicates that the GBIC is locked into the slot.

e. When you are ready to attach the network fiber-optic cable, remove the protective plug from the GBIC, save the plug for future use, then plug the fiber connector into the GBIC.

f. Continue with Step 7.

Step 6 For SFPs and XFPs:

a. Plug the LC duplex connector of the fiber into a Cisco-supported SFP or XFP.

b. If the new SFP or XFP has a latch, close the latch over the cable to secure it.

c. Plug the cabled SFP or XFP into the card port until it clicks.

SFPs and XFPs must be provisioned in CTC. If you installed a multirate PPM, complete the "DLP-A574 Provision a PPM on the MRC-12 or MRC-2.5G-4 Card" task on page 22-88. (Single-rate XFPs do not need to be provisioned in CTC.)

Step 7 Return to your originating procedure (NTP).

DLP-A470 Remove GBIC or SFP/XFP Devices

Purpose	This task disconnects fiber attached to GBICs, SFPs, or XFPs and removes the GBICs, SFPs, or XFPs from their cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A469 Install a GBIC or SFP/XFP Device, page 21-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Step 1 Disconnect the network fiber cable from the GBIC SC connector or the SFP/XFP LC duplex connector. If the SFP/XFP connector has a latch securing the fiber cable, pull it upward to release the cable.

Step 2 If you are using a GBIC with clips:

a. Release the GBIC from the slot by squeezing the two plastic tabs on each side of the GBIC.

b. Slide the GBIC out of the slot. A flap closes over the slot to protect the connector on the Gigabit Ethernet card.

Step 3 If you are using a GBIC with a handle:

a. Release the GBIC by opening the handle.

b. Pull the handle of the GBIC.

c. Slide the GBIC out of the slot. A flap closes over the slot to protect the connector on the Gigabit Ethernet card.

Step 4 If you are using an SFP/XFP:

a. If the SFP/XFP connector has a latch securing the fiber cable, pull it upward to release the cable.

b. Pull the fiber cable straight out of the connector.

c. Unplug the SFP/XFP connector and fiber from the card.

d. Slide the SFP/XFP out of the slot.

Step 5 Return to your originating procedure (NTP).

DLP-A489 Cancel a Roll

Purpose	This task cancels a roll. When the roll mode is Manual, you can only cancel a roll before you click the Complete button. When the roll mode is Auto, cancelling a roll is only allowed before a good signal is detected by the node or before clicking the Force Valid Signal button. A dual or single roll can be cancelled before the roll state changes to ROLL_COMPLETED.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 NTP-A334 Bridge and Roll Traffic, page 7-11
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution If you click cancel while performing a dual roll in Manual mode and have a valid signal detected on both rolls, you will see a dialog box stating that this can cause a traffic hit and asking if you want to continue with the cancellation. Cisco does not recommend cancelling a dual roll after a valid signal has been detected. To return the circuit to the original state, Cisco recommends completing the roll, then using bridge and roll again to roll the circuit back.

Step 1 From node or network view, click the **Circuits > Rolls** tabs.

Step 2 Click the rolled circuit that you want to cancel.

Step 3 Click **Cancel.**

Step 4 Return to your originating procedure (NTP).

DLP-A495 Consolidate Links in Network View

Purpose	This task consolidates data communications channel (DCC), GCC, optical transport section (OTS), provisionable patchcord (PPC), and server trail links in the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note Global consolidation persists when CTC is re-launched but local consolidation does not.

Step 1 From the View menu, choose **Go to Network View**. CTC shows the link icons by default.

Step 2 Perform the following steps as needed:

- To toggle between the links, go to Step 3.
- To consolidate all the links on the network map, go to Step 4.
- To consolidate a link or links between two nodes, go to Step 5.
- To view information about a consolidated link, go to Step 6.
- To access an individual link within a consolidated link, go to Step 7.
- To expand consolidated links, go to Step 8.
- To filter the links by class, go to Step 9.

Step 3 Right-click on the network map and choose **Show Link Icons** to toggle the link icons on and off.

Step 4 To consolidate all the links on the network map (global consolidation):

a. Right-click anywhere on the network map.

b. Choose **Collapse/Expand Links** from the shortcut menu. The Collapse/Expand Links dialog window appears.

c. Select the check boxes for the link classes you want to consolidate.

d. Click **OK**. The selected link classes are consolidated throughout the network map.

Step 5 To consolidate a link or links between two nodes (local consolidation):

a. Right-click the link on the network map.

b. Choose **Collapse Link** from the shortcut menu. The selected link type consolidates to show only one link.

Note The links consolidate by class. For example, if you select a DCC link for consolidation only the DCC links will consolidate, leaving any other link classes expanded.

Figure 21-13 shows the network view with unconsolidated DCC and PPC links.

Figure 21-13 Unconsolidated Links in the Network View

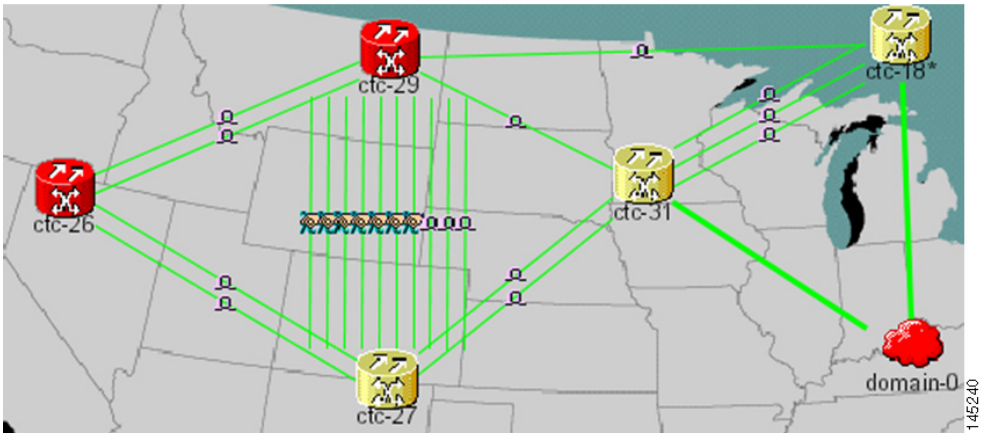


Figure 21-14 shows a network view with globally consolidated links.

Figure 21-14 Consolidated Links in the Network View

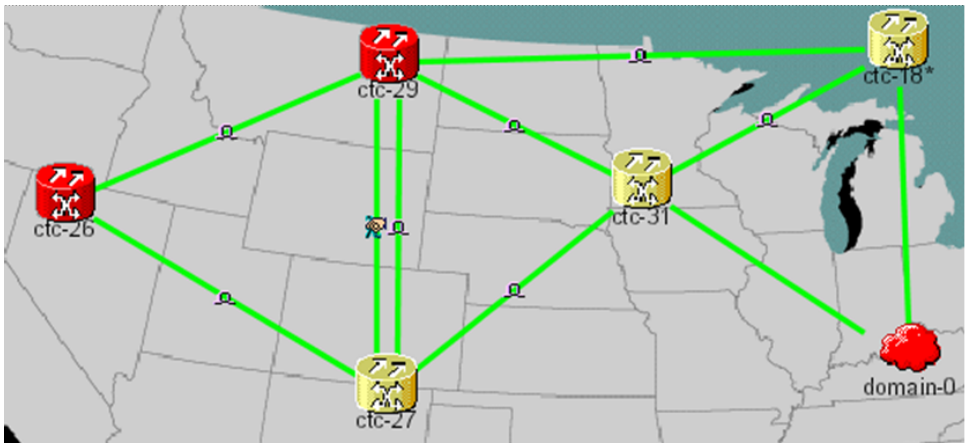
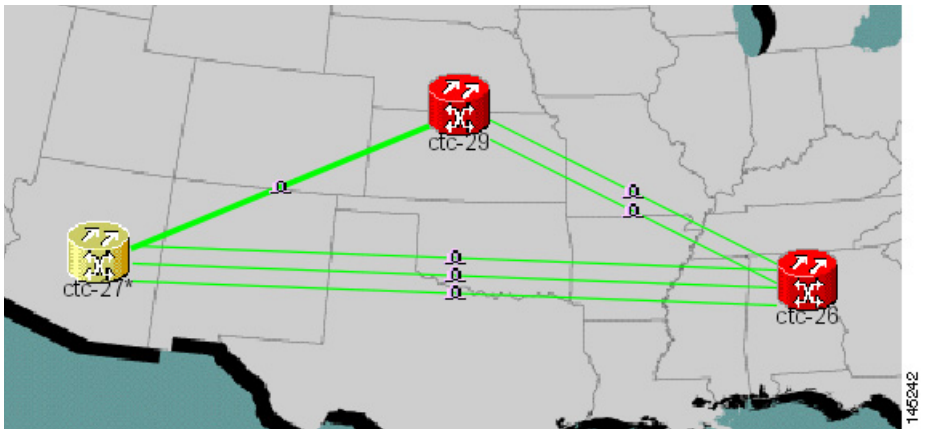


Figure 21-15 shows a network view with local DCC link consolidation between two nodes.

Figure 21-15 Network View with Local Link Consolidation



Step 6 To view information about a consolidated link, either move your mouse over the link (the tooltip displays the number of links and the link class) or single-click the link to display detailed information on the left side of the window.

Step 7 To access an individual link within a consolidated link (for example, if you need to perform a span upgrades):

- **a.** Right-click the consolidated link. A shortcut menu appears with a list of the individual links.
- **b.** Hover the mouse over the selected link. A cascading menu appears where you can select an action for the individual link or navigate to one of the nodes where the link is attached.

Step 8 To expand locally consolidated links, right-click the consolidated link and choose **Expand [***link class***] Links** from the shortcut menu, where "link class" is DCC, GCC, OTS, PPC, or Server Trail.

Step 9 To filter the links by class:

- **a.** Click the **Link Filter** button in the upper right area of the window. The Link Filter dialog appears.

The link classes that appear in the Link Filter dialog are determined by the Network Scope you choose in the network view (Table 21-7).

Table 21-7 Link Classes By Network Scope

Network Scope	Displayed Link Classes
ALL	DCC, GCC, OTS, PPC, Server Trail
DWDM	GCC, OTS, PPC
TDM	DCC, PPC, Server Trail

b. Check the check boxes next to the links you want to display.

c. Click **OK**.

Step 10 Return to your originating procedure (NTP).

DLP-A498 Switch Between TDM and DWDM Network Views

Purpose	This task switches between time division multiplexing (TDM) and dense wavelength division multiplexing (DWDM) network views.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 From the Network Scope drop-down list on the toolbar, choose one of the following:

- **All**—Displays both TDM and DWDM nodes.
- **TDM**—Displays only ONS 15454s with SONET or SDH cards including the transponder (TXP) and muxponder (MXP) cards.
- **DWDM**—Displays only ONS 15454s with DWDM cards, including the TXP and MXP cards.

Note For information about DWDM, TXP, and MXP cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Step 3 Return to your originating procedure (NTP).

CHAPTER 22

DLPs A500 to A599

Note The terms “Unidirectional Path Switched Ring” and “UPSR” may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as “Path Protected Mesh Network” and “PPMN,” refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

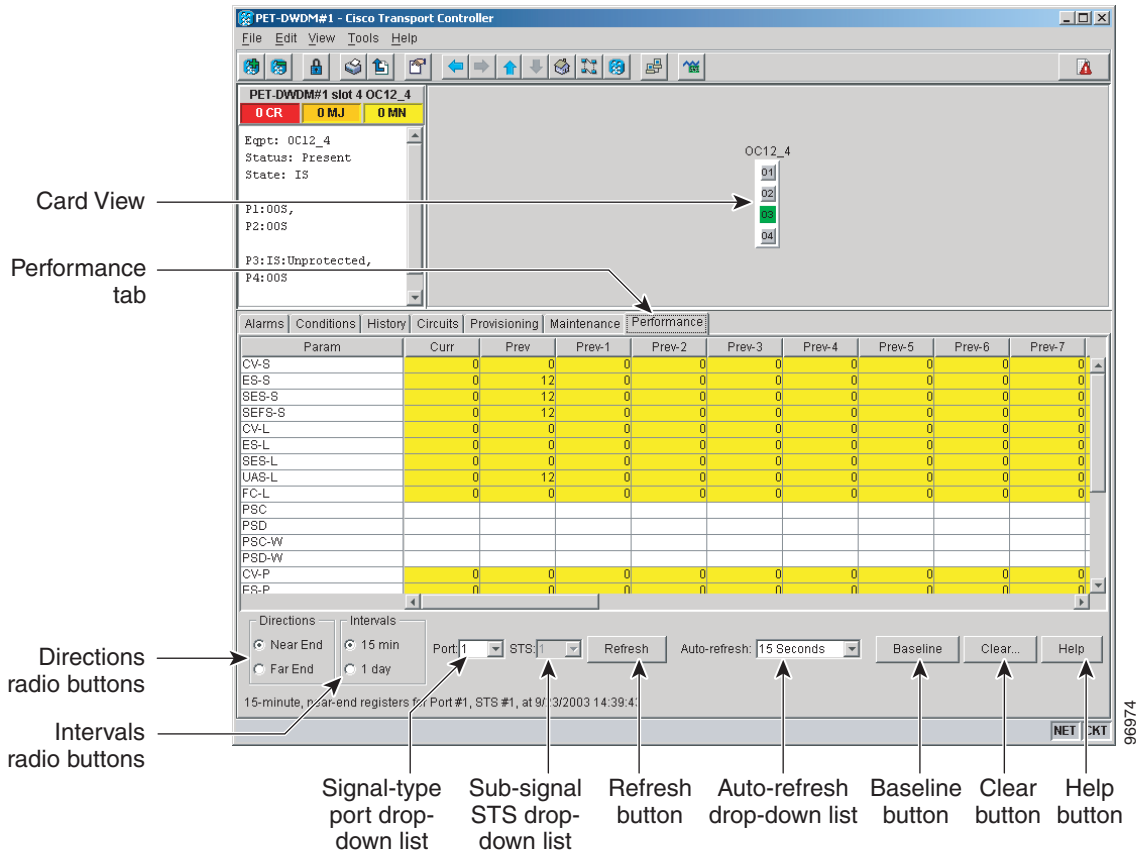
DLP-A507 View OC-N PM Parameters

Purpose	This task enables you to view performance monitoring (PM) counts on an OC-N card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the OC-N card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab (Figure 22-1).

Figure 22-1 Viewing OC-N Card Performance Monitoring Information



Step 3 In the Port drop-down list, click the port you want to monitor.

Step 4 Click **Refresh**.

Step 5 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current), and Prev-*n* (previous) columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 6 To monitor another port on a multiport card, choose another port from the Port drop-down list and click **Refresh**.

Step 7 Return to your originating procedure (NTP).

DLP-A509 Provision CE-1000-4 Ethernet Ports

Purpose	This task provisions CE-1000-4 Ethernet ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You can provision SONET contiguous concatenated (CCAT) or virtual concatenated (VCAT) circuits for the CE-1000-4 before or after provisioning the card's Ethernet ports and/or packet-over-SONET (POS) ports. See the "NTP-A343 Create an Automatically Routed Optical Circuit" procedure on page 6-40 or the "NTP-A264 Create an Automatically Routed VCAT Circuit" procedure on page 6-81, as needed.

Note CCAT circuits can be created only if a contiguous pool of STSs is available. The Ethernet ports are automatically allocated STSs from the available Cisco ONS 15454 SONET bandwidth on the CE-1000-4 card.

Step 1 In node view, double-click the CE-1000-4 card graphic to open the card.

Step 2 Click the **Provisioning > Ether Ports** tabs.

Step 3 For each CE-1000-4 port, provision the following parameters:

- Port Name—If you want to label the port, enter the port name.

Note Circuit table displays port name of the POS port and not the Ethernet port. For information on viewing the circuit table, see DLP-A416 View Circuit Information, page 21-2.

- Admin State—Select the service state for the port. See the "DLP-A214 Change the Service State for a Port" task on page 19-9 for more information.

Note CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.

- Flow Control—Select the flow control for the port. Possible values are **None**, **Symmetrical**, and **Pass Through**.
- Auto Negotiation—Click this check box to enable autonegotiation on the port (default). If you do not want to enable autonegotiation control, uncheck the box.
- MTU—If you want to permit the acceptance of jumbo size Ethernet frames, choose 10004(default). If you do not want to permit jumbo size Ethernet frames, choose 1548.
- Watermark—Select the flow control watermark for the port. To provision the Low Latency flow control watermark, choose **Low Latency** from the drop-down list. The Flow Ctrl Lo and Flow Ctrl Hi values change. To provision a Custom flow control watermark, choose **Custom** from the

drop-down list. Enter values in the Flow Ctrl Hi and Flow Ctrl Lo columns. The Flow Ctrl Lo value has a valid range from 1 to 510 and the Flow Ctrl Hi value has a valid range from 2 to 511. The Flow Ctrl Lo value must be lower than the Flow Ctrl Hi value.

Step 4 Click **Apply**.

Step 5 Refresh the Ethernet statistics:

a. Click the **Performance > Ether Ports > Statistics** tabs.

b. Click **Refresh**.

Note Reprovisioning an Ethernet port on the CE-1000-4 card does not reset the Ethernet statistics for that port.

Step 6 Return to your originating procedure (NTP).

DLP-A510 Provision a DS-3 Circuit Source and Destination

Purpose	This task provisions an electrical circuit source and destination for a DS-3 circuit.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note After you have selected the circuit properties in the Circuit Source dialog box according to the specific circuit creation procedure, you are ready to provision the circuit source.

Step 1 From the Node drop-down list, choose the node where the source will originate.

Step 2 From the Slot drop-down list, choose the slot containing the DS-3 card where the circuit will originate. If you are configuring a DS-3 circuit with a transmux card, choose the DS3XM-6 or DS3XM-12 card.

Step 3 From the Port drop-down list, choose the source DS-3, DS3/EC1-48, DS3XM-6, or DS3XM-12 card as appropriate.

Step 4 If you need to create a secondary source, for example, a path protection bridge/selector circuit entry point in a multivendor path protection configuration, click **Use Secondary Source** and repeat Steps 1 through 3 to define the secondary source. If you do not need to create a secondary source, continue with Step 5.

Step 5 Click **Next**.

Step 6 From the Node drop-down list, choose the destination (termination) node.

Step 7 From the Slot drop-down list, choose the slot containing the destination card. The destination is typically a DS3XM-6 or DS-3 card. You can also choose an OC-N card to map the DS-3 circuit to a synchronous transport signal (STS).

Step 8 Depending on the destination card, choose the destination port or STS from the drop-down lists that appear based on the card selected in Step 2. See Table 6-2 on page 6-3 for a list of valid options. Cisco Transport Controller (CTC) does not display ports, STSs, Virtual Tributaries (VTs), or DS3s if they are already in use by other circuits. If you and another user who is working on the same network choose the same port, STS, VT, port, or DS3 simultaneously, one of you receives a Path in Use error and is unable to complete the circuit. The user with the partial circuit needs to choose new destination parameters.

Step 9 If you need to create a secondary destination, for example, a path protection bridge/selector circuit exit point in a multivendor path protection configuration, click **Use Secondary Destination** and repeat Steps 6 through 8 to define the secondary destination.

Step 10 Click **Next**.

Step 11 Return to your originating procedure (NTP).

DLP-A512 Change Node Access and PM Clearing Privilege

Purpose	This task provisions the physical access points and shell programs used to connect to the ONS 15454 and sets the user security level that can clear node PM data.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning > Security > Access** tabs.

Step 2 In the Access area, provision the following:

- LAN access—Choose one of the following options to set the access paths to the node:
  - **No LAN Access**—Allows access to the node only through data communications channel (DCC) connections. Access through the TCC2/TCC2P RJ-45 port and backplane is not permitted.

Note After TCC reset, backplane LAN access gets enabled even if you have set the Access type to No LAN Access.

  - **Front only**—Allows access through the TCC2/TCC2P RJ-45 port. Access through the DCC and the backplane is not permitted.
  - **Backplane only**—Allows access through DCC connections and the backplane. Access through the TCC2/TCC2P RJ-45 port is not allowed.
  - **Front and Backplane**—Allows access through DCC, TCC2/TCC2P RJ-45, and backplane connections.

- Restore Timeout—Sets a time delay for enabling of front and backplane access when DCC connections are lost and "DCC only" is chosen in LAN Access. Front and backplane access is enabled after the restore timeout period has passed. Front and backplane access is disabled as soon as DCC connections are restored.
- Disable IPv4 access for IPv6 enabled ports—Select this option to disable IPv4 on ports which are IPv6 enabled. Before you select this option, ensure that IPv6 is enabled and the node is not in multishelf mode.

Step 3 In the Shell Access area, set the shell program used to access the node:

- Access State: Allows you to set the shell program access mode to Disable (disables shell access), Non-Secure, Secure. Secure mode allows access to the node using the Secure Shell (SSH) program. SSH is a terminal-remote host Internet protocol that uses encrypted links.
- Telnet Port: Allows access to the node using the Telnet port. Telnet is the terminal-remote host Internet protocol developed for the Advanced Agency Research Project Network (ARPANET). Port 23 is the default.
- Enable Shell Password: If checked, enables the SSH password. To disable the password, you must uncheck the check box and click Apply. You must type the password in the confirmation dialog box and click OK to disable it.

Step 4 In the TL1 Access area, select the desired level of TL1 access. Disabled completely disables all TL1 access; Non-Secure, Secure allows access using SSH.

Step 5 In the PM Clearing Privilege field, choose the minimum security level that can clear node PM data: PROVISIONING or SUPERUSER.

Step 6 Select the Enable Craft Port check box to turn on the shelf controller serial ports.

Step 7 Select the EMS access state from the list. Available states are Non-Secure and Secure (allows access using SSH).

In the TCC CORBA (IIOP/SSLIOP) Listener Port area, choose a listener port option:

- **Default - TCC Fixed**—Uses Port 57790 to connect to ONS 15454s on the same side of the firewall or if no firewall is used (default). This option can be used for access through a firewall if Port 57790 is open.
- **Standard Constant**—Uses Port 683 (IIOP) or Port 684 (SSLIOP), the Common Object Request Broker Architecture (CORBA) default port number.
- **Other Constant**—If the default port is not used, type the Internet Inter-ORB Protocol (IIOP) or SSLIOP port specified by your firewall administrator.

Step 8 In the SNMP Access area, set the Simple Network Management Protocol (SNMP) access state to Non-Secure or Disabled (disables SNMP access).

Step 9 Click **Apply**.

Step 10 Return to your originating procedure (NTP).

DLP-A513 Provision CE-100T-8 and CE-MR-10 Ethernet Ports

Purpose	This task provisions CE-100T-8 and CE-MR-10 Ethernet ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You can provision SONET contiguous concatenated (CCAT) or virtual concatenated (VCAT) circuits for the CE-100T-8 and CE-MR-10 cards before or after provisioning the card's Ethernet ports and/or packet-over-SONET (POS) ports. See the "NTP-A343 Create an Automatically Routed Optical Circuit" procedure on page 6-40 or the "NTP-A264 Create an Automatically Routed VCAT Circuit" procedure on page 6-81, as needed.

Step 1 In node view, double-click the CE-100T-8 or CE-MR-10 card graphic to open the card.

Step 2 Click the **Provisioning** > **Ether Ports** tabs.

Step 3 For each CE-100T-8 or CE-MR-10 port, provision the following parameters:

- Port Name—If you want to label the port, enter the port name.

Note Circuit table displays port name of the POS port and not the Ethernet port. For information on viewing the circuit table, see DLP-A416 View Circuit Information, page 21-2.

- Admin State—Choose **IS** to put the port in service.
- Expected Speed—Choose the expected speed of the device that is or will be attached to the Ethernet port. If you know the speed, choose **100 Mbps** or **10 Mbps** (for CE-100T-8), or **1000 Mbps**, **100 Mbps,** or **10 Mbps** (for CE-MR-10) to match the attached device. If you do not know the speed, choosing **Auto** enables autonegotiation for the speed of the port, and the CE-100T-8 or CE-MR-10 port will attempt to negotiate a mutually acceptable speed with the attached device. If the expected speed is set to **Auto**, you cannot enable selective autonegotiation.
- Expected Duplex—Choose the expected duplex of the device that is or will be attached to the Ethernet port. If you know the duplex, choose **Full** or **Half** to match the attached device. If you do not know the duplex, choosing **Auto** enables autonegotiation for the duplex of the port, and the CE-100T-8 or CE-MR-10 port will attempt to negotiate a mutually acceptable duplex with the attached device. If the expected duplex is set to **Auto**, you cannot enable selective autonegotiation.
- Enable Selective Auto Negotiation—Click this check box to enable selective autonegotiation on the Ethernet port. If you do not want to enable selective autonegotiation, uncheck the box. If checked, the CE-100T-8 or CE-MR-10 port attempts to autonegotiate only to the selected expected speed and duplex. The link will come up if both the expected speed and duplex of the attached autonegotiating device matches that of the port. You cannot enable selective autonegotiation if either the expected speed or expected duplex is set to **Auto**.
- Enable Flow Control—Click this check box to enable flow control on the port (default). If you do not want to enable flow control, uncheck the box. The CE-100T-8 or CE-MR-10 card attempts to negotiate symmetrical flow control with the attached device.

- 802.1Q VLAN CoS—For a class-of-service (CoS)-tagged frame, the CE-100T-8 or CE-MR-10 card can map the eight priorities specified in CoS for either priority or best effort treatment. Any CoS class higher than the class specified in CTC is mapped to priority, which is the treatment geared towards low latency. By default, the CoS is set to 7, which is the highest CoS value. The default results in all traffic being treated as best effort.
- IP ToS—The CE-100T-8 or CE-MR-10 card can also map any of the 256 priorities specified in IP type-of-service (ToS) to either priority or best effort treatment. Any ToS class higher than the class specified in CTC is mapped to priority, which is the treatment geared towards low latency. By default, the ToS is set to 255, which is the highest ToS value. This results in all traffic being sent to the best effort queue by default.

Note Untagged traffic is treated as best effort.

Note If traffic is tagged with both CoS and IP ToS, then the CoS value is used, unless the CoS value is 7.

Step 4 Click **Apply**.

Step 5 Refresh the Ethernet statistics:

a. Click the **Performance > Ether Ports > Statistics** tabs.

b. Click **Refresh**.

Note Reprovisioning an Ethernet port on the CE-100T-8 or CE-MR-10 card does not reset the Ethernet statistics for that port.

Step 6 Return to your originating procedure (NTP).

DLP-A514 Provision CE-100T-8, CE-1000-4, and CE-MR-10 POS Ports

Purpose	This task provisions CE-100T-8, CE-1000-4, or CE-MR-10 POS ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You can provision SONET CCAT or VCAT circuits for the CE-Series card before or after provisioning the card's Ethernet ports and/or POS ports. See the "NTP-A343 Create an Automatically Routed Optical Circuit" procedure on page 6-40 or the "NTP-A264 Create an Automatically Routed VCAT Circuit" procedure on page 6-81, as needed.

Step 1 In node view, double-click the CE-100T-8, CE-1000-4, or CE-MR-10 card graphic to open the card.

Step 2 Click the **Provisioning > POS Ports** tabs.

Step 3 For each CE-100T-8, CE-1000-4, or CE-MR-10 port, provision the following parameters:

- Port Name—If you want to label the port, enter the port name.

Note Circuit table displays port name of the POS port and not the Ethernet port. For information on viewing the circuit table, see DLP-A416 View Circuit Information, page 21-2.

- Admin State—Choose **IS** to put the port in service.
- Framing Type—Choose **GPF-F** POS framing (the default) or **HDLC** POS framing. The framing type needs to match the framing type of the POS device at the end of the SONET circuit.
- Encap CRC—With GFP-F framing, the user can configure a **32-bit** cyclic redundancy check (CRC) (the default) or **none** (no CRC). HDLC framing provides a set 32-bit CRC. The CRC should be set to match the CRC of the POS device on the end of the SONET circuit.

Note For more details about the interoperabilty of Optical Networking System (ONS) Ethernet cards, including information on encapsulation, framing, and CRC, refer to the "POS on ONS Ethernet Cards" chapter of the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

Note The CE-Series cards use LEX encapsulation, which is the primary POS encapsulation used in ONS Ethernet cards.

Step 4 Click **Apply**.

Step 5 Refresh the POS statistics:

a. Click the **Performance > POS Ports > Statistics** tabs.

b. Click **Refresh**.

Step 6 Return to your originating procedure (NTP).

DLP-A517 View Alarm or Event History

Purpose	This task is used to view past cleared and uncleared ONS 15454 alarm messages at the card, node, or network level. This task is useful for troubleshooting configuration, traffic, or connectivity issues that are indicated by alarms.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Decide whether you want to view the alarm message history at the node, network, or card level.

Step 2 To view node alarm history:

a. Click the **History > Session** tabs to view the alarms and conditions (events) raised during the current session.

b. Click the **History > Shelf** tabs.

If you check the **Alarms** check box, the node's alarm history appears. If you check the **Events** check box, the node's Not Alarmed and transient event history appears. If you check both check boxes, you will retrieve node history for both alarms and events.

c. Click **Retrieve** to view all available messages for the History > Shelf tabs.

Note Alarms can be unreported when they are filtered out of the display using the Filter button in either tab. See the "DLP-A225 Enable Alarm Filtering" task on page 19-17 for information.

Tip Double-click an alarm in the alarm table or an event (condition) message in the history table to display the view that corresponds to the alarm message. For example, double-clicking a card alarm takes you to card view. In network view, double-clicking a node alarm takes you to node view.

Step 3 To view network alarm history, from node view:

a. From the View menu choose **Go to Network View**.

b. Click the **History** tab.

Alarms and conditions (events) raised during the current session appear.

Step 4 To view card alarm history from node view:

a. From the View menu choose **Go to Previous View**.

b. Double-click a card on the shelf graphic to open the card-level view.

Note TCC2/TCCP cards and cross-connect (XCVT, XC10G, or XC-VXL-10G) cards do not have a card view.

c. Click the **History > Session** tab to view the alarm messages raised during the current session.

d. Click the **History > Card** tab to retrieve all available alarm messages for the card and click **Retrieve**.

If you check the **Alarms** check box, the node's alarm history appears. If you check the **Events** check box, the node's Not Alarmed and transient event history appears. If you check both check boxes, you will retrieve node history for both alarms and events.

Note The ONS 15454 can store up to 640 critical alarm messages, 640 major alarm messages, 640 minor alarm messages, and 640 condition messages. When any of these limits is reached, the ONS 15454 discards the oldest events in that category.

Raised and cleared alarm messages (and events, if selected) appear.

Step 5 Return to your originating procedure (NTP).

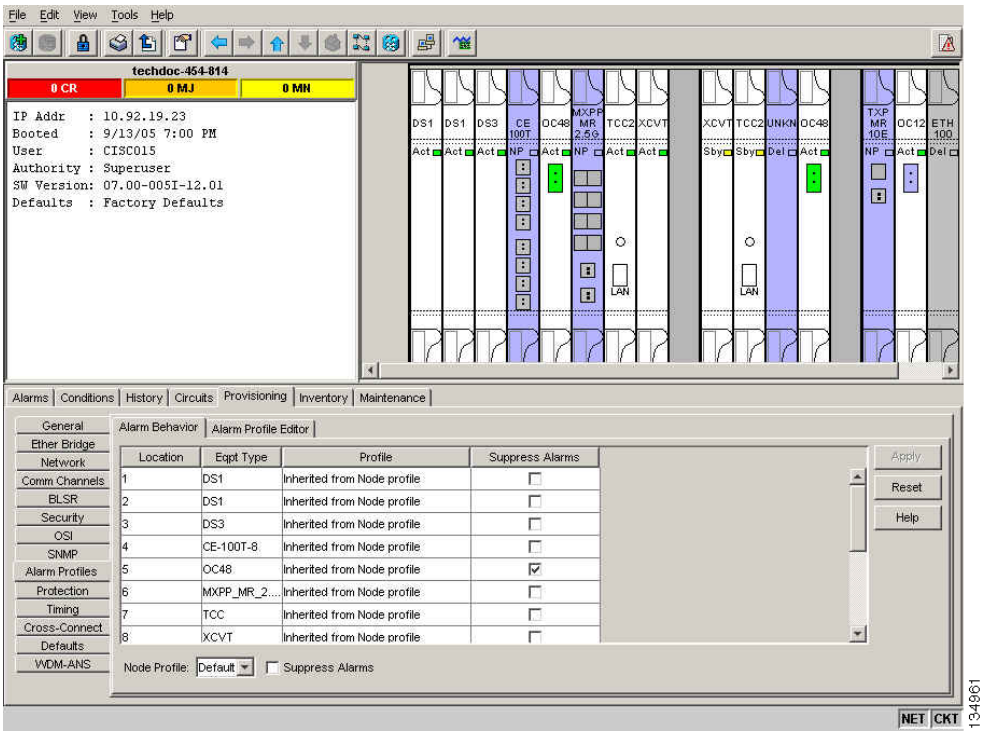
DLP-A518 Create a New or Cloned Alarm Severity Profile

Purpose	This task creates a custom severity profile or clones and modifies the default severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs.

Step 2 To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs (Figure 22-2).

Figure 22-2 Node View Alarm Profile Editor



Step 3 To access the profile editor from a card view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 4 If you want to create a new profile based upon the default profile in use, click **New**. Then go to Step 10.

Step 5 If you want to create a profile using an existing profile located on the node, click **Load** and **From Node** in the Load Profile(s) dialog box.

- **a.** Click the node name you are logged into in the Node Names list.
- **b.** Click the name of an existing profile in the Profile Names list, such as **Default**. Then go to Step 7.

Step 6 If you want to create a profile using an existing profile located in a file that is stored locally or on a network drive, click **From File** in the Load Profile(s) dialog box.

- **a.** Click **Browse**.
- **b.** Navigate to the file location in the **Open** dialog box.
- **c.** Click **Open**.

Note All default or user-defined severity settings that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.

Step 7 Click **OK**.

The alarm severity profile appears in the Alarm Profiles window. The alarm profile list contains a master list of alarms that is used for a mixed node network. Some of these alarms might not be used in all ONS nodes.

Step 8 Right-click anywhere in the profile column to view the profile editing shortcut menu. (Refer to Step 11 for further information about the Default profile.)

Step 9 Click **Clone** in the shortcut menu.

Tip To see the full list of profiles, including those available for loading or cloning, click Available. You must load a profile before you can clone it.

Step 10 In the New Profile or Clone Profile dialog box, enter a name in the New Profile Name field.

Profile names must be unique. If you try to import or name a profile that has the same name as another profile, CTC adds a suffix to create a new name. Long file names are supported.

Step 11 Click **OK**.

A new alarm profile (named in Step 10) is created. This profile duplicates the default profile severities and appears at the right of the previous profile column in the Alarm Profiles window. You can select it and drag it to a different position.

Note Up to 10 profiles, including the two reserved profiles, Inherited and Default, can be stored in CTC.

The Default profile sets severities to standard Telcordia GR-253-CORE settings. If an alarm has an Inherited profile, it inherits (copies) its severity from the same alarm's severity at the higher level. For example, if you choose the Inherited profile from the network view, the severities at the lower levels (node, card and port) will be copied from this selection. A card with an Inherited alarm profile copies the severities used by the node that contains the card. (If you are creating profiles, you can apply these separately at any level. To do this, complete the "DLP-A117 Apply Alarm Profiles to Cards and Nodes" task on page 18-5.)

Step 12 Modify (customize) the new alarm profile:

a. In the new alarm profile column, click the alarm severity you want to change in the custom profile.

b. Choose a severity from the drop-down list.

c. Repeat Steps a and b for each severity you want to customize. Refer to the following guidelines when you view the alarms or conditions after making modifications:

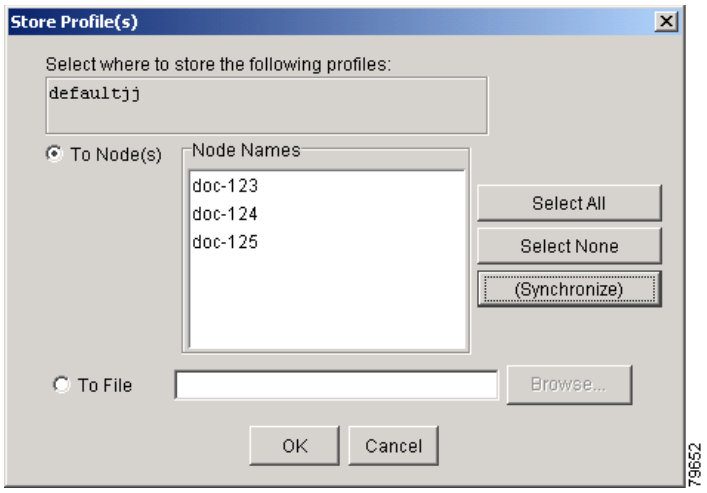
- All Critical (CR) or Major (MJ) default or user-defined severity settings are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.
- Default severities are used for all alarms and conditions until you create and apply a new profile.
- Changing a severity to inherited (I) or unset (U) does not change the severity of the alarm.

Step 13 After you have customized the new alarm profile, right-click the profile column to highlight it.

Step 14 Click **Store**.

Step 15 In the Store Profile(s) dialog box, click **To Node(s)** and go to Step a or click **To File** and go to Step b (Figure 22-3).

Figure 22-3 Store Profiles Dialog Box



a. Choose the nodes where you want to save the profile:
   - If you want to save the profile to only one node, click the node in the Node Names list.
   - If you want to save the profile to all nodes, click **Select All**.
   - If you do not want to save the profile to any nodes, click **Select None**.
   - If you want to update alarm profile information, click **(Synchronize)**.

b. Save the profile:
   - Click **Browse** and navigate to the profile save location.
   - Enter a name in the File name field.
   - Click **Select** to choose this name and location. Long file names are supported. CTC supplies a suffix of *.pfl to stored files.
   - Click **OK** to store the profile.

Step 16 As needed, perform any of the following actions:

- Click the **Hide Identical Rows** check box to configure the Alarm Profiles window to view rows with dissimilar severities.
- Click the **Hide Reference Values** check box to configure the Alarm Profiles window to view severities that do not match the Default profile.
- Click the **Only show service-affecting severities** check box to configure the Alarm Profiles window not to display Minor and some Major alarms that will not affect service.

Step 17 Return to your originating procedure (NTP).

DLP-A519 Apply Alarm Profiles to Ports

Purpose	This task applies a custom or default alarm severity profile to a port or ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A518 Create a New or Cloned Alarm Severity Profile, page 22-11 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, double-click a card to open the card view.

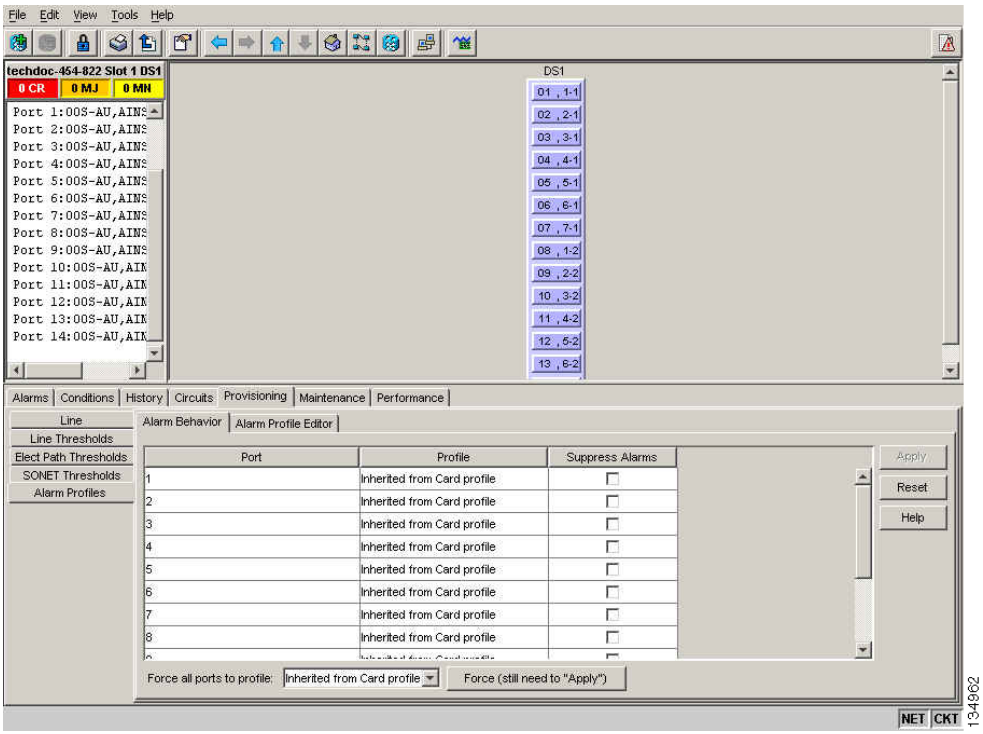
Note You can also apply alarm profiles to cards using the "DLP-A117 Apply Alarm Profiles to Cards and Nodes" task on page 18-5.

Note The card view is not available for the TCC2/TCCP or cross-connect cards.

Step 2 Click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

Figure 22-4 shows the alarm profiles of DS1/E1-56 card ports. CTC shows Parent Card Profile: Inherited.

Figure 22-4 DS1-N-14 Card Alarm Behavior Tab



Go to Step 3 to apply profiles to a port. Go to Step 4 to apply profiles to all ports on a card.

Step 3 To apply profiles on a port basis:

a. In card view, click the port row in the Profile column.

b. Choose the new profile from the drop-down list.

c. Click **Apply**.

Step 4 To apply profiles to all ports on a card:

a. In card view, click the **Force all ports to profile** drop-down arrow at the bottom of the window.

b. Choose the new profile from the drop-down list.

c. Click **Force (still need to "Apply")**.

d. Click **Apply**.

In node view the Port Level Profiles column indicates port-level profiles with a notation such as "exist (1)" (Figure 18-3 on page 18-6).

Step 5 To reapply a previous alarm profile after you have applied a new one, select the previous profile and click **Apply** again.

Step 6 Return to your originating procedure (NTP).

DLP-A520 Delete Alarm Severity Profiles

Purpose	This task deletes a custom or default alarm severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 To access the alarm profile editor from network view, go to network view and click the **Provisioning > Alarm Profiles** tabs.

Step 2 To access the profile editor from node view, go to node view and click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

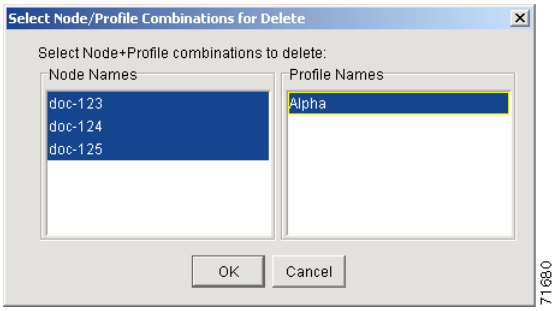
Step 3 To access the profile editor from a card view, double-click the card to display the card view and click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 4 Click the profile you are deleting to select it.

Step 5 Click **Delete**.

The Select Node/Profile Combination for Delete dialog box appears (Figure 22-5).

Figure 22-5 Select Node/Profile Combination For Delete Dialog Box



Note You cannot delete the Inherited or Default alarm profiles.

Note A previously created alarm profile cannot be deleted unless it has been stored on the node. If the profile is visible on the Alarm Profiles tab but is not listed in the Select Node/Profile Combinations to Delete dialog box, continue with Step 9.

Step 6 Click the node names in the Node Names list to highlight the profile location.

Tip If you hold the Shift key down, you can select consecutive node names. If you hold the Ctrl key down, you can select any combination of nodes.

Step 7 Click the profile names you want to delete in the Profile Names list.

Step 8 Click **OK**.

Click **Yes** in the Delete Alarm Profile dialog box.

Note If you delete a profile from a node, it still appears in the network view Provisioning > Alarm Profile Editor window unless you remove it using the following step.

Step 9 To remove the alarm profile from the window, right-click the column of the profile you deleted and choose **Remove** from the shortcut menu.

Note If a node and profile combination is selected but does not exist, a warning appears: "One or more of the profile(s) selected do not exist on one or more of the node(s) selected." For example, if node A has only profile 1 stored and the user tries to delete both profile 1 and profile 2 from node A, this warning appears. However, the operation still removes profile 1 from node A.

Note The Default and Inherited special profiles cannot be deleted and do not appear in the Select Node/Profile Combination for Delete Window.

Step 10 Return to your originating procedure (NTP).

DLP-A521 Modify Alarm, Condition, and History Filtering Parameters

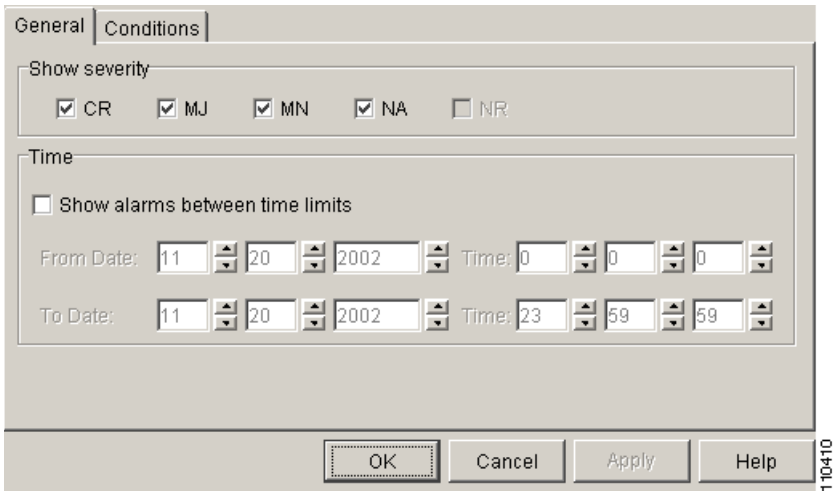
Purpose	This task changes alarm and condition reporting in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A225 Enable Alarm Filtering, page 19-17 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 At the node, network, or card view, click the **Alarms** tab, **Conditions** tab, or **History** tab.

Step 2 Click the **Filter** button at the lower-left of the bottom toolbar.

The filter dialog box appears, displaying the General tab. Figure 22-6 shows the Alarm Filter dialog box; the Conditions and History tabs have similar dialog boxes.

Figure 22-6 Alarm Filter Dialog Box General Tab



In the General tab Show Severity box, you can choose which alarm severities will show through the alarm filter and provision a time period during which filtered alarms show through the filter. To change the alarm severities shown in the filter, go to Step 3. To change the time period filter for the alarms go to Step 4.

Step 3 In the Show Severity area, click the check boxes for the severities [Critical (CR), Major (MJ), Minor (MN), or Not-Alarmed (NA)] you want to be reported at the network level. Leave severity check boxes deselected (unchecked) to prevent those severities from appearing.

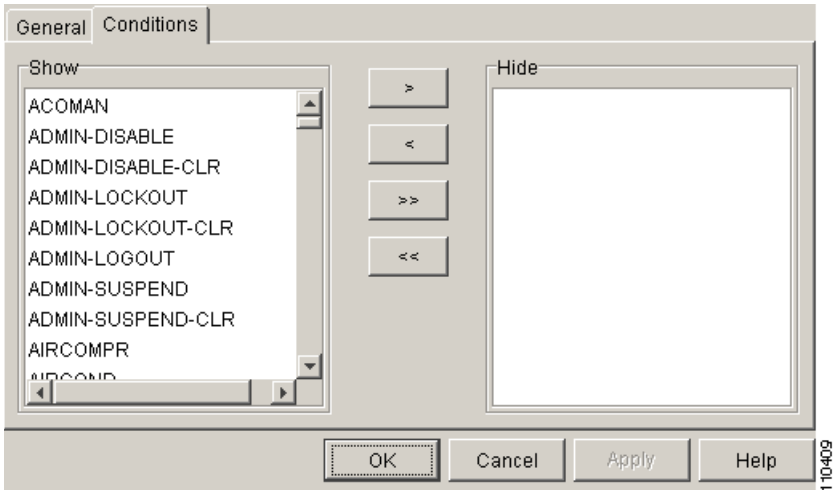
When alarm filtering is disabled, all alarms show.

Step 4 In the Time area, click the **Show alarms between time limits** check box to enable it. Click the up and down arrows in the From Date, To Date, and Time fields to modify what period of alarms are shown.

To modify filter parameters for conditions, continue with Step 5. If you do not need to modify them, continue with Step 6.

Step 5 Click the filter dialog box **Conditions** tab (Figure 22-7).

Figure 22-7 Alarm Filter Dialog Box Conditions Tab



When filtering is enabled, conditions in the Show list are visible and conditions in the Hide list are invisible.

- To move conditions individually from the Show list to the Hide list, click the > button.
- To move conditions individually from the Hide list to the Show list, click the < button.
- To move conditions collectively from the Show list to the Hide list, click the >> button.
- To move conditions collectively from the Hide list to the Show list, click the << button.

Note Conditions include alarms.

Step 6 Click **Apply** and **OK**.

Alarm and condition filtering parameters are enforced when alarm filtering is enabled (see the "DLP-A225 Enable Alarm Filtering" task on page 19-17), and the parameters are not enforced when alarm filtering is disabled (see the "DLP-A227 Disable Alarm Filtering" task on page 19-18).

Step 7 Return to your originating procedure (NTP).

DLP-A522 Suppress Alarm Reporting

Purpose	This task suppresses the reporting of ONS 15454 alarms at the node, card, or port level.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution If multiple CTC/TL1 sessions are open, suppressing alarms in one session suppresses the alarms in all other open sessions.

Note Alarm suppression at the node level does not supersede alarm suppression at the card or port level. Suppression can exist independently for all three entities, and each entity will raise separate alarms suppressed by the user command (AS-CMD) alarm.

Step 1 If you are in node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

Step 2 To suppress alarms for the entire node:

a. Check the **Suppress Alarms** check box.

b. Click **Apply**.

All raised alarms for the node will change color to white in the Alarms window and their status will change to cleared. After suppressing alarms, clicking **Synchronize** in the Alarms window will remove cleared alarms from the window. However, an AS-CMD alarm will show in node or card view to indicate that node-level alarms were suppressed, and the word System will appear in the Object column.

Note The only way to suppress BITS, power source, or system alarms is to suppress alarms for the entire node. These cannot be suppressed separately, but the shelf backplane can be.

Step 3 To suppress alarms for individual cards:

a. Locate the card row (using the Location column for the slot number or the Eqpt Type column for the equipment name).

b. Check the **Suppress Alarms column** check box on that row.

Alarms that directly apply to this card will change appearance as described in Step 2. For example, if you suppressed raised alarms for an OC-48 card in Slot 16, raised alarms for this card will change in node or card view. The AS-CMD alarm will show the slot number in the Object number. For example, if you suppressed alarms for a Slot 16 OC-48 card, the AS-CMD object will be "SLOT-16."

Click **Apply**.

Step 4 To suppress alarms for individual card ports, double-click the card in node view.

Step 5 Click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

Step 6 Check the **Suppress Alarms** column check box for the port row where you want to suppress alarms (Figure 22-4 on page 22-16).

Step 7 Click **Apply**.

Alarms that apply directly to this port will change appearance as described in Step 2. (However, alarms raised on the entire card will remain raised.) A raised AS-CMD alarm that shows the port as its object will appear in either alarm window. For example, if you suppressed alarms for Port 1 on the Slot 16 OC-48 card, the alarm object will show "FAC-16-1."

Step 8 Return to your originating procedure (NTP).

DLP-A523 Discontinue Alarm Suppression

Purpose	This task discontinues alarm suppression and reenables alarm reporting on a port, card, or node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A522 Suppress Alarm Reporting, page 22-20 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution If multiple CTC sessions are open, discontinuing suppression in one session will discontinue suppression in all other open sessions.

Step 1 To discontinue alarm suppression for the entire node:

a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tab.

b. Uncheck the **Suppress Alarms** check box.

Suppressed alarms will reappear in the Alarms window. (They might have previously been cleared from the window using the Synchronize button.) The AS-CMD alarm with the System object will be cleared in all views.

Step 2 To discontinue alarm suppression for individual cards:

a. In the node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

b. Locate the card that was suppressed in the slot list.

c. Uncheck the Suppress Alarms column check box for that slot.

d. Click **Apply**.

Suppressed alarms will reappear in the Alarms window. (They might have previously been cleared from the window using the Synchronize button.) The AS-CMD alarm with the slot object (for example, SLOT-16) will be cleared in all views.

Step 3 To discontinue alarm suppression for ports, double-click the card to open the card view and click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

Step 4 Uncheck the **Suppress Alarms** check box for the port(s) you no longer want to suppress.

Step 5 Click **Apply**.

Suppressed alarms will reappear in the Alarms window. (They might have previously been cleared from the window using the Synchronize button.) The AS-CMD alarm with the port object (for example, FAC-16-1) will be cleared in all views.

Step 6 Return to your originating procedure (NTP).

DLP-A524 Download an Alarm Severity Profile

Purpose	This task downloads a custom alarm severity profile from a network-drive accessible CD-ROM, floppy disk, or hard disk location.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs.

Step 2 To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 3 To access the profile editor from a card view, double-click the card to open the card view and click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 4 Click **Load**.

Step 5 If you want to download a profile that exists on the node, click **From Node** in the Load Profile(s) dialog box.

a. Click the node name you are logged into in the Node Names list.

b. Click the name of the profile in the Profile Names list, such as **Default**.

Step 6 If you want to download a profile that is stored locally or on a network drive, click **From File** in the Load Profile(s) dialog box.

a. Click **Browse**.

b. Navigate to the file location in the **Open** dialog box.

c. Click **Open**.

Note The Default alarm profile list contains alarm and condition severities that correspond when applicable to default values established in Telcordia GR-253-CORE.

Note All default or user-defined severity settings that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.

Step 7 Click **OK**.

The downloaded profile appears at the right side of the Alarm Profiles window.

Step 8 Right-click anywhere in the downloaded profile column to view the profile editing shortcut menu.

Step 9 Click **Store**.

Step 10 In the Store Profile(s) dialog box, click **To Node(s)**.

a. Choose the nodes where you want to save the profile:

- If you want to save the profile to only one node, click the node in the Node Names list.
- If you want to save the profile to all nodes, click **Select All**.
- If you do not want to save the profile to any nodes, click **Select None**.
- If you want to update alarm profile information, click (**Synchronize**).

b. **Click OK**.

Step 11 Return to your originating procedure (NTP).

DLP-A526 Change Line and Threshold Settings for the DS3i-N-12 Cards

Purpose	This task changes the line and threshold settings for the DS3i-N-12 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 In node view, double-click the DS3i-N-12 card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line**, **Line Thresholds**, **Elect Path Thresholds**, or **SONET Thresholds** subtab.

Note See Chapter 8, "Manage Alarms" for information about the Alarm Profiles tab.

Note If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Step 4 Modify the settings found under these subtabs by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

For definitions of the line settings, see Table 22-1. For definitions of the line threshold settings, see Table 22-2 on page 22-26. For definitions of the electrical path threshold settings, see Table 22-3 on page 22-27. For definitions of the SONET threshold settings, see Table 22-4 on page 22-27.

Table 22-1 describes the values on the Provisioning > Line tabs for the DS3i-N-12 cards.

Table 22-1 Line Options for the DS3i-N-12 Cards

Parameter	Description	Options
Port	(Display only) Port number.	1 to 12
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 20-8.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Line Type	Defines the line framing type.	• Unframed • M13 • C Bit • Auto Provisioned

Table 22-1 Line Options for the DS3i-N-12 Cards (continued)

Parameter	Description	Options
Detected Line Type	Displays the detected line type.	• M13 • C Bit • Unframed • Unknown
Line Coding	(Display only) Defines the DS3E transmission coding type.	B3ZS
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450
Admin State	Sets the port administrative service state unless network conditions prevent the change.	• IS—Puts the port in-service. The port service state changes to IS-NR. • IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. • OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. • OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT. **Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.

Table 22-1 Line Options for the DS3i-N-12 Cards (continued)

Parameter	Description	Options
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—(In-Service and Normal) The port is fully operational and performing as provisioned. • OOS-AU,AINS—(Out-Of-Service and Autonomous, Automatic In-Service) The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. • OOS-MA,DSBLD—(Out-of-Service and Management, Disabled) The port is out-of-service and unable to carry traffic. • OOS-MA,MT—(Out-of-Service and Management, Maintenance) The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments

Table 22-2 describes the parameters on the Provisioning > Line Thresholds tabs for the DS3i-N-12 cards.

Table 22-2 Line Threshold Options for the DS3i-N-12 Cards

Parameter	Description
Port	(Display only) Port number; 1 to 12
CV	Coding violations.
ES	Errored seconds
SES	Severely errored seconds
LOSS	Loss of signal seconds; number of one-second intervals containing one or more LOS defects
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 22-3 describes the parameters on the Provisioning > Elect Path Thresholds tabs for the DS3i-N-12 cards.

Table 22-3 Electrical Path Options for the DS3i-N-12 Cards

Parameter	Description
Port	(Display only) Port number; Port 1 to 12.
CVP	Coding violations - path. Available for DS3 Pbit, Near End only; and for DS3 CPbit, Near End and Far End.
ESP	Errored seconds - path. Available for DS3 Pbit, Near End only; and for DS3 CPbit, Near End and Far End.
SESP	Severely errored seconds - path. Available for DS3 Pbit, Near End only; and for DS3 CPbit, Near End and Far End.
SASP	Severely errored frame/alarm indication signal - path. Available for DS3 Pbit, Near End only; and for DS3 CPbit, Near End and Far End.
UASP	Unavailable seconds - path. Available for DS3 Pbit, Near End only; and for DS3 CPbit, Near End and Far End.
AISSP	Alarm indication signal seconds - path. Available for DS3 Pbit, Near End only; and for DS3 CPbit, Near End and Far End.
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 22-4 describes the values on the Provisioning > SONET Thresholds tabs for the DS3i-N-12 cards.

Table 22-4 SONET Threshold Options for DS3i-N-12 Cards

Parameter	Description
Port	(Display only) Port number; 1 to 12
CV	Coding violations
ES	Errored seconds
FC	Failure count
SES	Severely errored seconds
UAS	Unavailable seconds
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Note The threshold value appears after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-A527 Change the OC-N Card ALS Maintenance Settings

Purpose	This task changes the automatic laser shutdown (ALS) maintenance settings for the OC-N cards. This feature is available for OC3-8, OC-192, and MRC-12 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

Step 1 In node view, double-click the OC-N card where you want to change the ALS maintenance settings.

Step 2 Click the **Maintenance > ALS** tabs.

Step 3 Modify any of the settings described in Table 22-5 by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value or select or deselect a check box. The provisionable parameters are listed in the options column in the table.

Step 4 Click **Apply**. If the change affects traffic, a warning message displays. Click **Yes** to complete the change.

Table 22-5 OC-N Maintenance Settings

Parameter	Description	Options
Port number	(Display only) Port number	—
ALS Mode	Automatic laser shutdown mode. ALS provides the ability to shut down the TX laser when the RX detects a loss of signal (LOS).	From the drop-down list, choose one of the following: • Disable—Deactivates ALS. • Auto Restart—(Default) ALS is active. The power is automatically shut down when needed and automatically tries to restart using a probe pulse until the cause of the failure is repaired. • Manual Restart—failure is repaired. • Manual Restart—ALS is active. When conditions that caused the outage are resolved the laser must be manually restarted only if both ends are provisioned in Manual Restart mode. • Manual Restart for Test—Manually restarts the laser for testing.
Recovery Pulse Duration	Sets the recovery laser pulse duration, in seconds, for the initial, recovery optical power pulse following a laser shutdown.	Numeric. For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.
Recovery Pulse Interval	Sets the recovery laser pulse interval, in seconds. This is the period of time that must past before the recover pulse is repeated.	Numeric. For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.
Currently Shutdown	(Display only) Displays the current status of the laser.	Numeric. For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.
Request Laser Restart	If checked, allows you to restart the laser for maintenance. **Note** Restarting a laser might be traffic-affecting.	Checked or unchecked

Step 5 Return to your originating procedure (NTP).

DLP-A528 Change the Default Network View Background Map

Purpose	This task changes the default map of the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note If you modify the background image, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

Step 1 From the Edit menu, choose **Preferences > Map** and check the **Use Default Map** check box.

Step 2 In the node view, click the **Provisioning > Defaults** tabs.

Step 3 In the Defaults Selector area, choose **CTC** and then **network**.

Step 4 Click the **Default Value** field and choose a default map from the drop-down list. Map choices are: Germany, Japan, Netherlands, South Korea, United Kingdom, and the United States (default).

Step 5 Click **Apply**. The new network map appears.

Step 6 Click **OK**.

Step 7 If the ONS 15454 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until all the ONS 15454 icons are visible. (You can also choose **Fit Graph to Window**.)

Step 8 If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.

Step 9 If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15454 icons are displayed at the magnification you want.

Step 10 Return to your originating procedure (NTP).

DLP-A529 Delete Ethernet RMON Alarm Thresholds

Purpose	This task deletes remote monitoring (RMON) threshold crossing alarms for Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A533 Create Ethernet RMON Alarm Thresholds, page 22-36 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The ONS 15454 ML-Series cards use the Cisco IOS command line interface (CLI) to manage RMON.

Step 1 Double-click the Ethernet card where you want to delete the RMON alarm thresholds.

Step 2 In card view, click the **Provisioning > Ether Ports > RMON Thresholds** tabs.

Note For the CE-Series, click the **Provisioning > Ether Ports > RMON Thresholds** tabs or **Provisioning > POS Ports > RMON Thresholds** tabs.

Step 3 Click the RMON alarm threshold you want to delete.

Step 4 Click **Delete**. The Delete Threshold dialog box appears.

Step 5 Click **Yes** to delete the threshold.

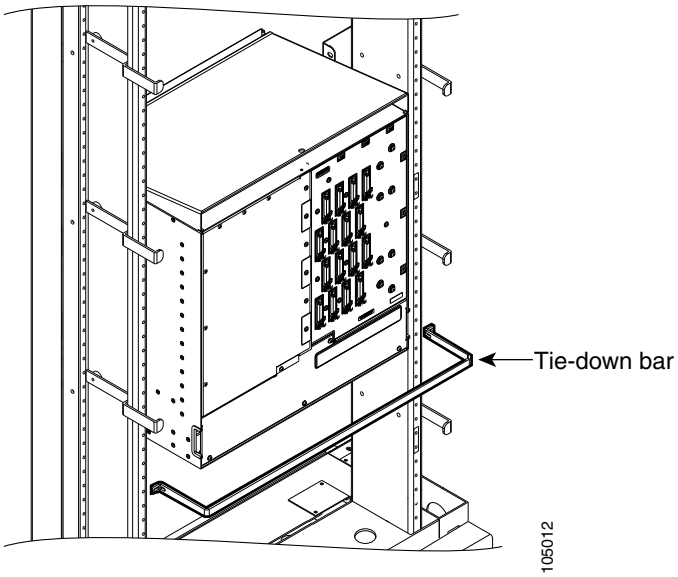
Step 6 Return to your originating procedure (NTP).

DLP-A530 Install the Tie-Down Bar

Purpose	This task installs the tie-down bar used to secure cabling on the rear of the ONS 15454. The tie-down bar can be used to provide a diverse path for redundant power feeds and cables.
Tools/Equipment	Tie-down bar Screws (4)
Prerequisite Procedures	DLP-A5 Mount the Shelf Assembly in a Rack (One Person), page 17-5 DLP-A6 Mount the Shelf Assembly in a Rack (Two People), page 17-6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Align the ends of the tie-down bar with the four screw holes located 1 RU below the ONS 15454. Figure 22-8 shows the tie-down bar, the ONS 15454, and the rack.

Figure 22-8 Tie-Down Bar



Step 2 Install the four screws into the rack.

Step 3 Return to your originating procedure (NTP).

DLP-A531 Print CTC Data

Purpose	This task prints CTC card, node, or network data in graphical or tabular format on a Windows-provisioned printer.
Tools/Equipment	Printer connected to the CTC computer by a direct or network connection
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Click the tab (and subtab, if present) containing the information you want to print. For example, click the **Alarms** tab to print Alarms window data.

The print operation is available for all network, node, and card view windows.

Step 2 From the File menu choose **Print**.

Step 3 In the Print dialog box, click a printing option (Figure 22-9).

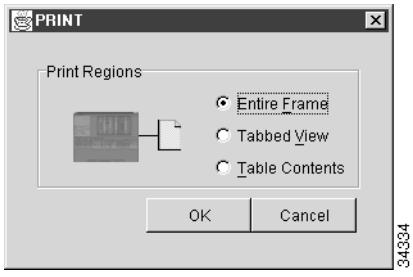
- Entire Frame—Prints the entire CTC window including the graphical view of the card, node, or network. This option is available for all windows.

- Tabbed View—Prints the lower half of the CTC window containing tabs and data. The printout includes the selected tab (on top) and the data shown in the tab window. For example, if you print the History window Tabbed View, you print only history items appearing in the window. This option is available for all windows.
- Table Contents—Prints CTC data in table format without graphical representations of shelves, cards, or tabs. This option does not apply to the following windows:
  - Provisioning > General tab (General, Power Monitor, and Multishelf Config) windows
  - Provisioning > Network > General window
  - Provisioning > Security > Policy, Access, and Legal Disclaimer windows
  - Provisioning > SNMP window
  - Provisioning > Timing > General and BITS Facilities windows
  - Provisioning > Cross-Connect window
  - Provisioning > OSI > Main Setup window and OSI > TARP > Config window
  - Provisioning > Comm Channels > LMP > General window
  - Provisioning > WDM-ANS > Node Setup window
  - Maintenance > Cross-Connect > Cards window
  - Maintenance > Database window
  - Maintenance > Diagnostic window
  - Maintenance > Protection window
  - Maintenance > Timing > Source window
  - Maintenance > DWDM > ROADM Power Monitoring window

  The Table Contents option prints all the data contained in a table and the table column headings. For example, if you print the History window Table Contents view, you print all data included in the table whether or not items appear in the window.

Tip When you print using the Tabbed View option, it can be difficult to distinguish whether the printout applies to the network, node, or card view. To determine the view, compare the tabs on the printout. The network, node, and card views are identical except that network view does not contain an Inventory tab or Performance tab.

Figure 22-9 Selecting CTC Data For Print



Step 4 Click **OK**.

Step 5 In the Windows Print dialog box, click a printer and click **OK**.

Step 6 Repeat this task for each window that you want to print.

Step 7 Return to your originating procedure (NTP).

DLP-A532 Export CTC Data

Purpose	This task exports CTC table data as delineated text to view or edit the data in text editor, word processor, spreadsheet, database management, or web browser applications. You can also export data from the Edit Circuits window.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Click the tab containing the information you want to export (for example, the Alarms tab or the Circuits tab).

Step 2 If you want to export detailed circuit information, complete the following:

a. In the Circuits window, choose a circuit and click **Edit** to open it in the Edit Circuits window.

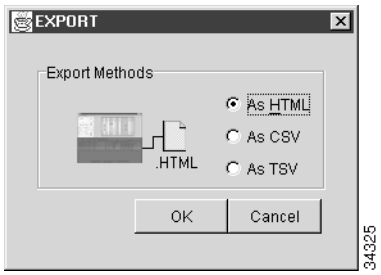
b. In the Edit Circuits window, choose the desired tab: Drops, Path Protection Selectors, Path Protection Switch Counts, State, or Merge. (Depending on your configuration, you may or may not see all of these tabs.)

Step 3 From the File menu, choose **Export**.

Step 4 In the Export dialog box, click a data format (Figure 22-10):

- **As HTML**—Saves data as a simple HTML table file without graphics. The file must be viewed or edited with applications such as Netscape Navigator, Microsoft Internet Explorer, or other applications capable of opening HTML files.
- **As CSV**—Saves the CTC table as comma-separated values (CSV). This option does not apply to the Maintenance > Timing > Report window.
- **As TSV**—Saves the CTC table as tab-separated values (TSV).

Figure 22-10 Selecting CTC Data For Export



Step 5 If you want to open a file in a text editor or word processor application, procedures vary. Typically, you can use the File > Open command to view the CTC data, or you can double-click the file name and choose an application such as Notepad.

Text editor and word processor applications format the data exactly as it is exported, including comma or tab separators. All applications that open the data files allow you to format the data.

Step 6 If you want to open the file in spreadsheet and database management applications, procedures vary. Typically, you need to open the application and choose File > Import, then choose a delimited file to format the data in cells.

Spreadsheet and database management programs also allow you to manage the exported data.

Note An exported file cannot be opened in CTC.

The export operation does not apply to the following windows:

- Provisioning > General > General, Power Monitor, and Multishelf Config window
- Provisioning > Network > General window
- Provisioning > Security > Policy, Access, and Legal Disclaimer window
- Provisioning > SNMP window
- Provisioning > Timing > General and BITS FAcilities windows
- Provisioning > OSI > Main Setup window and OSI > TARP > Config window
- Provisioning > Comm Channels > LMP > General window
- Provisioning > Cross-Connect window
- Provisioning > WDM-ANS > Node Setup window
- Maintenance > Cross-Connect > Cards window
- Maintenance > Database window
- Maintenance > Diagnostic window
- Maintenance > Protection window
- Maintenance > Timing > Source window
- Maintenance > DWDM > ROADM Power Monitoring window

Step 7 Click **OK**.

Step 8 In the Save dialog box, enter a name in the File name field using one of the following formats:

- *filename*.html for HTML files
- *filename*.csv for CSV files
- *filename*.tsv for TSV files

Step 9 Navigate to a directory where you want to store the file.

Step 10 Click **OK**.

Step 11 Repeat the task for each window that you want to export.

Step 12 Return to your originating procedure (NTP).

DLP-A533 Create Ethernet RMON Alarm Thresholds

Purpose	This procedure sets up remote monitoring (RMON) to allow network management systems to monitor Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The ONS 15454 ML-Series cards use the Cisco IOS CLI to manage RMON.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to set up RMON. If you are already logged in, continue with Step 2.

Step 2 Double-click the Ethernet card where you want to create the RMON alarm thresholds.

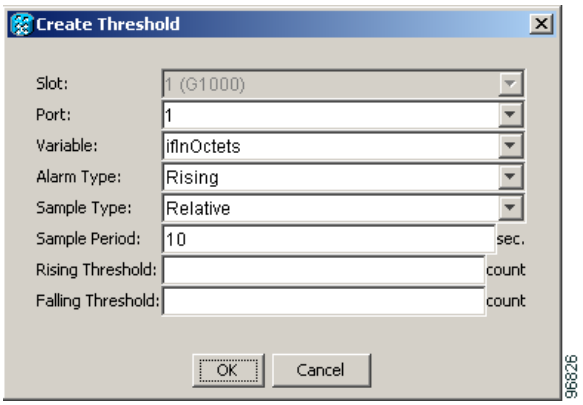
Step 3 In card view, click the **Provisioning > RMON Thresholds** tabs.

Note For CE- and ML-Series Ethernet cards, click the **Provisioning > Ether Ports > RMON Thresholds** tabs or **Provisioning > POS Ports > RMON Thresholds** tabs.

Step 4 Click **Create**.

The Create Ether Threshold dialog box appears (Figure 22-11).

Figure 22-11 Creating RMON Thresholds



Step 5 From the Port drop-down list, choose the applicable port on the Ethernet card you selected.

Step 6 From the Variable drop-down list, choose the variable. See Table 22-6 and Table 22-7 for a list of the Ethernet and POS threshold variables available in this field.

Table 22-6 Ethernet Threshold Variables (MIBs)

Variable	Definition
iflnOctets	Total number of octets received on the interface, including framing octets
iflnUcastPkts	Total number of unicast packets delivered to an appropriate protocol
ifInMulticastPkts	(G-Series, CE-Series, and ML-Series only) Number of multicast frames received error free
ifInBroadcastPkts	(G-Series, CE-Series, and ML-Series only) The number of packets, delivered by this sublayer to a higher (sub)layer, that were addressed to a broadcast address at this sublayer
ifInDiscards	(G-Series, CE-Series, and ML-Series only) The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol
iflnErrors	Number of inbound packets discarded because they contain errors
ifOutOctets	Total number of transmitted octets, including framing packets
ifOutUcastPkts	Total number of unicast packets requested to transmit to a single address
ifOutMulticastPkts	(G-Series, CE-Series, and ML-Series only) Number of multicast frames transmitted error free
ifOutBroadcastPkts	(G-Series, CE-Series, and ML-Series only) The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this sublayer, including those that were discarded or not sent
ifOutDiscards	(G-Series only) The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted
dot3statsAlignmentErrors	Number of frames with an alignment error, that is, the length is not an integral number of octets and the frame cannot pass the frame check sequence (FCS) test
dot3StatsFCSErrors	Number of frames with framecheck errors, that is, there is an integral number of octets, but an incorrect FCS
dot3StatsSingleCollisionFrames	(Not supported by E-Series or G-Series) Number of successfully transmitted frames that had exactly one collision
dot3StatsMutlipleCollisionFrames	(Not supported by E-Series or G-Series) Number of successfully transmitted frames that had multiple collisions
dot3StatsDeferredTransmissions	(Not supported by E-Series or G-Series) Number of times the first transmission was delayed because the medium was busy
dot3StatsLateCollisions	(Not supported by E-Series or G-Series) Number of times that a collision was detected later than 64 octets into the transmission (also added into collision count)

Table 22-6 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
dot3StatsExcessiveCollisions	(Not supported by E-Series or G-Series) Number of frames where transmissions failed because of excessive collisions
dot3StatsCarrierSenseErrors	(G-Series only) The number of transmission errors on a particular interface that are not otherwise counted
dot3StatsSQETestErrors	(G-Series only) A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address; this does not include multicast packets
etherStatsCollisions	An estimate of the total number of collisions on this Ethernet segment. The value returned depends on the location of the RMON probe. Section 8.2.1.3 (10Base5) and Section 10.3.1.3 (10Base2) of the IEEE 802.3 standard state that a station must detect a collision, in the receive mode, if three or more stations are transmitting simultaneously. A repeater port must detect a collision when two or more stations are transmitting simultaneously. Thus, a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment. Probe location plays a much smaller role when considering 10BaseT. Section 14.2.1.4 (10BaseT) of the IEEE 802.3 standard defines a collision as the simultaneous presence of signals on the DO and RD circuits (transmitting and receiving at the same time). A 10BaseT station can only detect collisions when it is transmitting. Thus, probes placed on a station and a repeater should report the same number of collisions. An RMON probe inside a repeater should report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.

Table 22-6 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
etherStatsCollisionFrames	An estimate of the total number of collisions on this Ethernet segment. The value returned will depend on the location of the RMON probe. Section 8.2.1.3 (10Base5) and Section 10.3.1.3 (10Base2) of the IEEE 802.3 standard state that a station must detect a collision, in the receive mode, if three or more stations are transmitting simultaneously. A repeater port must detect a collision when two or more stations are transmitting simultaneously. Thus, a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment. Probe location plays a much smaller role when considering 10BaseT. Section 14.2.1.4 (10BASE-T) of the IEEE 802.3 standard defines a collision as the simultaneous presence of signals on the DO and RD circuits (transmitting and receiving at the same time). A 10BaseT station can only detect collisions when it is transmitting. Thus, probes placed on a station and a repeater, should report the same number of collisions. An RMON probe inside a repeater should report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.
etherStatsDropEvents	The total number of events in which packets were dropped by the probe due to lack of resources. This number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.
etherStatsJabbers	Total number of octets of data (including bad packets) received on the network
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast.
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
etherStatsUndersizePkts	Number of packets received with a length less than 64 octets
etherStatsFragments	Total number of packets that are not an integral number of octets or have a bad FCS, and that are less than 64 octets long
etherStatsPkts64Octets	Total number of packets received (including error packets) that were 64 octets in length
etherStatsPkts65to127Octets	Total number of packets received (including error packets) that were 65 to 172 octets in length
etherStatsPkts128to255Octets	Total number of packets received (including error packets) that were 128 to 255 octets in length
etherStatsPkts256to511Octets	Total number of packets received (including error packets) that were 256 to 511 octets in length

Table 22-6 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
etherStatsPkts512to1023Octets	Total number of packets received (including error packets) that were 512 to 1023 octets in length
etherStatsPkts1024to1518Octets	Total number of packets received (including error packets) that were 1024 to 1518 octets in length
etherStatsJabbers	Total number of packets longer than 1518 octets that were not an integral number of octets or had a bad FCS
etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets
etherStatsCollisions	Best estimate of the total number of collisions on this segment
etherStatsCollisionFrames	Best estimate of the total number of frame collisions on this segment
etherStatsCRCAlignErrors	Total number of packets with a length between 64 and 1518 octets, inclusive, that had a bad FCS or were not an integral number of octets in length
receivePauseFrames	(G-Series only) The number of received IEEE 802.x pause frames
transmitPauseFrames	(G-Series only) The number of transmitted IEEE 802.x pause frames
receivePktsDroppedInternalCongestion	(G-Series only) The number of received framed dropped due to frame buffer overflow as well as other reasons
transmitPktsDroppedInternalCongestion	(G-Series only) The number of frames dropped in the transmit direction due to frame buffer overflow as well as other reasons
txTotalPkts	Total number of transmit packets
rxTotalPkts	Total number of receive packets
mediaIndStatsOversizeDropped	Number of received packets larger than the CE-100T-8 remote monitoring (RMON) threshold.
mediaIndStatsTxFramesTooLong	Number of packets transmitted that are greater than 1548

Table 22-7 POS Threshold Variables (MIBs)

Variable	Definition
ifInPayloadCrcErrors	Number of CRC errors in the frame inside the GFP/HDLC payload coming in from the SONET receive (RX) direction.
ifOutPayloadCrcErrors	Number of CRC errors in the frame inside the GFP/HDLC payload coming in from the SONET transmit (TX) direction
ifOutOversizePkts	Number of packets larger than 1518 bytes sent out into SONET. Packets larger than 1600 bytes do not get transmitted.
etherStatsDropEvents	Number of received frames dropped at the port level.
gfpStatsRxSBitErrors	Receive frames with Single Bit Errors (cHEC, tHEC, eHEC)
gfpStatsRxMBitErrors	Receive frames with Multi Bit Errors (cHEC, tHEC, eHEC)

Table 22-7 POS Threshold Variables (MIBs) (continued)

Variable	Definition
gfpStatsRxTypeInvalid	Receive frames with invalid type (PTI, EXI, UPI)
gfpStatsRxCRCErrors	Receive data frames with Payload cyclic redundancy check (CRC) errors
gfpStatsRxCIDInvalid	Receive frames with Invalid CID
gfpStatsCSFRaised	Number of receive (Rx) client management frames with Client Signal Fail indication.
gfpStatsRxFrame	Receive data frames
gfpStatsTxFrame	Transmit data frames
gfpStatsRxOctets	Received data Octets
gfpStatsTxOctets	Transmit data Octets

Step 7 From the Alarm Type drop-down list, indicate whether the event will be triggered by the rising threshold, falling threshold, or both the rising and falling thresholds.

Step 8 From the Sample Type drop-down list, choose either **Relative** or **Absolute**. Relative restricts the threshold to use the number of occurrences in the user-set sample period. Absolute sets the threshold to use the total number of occurrences, regardless of time period.

Step 9 Type in an appropriate number of seconds for the Sample Period.

Step 10 Type in the appropriate number of occurrences for the Rising Threshold.

For a rising type of alarm, the measured value must move from below the falling threshold to above the rising threshold. For example, if a network is running below a rising threshold of 1000 collisions every 15 seconds and a problem causes 1001 collisions in 15 seconds, the excess occurrences trigger an alarm.

Step 11 Enter the appropriate number of occurrences in the Falling Threshold field. In most cases a falling threshold is set lower than the rising threshold.

A falling threshold is the counterpart to a rising threshold. When the number of occurrences is above the rising threshold and then drops below a falling threshold, it resets the rising threshold. For example, when the network problem that caused 1001 collisions in 15 minutes subsides and creates only 799 collisions in 15 minutes, occurrences fall below a falling threshold of 800 collisions. This resets the rising threshold so that if network collisions again spike over a 1000 per 15-minute period, an event again triggers when the rising threshold is crossed. An event is triggered only the first time a rising threshold is exceeded (otherwise, a single network problem might cause a rising threshold to be exceeded multiple times and cause a flood of events).

Step 12 Click **OK** to complete the procedure.

Step 13 Return to your originating procedure (NTP).

DLP-A534 Provision OSI Routing Mode

Purpose	This task provisions the Open System Interconnection (OSI) routing mode. Complete this task when the ONS 15454 is connected to networks with third party network elements (NEs) that use the OSI protocol stack for data communications network (DCN) communication.
Tools/Equipment	None
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Do not complete this task until you confirm the role of the node within the network. It will be either an ES, IS Level 1, or IS Level 1/Level 2. This decision must be carefully considered. For additional information about OSI provisioning, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15454 Reference Manual*.

Caution Link State Protocol (LSP) buffers must be the same at all NEs within the network, or loss of visibility might occur. Do not modify the LSP buffers unless you confirm that all NEs within the OSI have the same buffer size.

Caution LSP buffer sizes cannot be greater than the LAP-D maximum transmission unit (MTU) size within the OSI area.

Note For ONS 15454 nodes, three virtual routers can be provisioned. The node primary NSAP address is also the Router 1 primary manual area address. To edit the primary NSAP, you must edit the Router 1 primary manual area address. After you enable Router 1 on the Routers subtab, the Change Primary Area Address button is available to edit the address.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you want to provision the OSI routing mode. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Provisioning > OSI > Main Setup** tabs.

Step 3 Choose a routing mode:

- End System—The ONS 15454 performs OSI end system (ES) functions and relies upon an intermediate system (IS) for communication with nodes that reside within its OSI area.

  Note The End System routing mode is not available if more than one virtual router is enabled.

- Intermediate System Level 1—The ONS 15454 performs OSI IS functions. It communicates with IS and ES nodes that reside within its OSI area. It depends upon an IS L1/L2 node to communicate with IS and ES nodes that reside outside its OSI area.

- Intermediate System Level 1/Level 2—The ONS 15454 performs IS functions. It communicates with IS and ES nodes that reside within its OSI area. It also communicates with IS L1/L2 nodes that reside in other OSI areas. Before choosing this option, verify the following:
  - The node is connected to another IS Level 1/Level 2 node that resides in a different OSI area.
  - The node is connected to all nodes within its area that are provisioned as IS L1/L2.

Step 4 If needed, change the LSP data buffers:

- L1 LSP Buffer Size—Adjusts the Level 1 link state PDU buffer size. The default is 512. It should not be changed.
- L2 LSP Buffer Size—Adjusts the Level 2 link state PDU buffer size. The default is 512. It should not be changed.

Step 5 Return to your originating procedure (NTP).

DLP-A535 Provision or Modify TARP Operating Parameters

Purpose	This task provisions or modifies the Target Identifier Address Resolution Protocol (TARP) operating parameters including TARP protocol data unit (PDU) propagation, timers, and loop detection buffer (LDB).
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning > OSI > TARP > Config** tabs.

Step 2 Provision the following parameters, as needed:

- TARP PDUs L1 Propagation—If checked (default), TARP Type 1 PDUs that are received by the node and are not excluded by the LDB are propagated to other NEs within the Level 1 OSI area. (Type 1 PDUs request a protocol address that matches a target identifier [TID] within a Level 1 routing area.) The propagation does not occur if the NE is the target of the Type 1 PDU, and PDUs are not propagated to the NE from which the PDU was received.

Note The TARP PDUs L1 Propagation parameter is not used when the Node Routing Area (Provisioning > OSI > Main Setup tab) is set to End System.

- TARP PDUs L2 Propagation—If checked (default), TARP Type 2 PDUs received by the node that are not excluded by the LDB are propagated to other NEs within the Level 2 OSI areas. (Type 2 PDUs request a protocol address that matches a TID within a Level 2 routing area.) The propagation occurs if the NE is not the target of the Type 2 PDU, and PDUs are not propagated to the NE from which the PDU was received.

Note The TARP PDUs L2 Propagation parameter is only used when the Node Routing Area is provisioned to Intermediate System Level 1/Level 2.

- TARP PDUs Origination—If checked (default), the node performs all TARP origination functions including:
  - TID to Network Service Access Point (NSAP) resolution requests (originate TARP Type 1 and Type 2 PDUs)
  - NSAP to TID requests (originate Type 5 PDUs)
  - TARP address changes (originate Type 4 PDUs)

Note TARP Echo and NSAP to TID is not supported.

- TARP Data Cache—If checked (default), the node maintains a TARP data cache (TDC). The TDC is a database of TID to NSAP pairs created from TARP Type 3 PDUs received by the node and modified by TARP Type 4 PDUs (TID to NSAP updates or corrections). TARP 3 PDUs are responses to Type 1 and Type 2 PDUs. The TDC can also be populated with static entries entered on the TARP > Static TDC tab.

Note This parameter is only used when the TARP PDUs Origination parameter is enabled.

- L2 TARP Data Cache—If checked (default), the TIDs and NSAPs of NEs originating Type 2 requests are added to the TDC before the node propagates the requests to other NEs.

The TARP Data Cache parameter is designed for Intermediate System Level 1/Level 2 nodes that are connected to other Intermediate System Level 1/Level 2 nodes. Enabling the parameter for Intermediate System Level 1 nodes is not recommended.

- LDB—If checked (default), enables the TARP loop detection buffer. The LDB prevents TARP PDUs from being sent more than once on the same subnet.

The LDP parameter is not used if the Node Routing Mode is provisioned to End System or if the TARP PDUs L1 Propagation parameter is not enabled.

- LAN TARP Storm Suppression—If checked (default), enables TARP storm suppression. This function prevents redundant TARP PDUs from being unnecessarily propagated across the LAN network.
- Send Type 4 PDU on Startup—If checked, a TARP Type 4 PDU is originated during the initial ONS 15454 startup. Type 4 PDUs indicate that a TID or NSAP change has occurred at the NE. (The default setting is not enabled.)
- Type 4 PDU Delay—Sets the amount of time that will pass before the Type 4 PDU is generated when Send Type 4 PDU on Startup is enabled. 60 seconds is the default. The range is 0 to 255 seconds.

Note The Send Type 4 PDU on Startup and Type 4 PDU Delay parameters are not used if TARP PDUs Origination is not enabled.

- LDB Entry—Sets the TARP loop detection buffer timer. The LDB buffer time is assigned to each LDB entry for which the TARP sequence number (tar-seq) is zero. The default is 5 minutes. The range is 1 to 10 minutes.
- LDB Flush—Sets the frequency period for flushing the LDB. The default is 5 minutes. The range is 0 to 1440 minutes.
- T1—Sets the amount of time to wait for a response to a Type 1 PDU. Type 1 PDUs seek a specific NE TID within an OSI Level 1 area. The default is 15 seconds. The range is 0 to 3600 seconds.

- T2—Sets the amount of time to wait for a response to a Type 2 PDU. TARP Type 2 PDUs seek a specific NE TID value within OSI Level 1 and Level 2 areas. The default is 25 seconds. The range is 0 to 3600 seconds.
- T3—Sets the amount of time to wait for an address resolution request. The default is 40 seconds. The range is 0 to 3600 seconds.
- T4—Sets the amount of time to wait for an error recovery. This timer begins after the T2 timer expires without finding the requested NE TID. The default is 20 seconds. The range is 0 to 3600 seconds.

Note The T1, T2, and T4 timers are not used if TARP PDUs Origination is not enabled.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-A536 Add a Static TID to NSAP Entry to the TARP Data Cache

Purpose	This task adds a static TID to NSAP entry to the TDC. The static entries are required for NEs that do not support TARP and are similar to static routes. For a specific TID, you must force a specific NSAP.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioner or higher

Step 1 In node view, click the **Provisioning > OSI > TARP > Static TDC** tabs.

Step 2 Click **Add Static Entry**.

Step 3 In the Add Static Entry dialog box, enter the following:

- TID—Enter the TID of the NE. (For ONS nodes, the TID is the Node Name parameter on the node view Provisioning > General tab.)
- NSAP—Enter the OSI NSAP address in the NSAP field or, if preferred, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box.

Step 4 Click **OK** to close the Masked NSAP Entry dialog box, if used, and then click **OK** to close the Add Static Entry dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-A537 Remove a Static TID to NSAP Entry from the TARP Data Cache

Purpose	This task removes a static TID to NSAP entry from the TDC.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioner or higher

Step 1 In node view, click the **Provisioning > OSI > TARP > Static TDC** tabs.

Step 2 Click the static entry that you want to delete.

Step 3 Click **Delete Static Entry**.

Step 4 In the Delete TDC Entry dialog box, click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-A538 Add a TARP Manual Adjacency Table Entry

Purpose	This task adds an entry to the TARP manual adjacency table (MAT). Entries are added to the MAT when the ONS 15454 must communicate across routers or non-SONET NEs that lack TARP capability.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, click the **Provisioning > OSI > TARP > MAT** tabs.

Step 2 Click **Add**.

Step 3 In the Add TARP Manual Adjacency Table Entry dialog box, enter the following:

- Level—Sets the TARP Type Code that will be sent:
  - **Level 1**—Indicates that the adjacency is within the same area as the current node. The entry generates Type 1 PDUs.
  - **Level 2**—Indicates that the adjacency is in a different area than the current node. The entry generates Type 2 PDUs.
- NSAP—Enter the OSI NSAP address in the NSAP field or, if preferred, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box.

Step 4 Click **OK** to close the Masked NSAP Entry dialog box, if used, and then click **OK** to close the Add Static Entry dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-A539 Provision OSI Routers

Purpose	This task enables an OSI router and edits its primary manual area address.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Router 1 must be enabled before you can enable and edit the primary manual area addresses for Routers 2 and 3.

Note The Router 1 manual area address, System ID, and Selector "00" create the node NSAP address. Changing the Router 1 manual area address changes the node's NSAP address.

Note The System ID for Router 1 is the node MAC address. The System IDs for Routers 2 and 3 are created by adding 1 and 2 respectively to the Router 1 System ID. You cannot edit the System IDs.

Step 1 In node view, click the **Provisioning > OSI > Routers > Setup** tabs.

Step 2 Chose the router you want provision and click **Edit**. The OSI Router Editor dialog box appears.

Step 3 In the OSI Router Editor dialog box:

a. Check **Enable Router** to enable the router and make its primary area address available for editing.

b. Click the manual area address, then click **Edit**.

c. In the Edit Manual Area Address dialog box, edit the primary area address in the Area Address field. If you prefer, click **Use Mask** and enter the edits in the Masked NSAP Entry dialog box. The address (hexadecimal format) can be 8 to 24 alphanumeric characters (0–9, a–f) in length.

d. Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Edit Manual Area Address, and OSI Router Editor.

Step 4 Return to your originating procedure (NTP).

DLP-A540 Provision Additional Manual Area Addresses

Purpose	This task provisions the OSI manual area addresses. One primary and two additional manual areas can be created for each virtual router.
Tools/Equipment	None
Prerequisite Procedures	DLP-A539 Provision OSI Routers, page 22-47 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > OSI > Routers > Setup** tabs.

Step 2 Chose the router where you want provision an additional manual area address and click **Edit**. The OSI Router Editor dialog box.

Step 3 In the OSI Router Editor dialog box:

a. Check **Enable Router** to enable the router and make its primary area address available for editing.

b. Click the manual area address, then click **Add**.

c. In the Add Manual Area Address dialog box, enter the primary area address in the Area Address field. If you prefer, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box. The address (hexadecimal format) can be 2 to 24 alphanumeric characters (0–9, a–f) in length.

d. Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Add Manual Area Address, and OSI Router Editor.

Step 4 Return to your originating procedure (NTP).

DLP-A541 Enable the OSI Subnet on the LAN Interface

Purpose	This task enables the OSI subnetwork point of attachment on the LAN interface.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note OSI subnetwork points of attachment are enabled on DCCs when you create DCCs. See the "DLP-A377 Provision Section DCC Terminations" task on page 20-69 and the "DLP-A378 Provision Line DCC Terminations" task on page 20-71.

Note The OSI subnetwork point of attachment cannot be enabled for the LAN interface if the OSI routing mode is set to ES (end system).

Note If Secure Mode is on, the OSI Subnet is enabled on the backplane LAN port, not the front TCC2P port.

Step 1 In node view, click the **Provisioning > OSI > Routers > Subnet** tabs.

Step 2 Click **Enable LAN Subnet**.

Step 3 In the Enable LAN Subnet dialog box, complete the following fields:

- ESH—Sets the End System Hello (ESH) propagation frequency. End system NEs transmit ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- ISH—Sets the Intermediate System Hello PDU propagation frequency. Intermediate system NEs send ISHs to other ESs and ISs to inform them about the IS NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- IIH—Sets the Intermediate System to Intermediate System Hello PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
- IS-IS Cost—Sets the cost for sending packets on the LAN subnet. The IS-IS protocol uses the cost to calculate the shortest routing path. The default IS-IS cost for LAN subnets is 20. It normally should not be changed.
- DIS Priority—Sets the designated intermediate system (DIS) priority. In IS-IS networks, one router is elected to serve as the DIS (LAN subnets only). Cisco router DIS priority is 64. For the ONS 15454 LAN subnet, the default DIS priority is 63. It normally should not be changed.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-A542 Create an IP-Over-CLNS Tunnel

Purpose	This task creates an IP-over-CLNS tunnel to allow ONS 15454s to communicate across equipment and networks that use the OSI protocol stack.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution IP-over-CLNS tunnels require two end points. You will create one point on an ONS 15454. The other end point is generally provisioned on non-ONS equipment including routers and other network elements (NE). Before you begin, verify that you have the capability to create an OSI over IP tunnel on the other equipment location.

Step 1 In node view, click the **Provisioning > OSI > Tunnels** tabs.

Step 2 Click **Create**.

Step 3 In the Create IP Over OSI Tunnel dialog box, complete the following fields:

- Tunnel Type—Choose a tunnel type:
  - Cisco—Creates the proprietary Cisco IP tunnel. Cisco IP tunnels add the CLNS header to the IP packets.
  - GRE—Creates a Generic Routing Encapsulation tunnel. GRE tunnels add the CLNS header and a GRE header to the IP packets.

  The Cisco proprietary tunnel is slightly more efficient than the GRE tunnel because it does not add the GRE header to each IP packet. The two tunnel types are not compatible. Most Cisco routers support the Cisco IP tunnel, while only a few support both GRE and Cisco IP tunnels. You generally should create Cisco IP tunnels if you are tunneling between two Cisco routers or between a Cisco router and an ONS node.

Caution Always verify that the IP-over-CLNS tunnel type you choose is supported by the equipment at the other end of the tunnel.

- IP Address—Enter the IP address of the IP-over-CLNS tunnel destination.
- IP Mask—Enter the IP address subnet mask of the IP-over-CLNS destination.
- OSPF Metric—Enter the Open Shortest Path First (OSPF) metric for sending packets across the IP-over-CLNS tunnel. The OSPF metric, or cost, is used by OSPF routers to calculate the shortest path. The default is 110. Normally, it is not be changed unless you are creating multiple tunnel routes and want to prioritize routing by assigning different metrics.
- NSAP Address—Enter the destination NE or OSI router NSAP address.

Step 4 Click **OK**.

Step 5 Provision the other tunnel end point using the documentation.

Step 6 Return to your originating procedure (NTP).

DLP-A543 Remove a TARP Manual Adjacency Table Entry

Purpose	This task removes an entry from the TARP manual adjacency table.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution If TARP manual adjacency is the only means of communication to a group of nodes, loss of visibility will occur when the adjacency table entry is removed.

Step 1 In node view, click the **Provisioning > OSI > TARP > MAT** tabs.

Step 2 Click the MAT entry that you want to delete.

Step 3 Click **Remove**.

Step 4 In the Delete TDC Entry dialog box, click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-A544 Change the OSI Routing Mode

Purpose	This task changes the OSI routing mode.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Do not complete this procedure until you confirm the role of the node within the network. It will be either an ES, IS Level 1, or IS Level 1/Level 2. This decision must be carefully considered. For additional information about OSI provisioning, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15454 Reference Manual*.

Caution LSP buffers must be the same at all NEs within the network, or loss of visibility could occur. Do not modify the LSP buffers unless you are sure that all NEs within the OSI have the same buffer size.

Caution LSP buffer sizes cannot be greater than the LAP-D MTU size within the OSI area.

Step 1 Verify the following:

- All L1/L2 virtual routers on the NE must reside in the same area. This means that all neighboring virtual routers must have at least one common area address.
- For OSI L1/L2 to ES routing mode changes, only one L1/L2 virtual router and no more than one subnet can be configured.
- For OSI L1 to ES routing mode changes, only one L1 virtual router and no more than one subnet can be configured.

Step 2 In node view, click the **Provisioning > OSI** tabs.

Step 3 Choose one of the following routing modes:

- **End System**—The ONS 15454 performs OSI IS functions. It communicates with IS and ES nodes that reside within its OSI area. It depends upon an IS L1/L2 node to communicate with IS and ES nodes that reside outside its OSI area.
- **Intermediate System Level 1/Level 2**—The ONS 15454 performs IS functions. It communicates with IS and ES nodes that reside within its OSI area. It also communicates with IS L1/L2 nodes that reside in other OSI areas. Before choosing this option, verify the following:
  - The node is connected to another IS Level 1/Level 2 node that resides in a different OSI area.
  - The node is connected to all nodes within its area that are provisioned as IS L1/L2.

Note Changing a routing mode should be carefully considered. Additional information about OSI ESs and ISs and the ES-IS and IS-IS protocols are provided in the "Management Network Connectivity" chapter of the *Cisco ONS 15454 Reference Manual*.

Step 4 Although Cisco does not recommend changing the LSP (Link State Protocol Data Unit) buffer sizes, you can adjust the buffers in the following fields:

- L1 LSP Buffer Size—Adjusts the Level 1 link state PDU buffer size.
- L2 LSP Buffer Size—Adjusts the Level 2 link state PDU buffer size.

Step 5 Return to your originating procedure (NTP).

DLP-A545 Edit the OSI Router Configuration

Purpose	This task allows you to edit the OSI router configuration, including enabling and disabling OSI routers, editing the primary area address, and creating or editing additional area addresses.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > OSI > Routers > Setup** tabs.

Step 2 Chose the router you want provision and click **Edit**.

Step 3 In the OSI Router Editor dialog box:

a. Check or uncheck the Enabled box to enable or disable the router.

Note Router 1 must be enabled before you can enable Routers 2 and 3.

b. For enabled routers, edit the primary area address, if needed. The address can be between 8 and 24 alphanumeric characters in length.

c. If you want to add or edit an area address to the primary area, enter the address at the bottom of the Multiple Area Addresses area. The area address can be 2 to 26 numeric characters (0–9) in length. Click **Add**.

d. Click **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-A546 Edit the OSI Subnetwork Point of Attachment

Purpose	This task allows you to view and edit the OSI subnetwork point of attachment parameters. The parameters are initially provisioned when you create a Section DCC (SDCC), Line DCC (LDCC), generic communications channel (GCC), or optical service channel (OSC), or when you enable the LAN subnet.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > OSI > Routers > Subnet** tabs.

Step 2 Choose the subnet you want to edit, then click **Edit**.

Step 3 In the Edit <*subnet type*> Subnet <*slot/port*> dialog box, edit the following fields:

- ESH—The End System Hello PDU propagation frequency. An end system NE transmits ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- ISH—The Intermediate System Hello PDU propagation frequency. An intermediate system NE sends ISHs to other ESs and ISs to inform them about the NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- IIH—The Intermediate System to Intermediate System Hello PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.

Note The IS-IS Cost and DIS Priority parameters are provisioned when you create or enable a subnet. You cannot change the parameters after the subnet is created. To change the DIS Priority and IS-IS Cost parameters, delete the subnet and create a new one.

Click **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-A547 Edit an IP-Over-CLNS Tunnel

Purpose	This task allows you to edit the parameters of an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite procedures	DLP-A542 Create an IP-Over-CLNS Tunnel, page 22-49 DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Changing the IP or NSAP addresses or an IP-over-CLNS tunnel can cause loss of NE visibility or NE isolation. Do not change network addresses until you verify the changes with your network administrator.

Step 1 In node view, click the **Provisioning > OSI > Tunnels** tabs.

Step 2 Click **Edit**.

Step 3 In the Edit IP Over OSI Tunnel dialog box, complete the following fields:

- Tunnel Type—Choose a tunnel type:
  - **Cisco**—Creates the proprietary Cisco IP tunnel. Cisco IP tunnels add the CLNS header to the IP packets.
  - **GRE**—Creates a Generic Routing Encapsulation tunnel. GRE tunnels add the CLNS header and a GRE header to the IP packets.

  The Cisco proprietary tunnel is slightly more efficient than the GRE tunnel because it does not add the GRE header to each IP packet. The two tunnel types are not compatible. Most Cisco routers support the Cisco IP tunnel, while only a few support both GRE and Cisco IP tunnels. You generally should create Cisco IP tunnels if you are tunneling between two Cisco routers or between a Cisco router and an ONS node.

Caution Always verify that the IP-over-CLNS tunnel type you choose is supported by the equipment at the other end of the tunnel.

- IP Address—Enter the IP address of the IP-over-CLNS tunnel destination.
- IP Mask—Enter the IP address subnet mask of the IP-over-CLNS destination.

- OSPF Metric—Enter the OSPF metric for sending packets across the IP-over-CLNS tunnel. The OSPF metric, or cost, is used by OSPF routers to calculate the shortest path. The default is 110. Normally, it is not be changed unless you are creating multiple tunnel routes and want to prioritize routing by assigning different metrics.
- NSAP Address—Enter the destination NE or OSI router NSAP address.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-A548 Delete an IP-Over-CLNS Tunnel

Purpose	This task allows you to delete an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Deleting an IP-over-CLNS tunnel might cause the nodes to loose visibility or cause node isolation. If node isolation occurs, onsite provisioning might be required to regain connectivity. Always confirm tunnel deletions with your network administrator.

Step 1 In node view, click the **Provisioning > OSI > Tunnels** tabs.

Step 2 Choose the IP-over-CLNS tunnel that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-A549 View IS-IS Routing Information Base

Purpose	This task allows you to view the Intermediate System to Intermediate System (IS-IS) protocol routing information base (RIB). IS-IS is an OSI routing protocol that floods the network with information about NEs on the network. Each NE uses the information to build a complete and consistent picture of a network topology. The IS-IS RIB shows the network view from the perspective of the IS node.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, click the **Maintenance > OSI > IS-IS RIB** tabs.

Step 2 View the following RIB information for Router 1:

- Subnet Type—Indicates the OSI subnetwork point of attachment type used to access the destination address. Subnet types include SDCC, LDCC, GCC, OSC, and LAN.
- Location—Indicates the OSI subnetwork point of attachment. For DCC subnets, the slot and port are displayed. LAN subnets are shown as LAN.
- Destination Address—The destination NSAP (network service access point) of the IS.
- MAC Address—For destination NEs that are accessed by LAN subnets, the NE's Media Access Control address.

Step 3 If additional routers are enabled, you can view their RIBs by choosing the router number in the Router field and clicking **Refresh**.

Step 4 Return to your originating procedure (NTP).

DLP-A550 View ES-IS Routing Information Base

Purpose	This task allows you to view the End System to Intermediate System (ES-IS) protocol routing information base (RIB). ES-IS is an OSI protocol that defines how end systems (hosts) and intermediate systems (routers) learn about each other. For ESs, the ES-IS RIB shows the network view from the perspective of the ES node. For ISs, the ES-IS RIB shows the network view from the perspective of the IS node.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Maintenance > OSI > ES-IS RIB** tabs.

Step 2 View the following RIB information for Router 1:

- Subnet Type—Indicates the OSI subnetwork point of attachment type used to access the destination address. Subnet types include SDCC, LDCC, GCC, OSC, and LAN.
- Location—Indicates the subnet interface. For DCC subnets, the slot and port are displayed. LAN subnets are shown as LAN.
- Destination Address—The destination IS NSAP (network service access point).
- MAC Address—For destination NEs that are accessed by LAN subnets, the NE's Media Access Control address.

Step 3 If additional routers are enabled, you can view their RIBs by choosing the router number in the Router field and clicking **Refresh**.

Step 4 Return to your originating procedure (NTP).

DLP-A551 Manage the TARP Data Cache

Purpose	This task allows you to view and manage the TARP data cache (TDC). The TDC facilitates TARP processing by storing a list of TID to NSAP mappings.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-60
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Maintenance > OSI > TDC** tabs.

Step 2 View the following TARP data cache information:

- TID—The target identifier of the originating NE. For ONS 15454s, the TID is the name entered in the Node Name/TID field on the Provisioning > General tab.
- NSAP/NET—The Network Service Access Point or Network Element Title of the originating NE.
- Type—Indicates how the TARP data cache entry was created:
  - Dynamic—The entry was created through the TARP propagation process.
  - Static—The entry was manually created and is a static entry.

Step 3 If you want to query the network for an NSAP that matches a TID, complete the following steps. Otherwise, continue with Step 4.

Note The TID to NSAP function is not available if the TARP data cache is not enabled on the Provisioning > OSI > TARP subtab.

a. Click the **TID to NSAP** button.

b. In the TID to NSAP dialog box, enter the TID you want to map to an NSAP.

c. Click **OK**, then click **OK** on the information message.

d. On the TDC tab, click **Refresh**.

   If TARP finds the TID in its TDC it returns the matching NSAP. If not, TARP sends PDUs across the network. Replies will return to the TDC later, and a check TDC later message is displayed.

Step 4 If you want to delete all the dynamically-generated TDC entries, click the **Flush Dynamic Entries** button. If not, continue with Step 5.

Step 5 Return to your originating procedure (NTP).

DLP-A552 Adjust the Java Virtual Memory Heap Size

Purpose	This task allows you to adjust the Java Virtual Memory (JVM) heap size from the default 256 MB to the maximum of 512 MB in order to improve CTC performance.
Tools/Equipment	None
Prerequisite procedures	None
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click **Start > Settings > Control Panel**. The Windows Control Panel appears.

Step 2 Double-click **System**. The System Properties window appears.

Step 3 Click the **Advanced** tab.

Step 4 Click **Environmental Variables**. The Environmental Variables window appears.

Step 5 In the User Variables area, click **New**. The New User Variable window appears.

Step 6 Type **CTC_HEAP** in the Variable Name field.

Step 7 Type **512** in the Variable Value field.

Step 8 Click **OK**.

Step 9 Reboot your PC.

Step 10 Return to your originating procedure (NTP).

DLP-A553 Upgrade DS1 or DS3-12 Cards in a 1:N or 1:1 Configuration to High-Density Electrical Cards

Purpose	This task upgrades low-density electrical cards in a 1:N protection scheme (where N = 1 or 2) to high-density electrical cards (DS3/EC1-48, DS1/E1-56). Low-density cards are defined as DS-1 and DS3-12.
Tools/Equipment	DS3/EC1-48 card(s), as needed DS1/E1-56 card(s), as needed High-density shelf assembly (15454-SA-HD) High-density EIA (MiniBNC, UBIC-V, UBIC-H) installed.
Prerequisite Procedures	NTP-A17 Install the Electrical Cards, page 2-11
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note You cannot have any DS-1 cards installed on the same side of the shelf as the DS3/EC1-48 card when you finish the low-density to high-density upgrade.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-68. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Determine which low-density card(s) (DS-1, DS-3, DS-3E) you want to upgrade to high-density, according to slot limitations.

Note For 1:N protection groups, the protect card is installed in Slot 3 on the A side of the shelf and Slot 15 on the B side. For 1:1 protect groups, working and protect cards can be installed in any traffic slot.

The following limitations apply if you are upgrading a low-density protect card:

- The protect card must be in a protection group.
- The protect card must not protect any low-density electrical cards in Slots 4, 5, or 6 on the A side of the shelf (Slots 12, 13, or 14 on the B side).
- For 1:N protection groups where N = 2: On the A side, the protect card cannot be upgraded if any electrical cards are installed or preprovisioned in Slots 4, 5, or 6 (or Slots 12, 13, or 14 on the B side).
- For 1:N protection groups where N = 1: On the A side, if the protect card is installed in Slot 3 and it protects a low-density card in Slot 1, the protect card cannot be upgraded if Slot 5 or 6 has an electrical card installed or preprovisioned. For the B side, if the protect card is installed in Slot 15 and it protects a low-density card in Slot 17, the protect card cannot be upgraded if Slot 12 or 13 has an electrical card installed or preprovisioned.

- For 1:N protection groups where N = 1: On the A side, if the protect card is installed in Slot 3 and it protects a low-density card in Slot 2, the protect card cannot be upgraded if an electrical card is installed or preprovisioned in Slot 4. On the B side, if the protect card is installed in Slot 15 and it protects a low-density card in Slot 16, the protect card cannot be upgraded if an electrical card is installed or preprovisioned in Slot 14.

The following limitations apply to upgrading a working card after you have upgraded the protect card:

- A working card in Slot 1 on the A side (Slot 17 on the B side) cannot be upgraded if an electrical card is installed or preprovisioned in Slot 5 or 6 (Slot 12 or 13 on the B side).
- A working card in Slot 2 on the A side (Slot 16 on the B side) cannot be upgraded if an electrical card is installed or preprovisioned in Slot 4 (Slot 14 on the B side).

Step 4 In node view, double-click the current protect card. The card view appears.

Step 5 Make sure the current protect card is not active:

a. In card view, click the Maintenance > Protection tabs.

b. Select the protection group where the protect card resides.

Step 6 If the card status is Protect/Active, perform a switch so that the protect card becomes standby:

a. Click Switch.

b. Click Yes in the confirmation dialog box.

Step 7 Physically remove the card:

a. Open the card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

Step 8 Right-click the Protect/Standby slot and change the low-density card to the high-density card:

a. Choose Change Card from the drop-down list.

b. Choose the new high-density card type from the Change to drop-down list.

c. Click OK.

Step 9 Physically insert the new high-density electrical card into the protect slot. Be sure to remove the plastic protective covers on rear of the card before installing the card.

a. Open the ejectors on the card.

b. Slide the card into the slot along the guide rails.

c. Close the ejectors.

Wait for the IMPROPRMVL alarm to clear and the card to become standby. For more information about LED behavior during the high-density card boot-up, see the “NTP-A17 Install the Electrical Cards” procedure on page 2-9.

Step 10 Because the low-density working card is now active, switch traffic away from the low-density card:

a. In node view, double-click the slot where the low-density card is installed.

b. Click the Maintenance > Protection tabs.

c. Double-click the protection group that contains the working card.

d. Click the low-density card slot.

e. Click Switch and Yes in the Confirmation dialog box.

Step 11 Physically remove the low-density card you switched traffic away from in Step 10:

a. Open the card ejectors.

a. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

Step 12 Change the low-density card to the high-density card in CTC:

a. Right-click the slot where you removed the low-density card and choose Change Card from the drop-down list.

b. Choose the new card type from the Change to drop-down list.

c. Click OK.

Step 13 Insert the new high-density electrical card into the slot where you removed the low-density card. Be sure to remove the plastic protective covers on rear of the card before installing the card:

a. Open the ejectors on the card.

b. Slide the card into the slot along the guide rails.

c. Close the ejectors.

Wait for the IMPROPRMVL alarm to clear and the card to become standby. For more information about LED behavior during high-density electrical card bootup, see the "NTP-A17 Install the Electrical Cards" procedure on page 2-9.

Step 14 Clear the switch you performed in Step 10:

a. In node view, double-click the slot where you installed the high-density card in Step 13.

b. In the Maintenance > Protection tab, double-click the protection group that contains the reporting card.

c. Click the selected group.

d. Click Switch and click Yes in the confirmation dialog box.

e. The protect card should now become standby.

Step 15 If you have upgraded to a DS3/EC1-48 card and are using 734A cables with UBIC electrical interface adapters (EIAs), you must set the LBO for Ports 13 to 48 (DS3/EC1-48), doing so according to the actual distance (in feet) from the LBX panel.

If you are using 735A cables, you must set the LBO for Ports 13 to 48 (DS3/EC1-48), doing so according to the following conventions:

- Actual distance from the DSX panel is less than 110 feet (33.53 m):

  LBO setting is "0 - 225."

- Actual distance from the DSX panel is greater than or equal to 110 feet (33.53 m):

  LBO setting is "226 to 450."

If you have upgraded to a DS1/E1-56 card with UBIC EIAs, you must set the LBO for Ports 15 to 56, doing so according to the actual distance (in feet) from the LBX panel. Repeat Steps 4 through 14 for any other low-density cards you want to upgrade to high-density cards.

Step 16 Return to your originating procedure (NTP).

DLP-A553 Upgrade DS3XM-6 Cards in a 1:1 Configuration to High-Density DS3XM-12 Electrical Cards

Purpose	This task upgrades low-density electrical cards in a 1:1 protection scheme to high-density electrical cards (DS3XM-12 cards). This procedure upgrades low-density DS3XM-6 cards in a 1:1 protection scheme to high-density DS3XM-12 cards.
Tools/Equipment	DS3XM-12 card(s), as needed. Upgrade of DS3XM-6 to DS3XM-12 does not require a High-density shelf assembly. The upgrade can be performed on low-density shelf assembly as well.
Prerequisite Procedures	NTP-A17 Install the Electrical Cards, page 2-11
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note You cannot have any DS-1 cards installed on the same side of the shelf as the DS3XM-12 card when you finish the low-density to high-density upgrade.

Caution After upgrading a DS3XM-6 card to a DS3XM-12 card, the newly installed DS3XM-12 card will run in STS-12 mode. To change the backplane throughput rate, make sure the card is out-of-service and not carrying live traffic. Changing the backplane throughput rate on a in-service card can cause a traffic outage of greater than 50 ms.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-68. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Determine which low-density card(s) (DS3XM-6) you want to upgrade to high-density, according to slot limitations.

Note For 1:1 protect groups, working and protect cards can be installed in any traffic slot. But both cards should be placed adjacent to each other.

The following limitations apply if you are upgrading a low-density protect card:

- The protect card must be in a protection group.
- For 1:N protection groups where N = 1: If 1:1 is created on A side protect card cannot be upgraded if an DS1 card is installed or preprovisioned in A side. If 1:1 is created On the B side the protect card cannot be DS1 card is installed or preprovisioned in B side

The following limitations apply to upgrading a working card after you have upgraded the protect card:

- A working card on the A cannot be upgraded if an DS1 card is installed or preprovisioned in A side.

- A working card on the B side cannot be upgraded if an DS1 card is installed or preprovisioned in B side.

Step 4 In node view, double-click the current protect card. The card view appears.

Step 5 Make sure the current protect card is not active:

a. In card view, click the Maintenance > Protection tabs.

b. Select the protection group where the protect card resides.

Step 6 If the card status is Protect/Active, perform a switch so that the protect card becomes standby:

a. Click Switch.

b. Click Yes in the confirmation dialog box.

Step 7 Physically remove the card:

a. Open the card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

Step 8 Right-click the Protect/Standby slot and change the low-density card to the high-density card:

a. Choose Change Card from the drop-down list.

b. Choose the new high-density card type from the Change to drop-down list.

c. Click OK.

Step 9 Physically insert the new high-density electrical card into the protect slot. Be sure to remove the plastic protective covers on rear of the card before installing the card.

a. Open the ejectors on the card.

b. Slide the card into the slot along the guide rails.

c. Close the ejectors.

Wait for the IMPROPRMVL alarm to clear and the card to become standby. For more information about LED behavior during the high-density card boot-up, see the "NTP-A17 Install the Electrical Cards" procedure on page 2-9.

Step 10 Because the low-density working card is now active, switch traffic away from the low-density card:

a. In node view, double-click the slot where the low-density card is installed.

b. Click the Maintenance > Protection tabs.

c. Double-click the protection group that contains the working card.

d. Click the low-density card slot.

e. Click Switch and Yes in the Confirmation dialog box.

Step 11 Physically remove the low-density card you switched traffic away from in Step 10:

a. Open the card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

Step 12 Change the low-density card to the high-density card in CTC:

a. Right-click the slot where you removed the low-density card and choose Change Card from the drop-down list.

b. Choose the new high-density card type from the Change to drop-down list.

c. Click OK.

Step 13 Insert the new high-density electrical card into the slot where you removed the low-density card. Be sure to remove the plastic protective covers on rear of the card before installing the card:

- **a.** Open the ejectors on the card.
- **b.** Slide the card into the slot along the guide rails.
- **c.** Close the ejectors.

Wait for the IMPROPRMVL alarm to clear and the card to become standby. For more information about LED behavior during high-density electrical card bootup, see the "NTP-A17 Install the Electrical Cards" procedure on page 2-9.

Step 14 Clear the switch you performed in Step 10:

- **a.** In node view, double-click the slot where you installed the high-density card in Step 13.
- **b.** In the Maintenance > Protection tab, double-click the protection group that contains the reporting card.
- **c.** Click the selected group.
- **d.** Click Switch and Click Yes in the confirmation dialog box.

The protect card should now become standby.

Note After upgrading a DS3XM-6 card to a DS3XM-12 card, the newly installed DS3XM-12 card will run in STS-12 mode. Go to CTC Card View/Maintenance/Card window to change Backplane Throughput bandwidth to STS48 and refresh viewer window.

If you want to create 1:N on DS3XM-12 cards only slot numbers 3 and 15 should be listed for protect card selection.

Step 15 If you have upgraded to a DS3XM-12 and are using 734A cables with UBIC electrical interface adapters (EIAs), you must set the LBO for Ports 7 to 12 (DS3XM-12doing so according to the actual distance (in feet) from the LBX panel.

If you are using 735A cables, you must set the LBO for Ports 7 to 12 (DS3XM-12doing so according to the following conventions:

Actual distance from the DSX panel is less than 110 feet (33.53 m):

LBO setting is "0 - 225."

Actual distance from the DSX panel is greater than or equal to 110 feet (33.53 m):

LBO setting is "226 to 450."

Step 16 Return to your originating procedure (NTP).

DLP-A554 Upgrade EC-1 Cards in a 1:1 Configuration to DS3/EC1-48 Cards

Purpose	This task upgrades low-density electrical cards in a 1:N protection scheme (where N = 1 or 2) to high-density electrical cards (DS3/EC1-48, DS1/E1-56, and DS3XM-12 cards). Low-density cards are defined as DS-1 and DS3-12. This procedure also upgrades low-density electrical cards (DS3XM-6 cards) in a 1:1 protection scheme to high-density electrical cards (DS3XM-12 cards).
Tools/Equipment	DS3/EC1-48 card(s), as needed DS3XM-12 card(s), as needed DS1/E1-56 card(s), as needed High-density shelf assembly (15454-SA-HD) High-density EIA (MiniBNC, UBIC-V, UBIC-H) installed
Prerequisite Procedures	NTP-A17 Install the Electrical Cards, page 2-11
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note You cannot have any DS-1 cards installed on the same side of the shelf as the DS3/EC1-48 card when you finish the low-density to high-density upgrade.

Caution After upgrading a DS3XM-6 card to a DS3XM-12 card, the newly installed DS3XM-12 card will run in STS-12 mode. To change the backplane throughput rate, make sure the card is out-of-service and not carrying live traffic. Changing the backplane throughput rate on a in-service card can cause a traffic outage of up to 50 ms.

Step 1 Complete the DLP-A60 Log into CTC, page 17-60. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5.

Step 3 Determine which low-density card(s) you want to upgrade to high-density, according to slot limitations.

Note For 1:N protection groups, the protect card is installed in Slot 3 on the A side of the shelf and Slot 15 on the B side. For 1:1 protect groups, working and protect cards can be installed in any traffic slot.

The following limitations apply if you are upgrading a low-density protect card:

- If you are upgrading an EC1-12 card in a 1:1 protection group to a DS3/EC1-48 card, the EC1-12 cards must be in either Slots 1 and 2 or 16 and 17.
- If you are upgrading EC1-12 cards in a 1:1 protection group to a DS3/EC1-48 card, Slot 3 needs to be unoccupied if upgrading on the A-Side, and Slot 15 needs to be unoccupied if upgrading on the B-Side.

Step 4 In node view, double-click the current protect card. The card view appears.

Slot 1 contains the protect card if you are working on the A side of the shelf, and Slot 17 contains the protect card if you are working on the B side of the shelf.

Step 5 Make sure the current protect card is not active:

a. In card view, click the **Maintenance > Protection** tabs.

b. Select the protection group where the protect card resides.

Step 6 If the card status is Protect/Active, perform a switch so that the protect card becomes standby:

a. Click **Switch**.

b. Click **Yes** in the confirmation dialog box.

Step 7 Physically insert the new high-density electrical card into the new 1:N protect slot (Slot 3 for the A-Side and Slot 15 for the B-Side). Be sure to remove the plastic protective covers on rear of the card before installing the card.

a. Open the ejectors on the card.

b. Slide the card into the slot along the guide rails.

c. Close the ejectors.

For more information about LED behavior during the high-density card boot-up, see theNTP-A17 Install the Electrical Cards, page 2-11. Allow the card to completely boot up before proceeding.

Step 8 Delete the 1:1 EC1-12 low density protection group. See the "DLP-A155 Delete a Protection Group" task on page 18-23.

a. Open the card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

Step 9 Create a 1:N protection group for the EC1-12 cards and the new DS3/EC1-48 card. See the"NTP-A324 Create Protection Groups" task on page 4-13.

Note Make sure that the new protection group is 1:N and not 1:1. If you upgrading the A side of the shelf, make sure the protect card is in Slot 3 and the working cards are Slots 1 and 2. If you are upgrading the B side of the shelf, make sure the protect card is in Slot 15 and the working cards are in Slots 16 and 17.

Step 10 Because the low-density card is now active, switch traffic away from the low-density card in Slot 1 if you are working on the A side, or Slot 17 if you are working on the B side:

a. In node view, double-click the card in Slot 1/Slot 17.

b. Click the **Maintenance > Protection** tabs.

c. Double-click the protection group that contains the working card in Slot 1/Slot 17.

d. Click the card in Slot 1/Slot 17.

e. Click **Switch** and **Yes** in the Confirmation dialog box.

Step 11 Physically remove the low-density card in Slot 1/Slot 17:

a. Open the card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

Step 12 Change the low-density card to the high-density card in CTC:

a. Right-click Slot 1/Slot 17 and choose **Change Card** from the drop-down list.

b. Choose the new card type from the Change to drop-down list.

c. Click **OK**.

Step 13 Insert the new high-density electrical card into Slot 1/Slot 17. Be sure to remove the plastic protective covers on rear of the card before installing the card:

a. Open the ejectors on the card.

b. Slide the card into the slot along the guide rails.

c. Close the ejectors.

Wait for the IMPROPRMVL alarm to clear and the card to become standby. For more information about LED behavior during the high-density card bootup, see the NTP-A17 Install the Electrical Cards, page 2-11.

Step 14 Clear the switch you performed in Step 10:

a. In node view, double-click the card in Slot 1/Slot 17.

b. In the Maintenance > Protection tab, double-click the protection group that contains the reporting card.

c. Click the selected group.

d. Click **Clear** and click **Yes** in the confirmation dialog box.

The protect card in Slot 3 (A side) or Slot 15 (B side) should now become standby.

Note If you have upgraded to a DS3/EC1-48 card and are using 734A cables with UBIC electrical interface adapters (EIAs), you must set the LBO for Ports 13 to 48, doing so according to the actual distance (in feet) from the LBX panel.

If you are using 735A cables, you must set the LBO for Ports 13 to 48, doing so according to the following conventions:

Actual distance from the DSX panel is less than 110 feet (33.53 m):
LBO setting is “0 - 225.”

Actual distance from the DSX panel is greater than or equal to 110 feet (33.53 m):
LBO setting is “226 to 450.”

Step 15 As necessary, repeat Steps 4 through 14 for other low-density electrical cards you want to upgrade.

Step 16 Return to your originating procedure (NTP).

DLP-A555 Set Up SDH External or Line Timing

Purpose	This task defines the SDH timing source (external or line) for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 In the Timing Standard area, make sure that the Current Timing Standard is SDH. If it is not, continue with Step 3. If the Current Timing Standard is SDH, skip to Step 4.

Step 3 Click **Change** to switch the timing from SONET to SDH.

Note Changing the timing standard reinitializes the node and might affect traffic.

Step 4 In the General Timing area, complete the following information:

- Timing Mode—Choose **External** if the ONS 15454 derives its timing from a BITS source wired to the backplane pins; choose **Line** if timing is derived from an OC-N card that is optically connected to the timing node. A third option, Mixed, allows you to set external and line timing references.

Note Because Mixed timing might cause timing loops, Cisco does not recommend its use. Use this mode with care.

- Revertive—Select this check box if you want the ONS 15454 to revert to a primary reference source after the conditions that caused it to switch to a secondary timing reference are corrected.
- Reversion Time—If Revertive is checked, choose the amount of time that the ONS 15454 will wait before reverting to its primary timing source. Five minutes is the default.

Step 5 In the Reference Lists area, complete the following information:

Note You can define up to three timing references for the node and up to six BITS Out references. BITS Out references define the timing references used by equipment that can be attached to the node's BITS Out pins on the backplane. If you attach equipment to BITS Out pins, you normally attach it to a node with Line mode because equipment near the external timing reference can be directly wired to the reference.

- NE Reference—Allows you to define three timing references (Ref 1, Ref 2, Ref 3). The node uses Reference 1 unless a failure occurs to that reference, in which case the node uses Reference 2. If Reference 2 fails, the node uses Reference 3, which is typically set to Internal Clock. The internal clock is the Synchronous Equipment Timing Source (SETS) clock provided on the TCC2/TCC2P card. The options that appear depend on the Timing Mode setting.
- If the Timing Mode is set to External, your options are BITS1, BITS2, and Internal Clock.

- If the Timing Mode is set to Line, your options are the node's working OC-N cards and the Internal Clock. Choose the cards/ports that are directly or indirectly connected to the node wired to the BITS source, that is, the node's trunk (span) cards. Set Reference 1 to the trunk card that is closest to the BITS source. For example, if Slot 5 is connected to the node wired to the BITS source, choose Slot 5 as Reference 1.
- If the Timing Mode is set to Mixed, both BITS and OC-N cards are available, allowing you to set a mixture of external BITS and OC-N trunk (span) cards as timing references.
- BITS-1 Out/BITS-2 Out—Define the timing references for equipment wired to the BITS Out pins on the backplane. BITS-1 Out and BITS-2 Out are enabled when BITS-1 and BITS-2 facilities are put in service. If Timing Mode is set to External, choose the OC-N card used to set the timing. If Timing Mode is set to Line, you can choose an OC-N card or choose NE Reference to have the BITS-1 Out and/or BITS-2 Out follow the same timing references as the NE.

Step 6 Click the **BITS Facilities** subtab.

The BITS Facilities section sets the parameters for your BITS1 and BITS2 timing references. Many of these settings are determined by the timing source manufacturer. If equipment is timed through BITS Out, you can set timing parameters to meet the requirements of the equipment.

Step 7 In the BITS In area, complete the following information:

- Facility Type—For TCC2 and TCC2P cards, choose the BITS signal type supported by your BITS clock, either E1 or 2 MHz. For the TCC2P card only, you can also choose 64 Khz.
- BITS In State—If Timing Mode is set to External or Mixed, set the BITS In State for BITS-1 and/or BITS-2 to **IS** (in service), depending on whether one or both BITS input pin pairs on the TCC2/TCC2P card are connected to the external timing source. If Timing Mode is set to Line, set the BITS In State to **OOS** (out of service).

Step 8 If BITS In State is set to OOS, continue with Step 9. If the BITS In State is set to IS, complete the following information:

- Coding—Choose the coding used by your BITS reference, either HDB3 (high-density bipolar order 3) or AMI (alternate mark inversion).
- Framing—Choose the framing used by your BITS reference, either Unframed, FAS (frame alignment signal), FAS+CAS (frame alignment signal plus channel associated signal), FAS+CRC (frame alignment signal plus cyclic redundancy check), or FAS+CAS+CRC (frame alignment signal plus channel associated signal plus cyclic redundancy check).
- Sync Messaging—Check this check box to enable SSM. SSM is not available if Framing is set to Unframed, FAS, or FAS+CAS.
- Admin SSM—If the Sync Messaging check box is not checked, you can choose the SSM type from the drop-down list.
- Sa Bit—Choose the Sa bit in the E1 stream to use for incoming SSM messaging, either bit 4, 5, 6, 7, or 8.

Step 9 In the BITS Out area, complete the following information, as needed:

- Facility Type—(Display only) If the BITS IN signal is E1, the only supported BITS OUT is E1; likewise, if the BITS In signal is 2 MHz, the only supported BITS OUT is 2 MHz.
- BITS Out State—If equipment is connected to the node's BITS output pins on the backplane and you want to time the equipment from a node reference, set the BITS Out State for BITS-1 and/or BITS-2 to **IS**, depending on which BITS Out pins are used for the external equipment. If equipment is not attached to the BITS output pins, set the BITS Out State to **OOS**.

Step 10 If the BITS Out State is set to OOS, continue with Step 11. If BITS Out State is set to IS, complete the following information:

- Coding—(Display only) The coding is the same as that selected in the BITS In area.
- Framing—(Display only) The framing is the same as that selected in the BITS In area.
- AIS Threshold—If SSM is disabled or Unframed, FAS, or FAS+CAS are used, choose the quality level where a node sends an alarm indication signal (AIS) from the BITS 1 Out and BITS 2 Out backplane pins. An AIS alarm is raised when the optical source for the BITS reference falls to or below the SSM quality level defined in this field.
- Sa Bit—Choose the Sa bit in the E1 stream to use for outgoing SSM messaging, either bit 4, 5, 6, 7, or 8.

Step 11 Click **Apply**.

Note Refer to the *Cisco ONS 15454 Troubleshooting Guide* for timing-related alarms.

Step 12 Return to your originating procedure (NTP).

DLP-A556 Provision the Card Mode for ML-Series Ethernet Cards

Purpose	This task provisions the card mode for ML-Series Ethernet cards (ML100T-12, ML1000-2,and ML100X-8)
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the ML-Series Ethernet card graphic to open the card.

Step 2 Click the **Provisioning > Card** tabs.

Step 3 For the ML-Series Ethernet card, select an option from the drop-down Mode menu:

- HDLC—High-level data link control. (Does not support VLAN trunking, which is standard on most Cisco data devices.)
- GFP-F—Frame-mapped generic framing procedure, a PDU-oriented adaptation mode that maps a client frame into one GFP frame.
- RPR 802.17—802.17 Resilient Packet Ring, which is IEEE- compliant.

Note For more details about the interoperabilty of Optical Networking System (ONS) Ethernet cards, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A557 View Multirate PM Parameters

Purpose	This task enables you to view PM counts on a multirate card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the multirate card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 In the Port drop-down list, click the port you want to monitor.

Step 4 Click **Refresh**.

Step 5 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current), and Prev-*n* (previous) columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 6 To monitor another port on a multiport card, choose another port from the Port drop-down list and click **Refresh**.

Step 7 Return to your originating procedure (NTP).

DLP-A558 Provision the Designated SOCKS Servers

Purpose	This task identifies the ONS 15454 SOCKS servers in SOCKS-proxy-enabled networks. Identifying the SOCKS servers reduces the amount of time required to log into a node and have all NEs appear in network view (NE discovery time). The task is recommended when the combined CTC login and NE discovery time is greater than five minutes in networks with SOCKS proxy enabled. Long (or failed) login and NE discovery times can occur in networks that have a high ENE-to-GNE ratio and a low number of ENEs with LAN connectivity.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note Note: If you cannot log into a network node, complete the "DLP-A60 Log into CTC" task on page 17-60 choosing the Disable Network Discovery option. Complete this task, then log in again with network discovery enabled.

Note To complete this task, you must have either the IP addresses or DNS names of all ONS 15454 nodes in the network with LAN access that have SOCKS proxy enabled.

Note SOCKS proxy servers can be any accessible ONS network nodes that have LAN access, including the ONS 15310-MA, ONS 15310-CL, ONS 15327, and ONS 15600, ONS 15600 SDH nodes.

Note You must repeat this task any time that changes to SOCKS proxy server nodes occur, for example, whenever LAN connectivity is added to or removed from a node, or when nodes are added or removed from the network.

Step 1 From the CTC Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **SOCKS** tab.

Step 3 In the Designated SOCKS Server field, type the IP address or DNS node name of the first ONS 15454 SOCKS server. The ONS 15454 that you enter must have SOCKS proxy server enabled, and it must have LAN access.

Step 4 Click **Add**. The node is added to the SOCKS server list. If you need to remove a node on the list, click **Remove**.

Step 5 Repeat Steps 3 and 4 to add all qualified ONS 15454s within the network. All ONS nodes that have SOCKS proxy enabled and are connected to the LAN should be added.

Step 6 Click **Check All Servers**. A check is conducted to verify that all nodes can perform as SOCKS servers. If so, a check is placed next to the node IP address or node name in the SOCKS server list. An X placed next to the node indicates one or more of the following:

- The entry does not correspond to a valid DNS name.
- The numeric IP address is invalid.
- The node cannot be reached.
- The node can be reached, but the SOCKS port cannot be accessed, for example, a firewall problem might exist.

Step 7 Click **Apply**. The list of ONS 15454s, including ones that received an X in Step 6, are added as SOCKS servers.

Step 8 Click **OK** to close the Preferences dialog box.

Step 9 Return to your originating procedure (NTP).

DLP-A559 Install or Reinstall the CTC JAR Files

Purpose	This task installs or reinstalls the CTC JAR files into the CTC cache directory on your PC. This is useful when you are using a new CTC version and want to install or reinstall the CTC JAR files without logging into a node or using the StartCTC application (StartCTC.exe).
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Insert the Cisco ONS 15454 Software Release 9.1, 9.2, or 9.2.1 CD into your CD drive.

Step 2 Navigate to the CacheInstall directory.

Note The CTC cache installer is also available on Cisco.com. If you are downloading SetupCtc-*version*.exe (where *version* is the release version, for example, SetupCtc-085000.exe) file from Cisco.com, skip Step 1 and Step 2.

Step 3 Copy the SetupCtc-*version*.exe file to your local hard drive. Use any location that is convenient for you to access, such as the Windows desktop. Ensure that you have enough disk space to copy and extract the SetupCtc-*version*.exe file.

Step 4 Double-click the SetupCtc-*version*.exe file. This creates a directory named SetupCtc-*version* (at the same location), which contains the LDCACHE.exe file and other CTC files.

Step 5 Double-click the LDCACHE.exe file to install or reinstall the new CTC JAR files into the CTC cache directory on your PC.

Step 6 Return to your originating procedure (NTP).

DLP-A560 Create an Optimized 1+1 Protection Group

Purpose	This task creates an optimized 1+1 protection group for OC3-4, OC3-8, and MRC-2.5G-4 cards (in OC-3 configurations).
Tools/Equipment	Installed OC3-4 cards, OC3-8 cards, MRC-2.5G-4 cards, or preprovisioned slots
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed; consult your network administrator before using this feature.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that the cards are installed according to the optimized 1+1 requirements specified in Table 4-1 on page 4-14.

Step 2 Change the port type from SONET to SDH for each applicable port on the OC3-4, OC3-8, or MRC-2.5G-4 card where you want to provision a 1+1 optimized protection group:

a. In node view, double-click the applicable card.

b. Click the **Provisioning > Line** tabs.

c. In the Type column next to port, choose **SDH** from the drop-down list and click **Apply**.

Step 3 In node view, click the **Provisioning > Protection** tabs.

Step 4 In the Protection Groups area, click **Create**.

Step 5 In the Create Protection Group dialog box, enter the following:

- Name—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (“) characters.
- Type—Choose **1+1 Optimized** from the drop-down list.
- Protect Port—Choose the protect port from the drop-down list. The list displays the available OC3-4, OC3-8, or MRC-2.5G-4 ports. If OC3-4, OC3-8, or MRC-2.5G-4 cards are not installed, no ports appear in the drop-down list.

After you choose the protect card, a list of cards available for protection appear in the Available Ports list. If no cards are available, no cards appear. If this occurs, you cannot complete this task until you install the physical cards or preprovision the ONS 15454 slots using the “DLP-A330 Preprovision a Card Slot” task on page 20-20.

Step 6 From the Available Ports list, choose the port that will be protected by the port you selected in the Protect Port field. Click the top arrow button to move each port to the Working Ports list.

Step 7 Complete the remaining fields:

- Reversion time—If Revertive is checked, choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. Reversion time is the amount of time that will elapse before the primary channel is automatically renamed as secondary and the secondary channel is renamed as primary. The reversion timer starts after conditions causing the switch are cleared.
- Verification guard time—Choose the verification guard time from the drop-down list. The range is 500ms to 1s. A verification guard timer is used to ensure the acceptance of a Force switch command from the far-end node. When the Force command is received, if no Lockout is present or if Secondary section is not in a failed state, then the outgoing K1 byte is changed to indicate Force and the verification guard timer is started. If a Force switch command is not acknowledged by the far-end within the verification guard timer duration, then the Force command is cleared.
- Recovery guard time—Choose the recovery guard time from the drop-down list. The range is 0s to 10s. The default is 1s. A recovery guard timer is used for preventing rapid switches due to SD/SF (Signal Degrade/Signal Failure) failures. After the SD/SF failure is cleared on the line, a recovery guard timer is started. Recovery guard time is the amount of time elapsed before the system declares that a condition is cleared after the detection of an SD/SF failure.
- Detection guard time—Choose the detection guard time from the drop-down list. The range is 0s to 5s. The default is 1s. The detection guard timer is started after detecting an SD/SF/LOS (Loss of Signal) /LOF (Loss of Frame) /AIS-L (Alarm Indication Signal - Line) failure. Detection guard time is the amount of time elapsed before a traffic switch is initiated to a standby card after the detection of an SD/SF/LOS/LOF/AIS-L failure on the active card.

Step 8 Click **OK**.

Step 9 Return to your originating procedure (NTP).

DLP-A561 Modify an Optimized 1+1 Protection Group

Purpose	This task modifies an optimized 1+1 protection group for OC3-4, OC3-8, and MRC-2.5G-4 cards (in OC-3 configurations).
Tools/Equipment	None
Prerequisite Procedures	DLP-A560 Create an Optimized 1+1 Protection Group, page 22-73 DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Protection** tabs.

Step 2 In the Protection Groups area, click the optimized 1+1 protection group you want to modify.

Step 3 In the Selected Group area, modify the following as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Reversion time—If Revertive is checked, choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. Reversion time is the amount of time that will elapse before the primary channel is automatically renamed as secondary and the secondary channel is renamed as primary.
- Verification guard time—Choose the verification guard time from the drop-down list. The range is 500ms to 1s. A verification guard timer is used to ensure the acceptance of a Force switch command from the far-end node. When the Force command is received, if no Lockout is present or if the Secondary section is not in a failed state, then the outgoing K1 byte is changed to indicate Force and the verification guard timer is started. If a Force user command is not acknowledged by the far-end within the verification guard timer duration, then the Force command is cleared.
- Recovery guard time—Choose the recovery guard time from the drop-down list. The range is 0s to 10s. The default is 1s. A recovery guard timer is used for preventing rapid switches due to signal degrade (SD) or signal failure (SF) failures. After the SD/SF failure is cleared on the line, a recovery guard timer is started. Recovery guard time is the amount of time elapsed before the system declares that a condition is cleared after the detection of an SD/SF failure.
- Detection guard time—Choose the detection guard time from the drop-down list. The range is 0s to 5s. The default is 1 second. The detection guard timer is started after detecting an SD, SF, loss of signal (LOS), loss of frame (LOF), or line alarm indication signal (AIS-L) failure. Detection guard time is the amount of time elapsed before a traffic switch is initiated to a standby card after the detection of an SD, SF, LOS, LOF, or AIS-L failure on the active card.

Step 4 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-A562 View ML-Series RPR Span PM Parameters

Purpose	This task enables you to view RPR span PM counts at selected time intervals on an ML-Series Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note For ML-Series card provisioning, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

Step 1 In node view, double-click the ML-Series Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance > RPR Span** tabs.

Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Port RPR East and Port RPR West columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 9-2.

Step 5 Return to your originating procedure (NTP).

DLP-A563 Configure an Automatically Routed BLSR DRI

Purpose	This task enables you to set the primary and secondary nodes and ring and path options for an automatically routed BLSR Dual Ring Interconnect (DRI), as well as set circuit routing constraints.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 You must check Dual Ring Interconnect on the Circuit Creation wizard during a circuit creation procedure (automatically routed).
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In the Circuit Constraints for Automatic Routing area, click **Add BLSR DRI**.

Step 2 In the confirmation window, click **OK**.

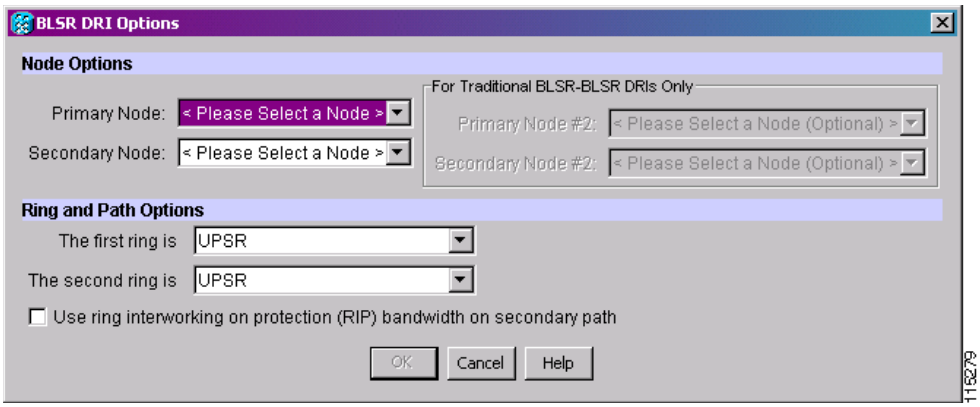
Step 3 In the Node options area of the BLSR DRI Options dialog box, complete the following (Figure 22-12):

- Primary Node—For a traditional or integrated BLSR-DRI, choose the node where the circuit interconnects the rings.
- Secondary Node—For a traditional or integrated BLSR-DRI, choose the secondary node for the circuit to interconnect the rings. This route is used if the route on the primary node fails.
- Primary Node #2—For a traditional BLSR-DRI where two primary nodes are required to interconnect rings, choose the second primary node.
- Secondary Node #2—For a traditional BLSR-DRI where two secondary nodes are required, choose the second secondary node.

Step 4 In the Ring and Path Options area, complete the following:

- The first ring is—Choose Path Protection or BLSR from the drop-down list.
- The second ring is—Choose Path Protection or BLSR from the drop-down list.
- Use ring interworking protection (RIP) on secondary path—Check this box to carry the secondary spans on the protection channels. These spans will be preempted during a ring/span switch.

Figure 22-12 Selecting BLSR DRI Primary and Secondary Node Assignments



Step 5 Click **OK**. The node information appears in the Required Nodes/Lines list, and the map graphic indicates which nodes are primary and secondary.

Step 6 In the Circuit Constraints for Automatic Routing area, click a node or span on the circuit map:

Step 7 Click **Include** to include the node or span in the circuit, or click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans is the order in which the circuit will be routed. Click spans twice to change the circuit direction. If you are creating a path protection to BLSR traditional handoff, exclude the unprotected links from the primary node towards the secondary node. If you are creating a path protection to BLSR integrated handoff, exclude unnecessary DRIs on the path protection segments.

Step 8 Review the circuit constraints. To change the circuit routing order, choose a node in the Required Nodes/Links list and click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 9 Return to your originating procedure (NTP).

DLP-A564 Configure a Manually Routed BLSR DRI

Purpose	This task enables you to set the primary and secondary nodes for a manually routed BLSR DRI, as well as set circuit routing constraints.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 You must check Dual Ring Interconnect on the Circuit Creation wizard during a circuit creation procedure (manually routed).
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In the Route/Review Edit area, click the **BLSR-DRI Nodes** tab.

Step 2 Click **Add BLSR DRI**.

Step 3 In the BLSR DRI Options dialog box, complete the following (Figure 22-13):

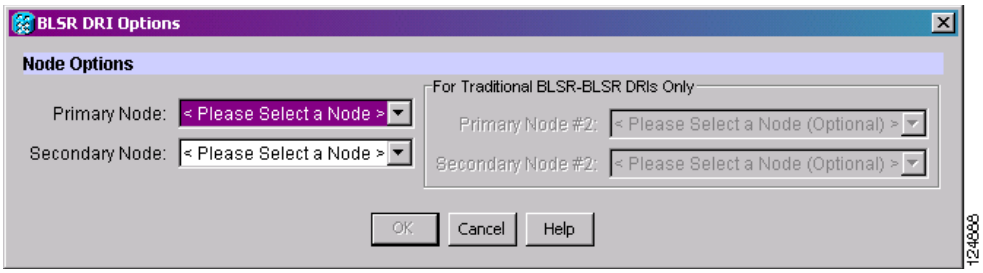
- Primary Node—For a traditional or integrated BLSR-DRI, choose the node where the circuit interconnects the rings.
- Secondary Node—For a traditional or integrated BLSR-DRI, choose the secondary node for the circuit to interconnect the rings. This route is used if the route on the primary node fails.
- Primary Node #2—For a traditional BLSR-DRI where two primary nodes are required to interconnect rings, choose the second primary node.
- Secondary Node #2—For a traditional BLSR-DRI where two secondary nodes are required, choose the second secondary node.

Step 4 Click **OK**.

Step 5 Review the circuit constraints. To change the circuit routing order, choose a node in the Required Nodes/Links list and click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 6 Click the **Included Spans** tab.

Figure 22-13 Selecting BLSR DRI Primary and Secondary Node Assignments (Manual Routing)



Step 7 Return to your originating procedure (NTP).

DLP-A565 Set Up a Solaris Workstation for a Craft Connection to an ONS 15454

Purpose	This task sets up a Solaris workstation for a craft connection to the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Log into the workstation as the root user.

Step 2 Check to see if the interface is plumbed by typing:

 # ifconfig *device*

For example:

 # ifconfig hme1

If the interface is plumbed, a message similar to the following appears:

```
hme1:flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 2 inet 0.0.0.0
netmask 0
```

If a message similar to this one appears, go to Step 4.

If the interface is not plumbed, a message similar to the following appears:

```
ifconfig: status: SIOCGLIFFLAGS: hme1: no such interface.
```

If a message similar to this one appears, go to Step 3.

Step 3 Plumb the interface by typing:

 # ifconfig *device* **plumb**

For example:

 # ifconfig hme1 plumb

Step 4 Configure the IP address on the interface by typing:

 # ifconfig *interface ip-address* **netmask** *netmask* **up**

For example:

 # ifconfig hme0 192.1.0.3 netmask 255.255.255.0 up

Note Enter an IP address that is identical to the ONS 15454 IP address except for the last octet. The last octet must be 1 or 3 through 254.

Step 5 In the Subnet Mask field, type **255.255.255.0**. Skip this step if you checked Enable Socks Proxy on Port and External Network Element (ENE) at Provisioning > Network > General > Gateway Settings.

Step 6 Test the connection:

a. Start Netscape Navigator.

b. Enter the ONS 15454 IP address in the web address (URL) field. If the connection is established, a Java Console window, CTC caching messages, and the Cisco Transport Controller Login dialog box appear. If this occurs, go to Step 2 of the "DLP-A60 Log into CTC" task on page 17-60 to complete the login. If the Login dialog box does not appear, complete Steps c and d.

c. At the prompt, type:

ping *ONS-15454-IP-address*

For example, to connect to an ONS 15454 with a default IP address of 192.1.0.2, type:

ping 192.1.0.2

If your workstation is connected to the ONS 15454, the following message appears:

```
IP-address is alive
```

Note Skip this step if you checked Enable Socks Proxy on Port and External Network Element (ENE) at Provisioning > Network > General > Gateway Settings.

d. If CTC is not responding, a "Request timed out" (Windows) or a "no answer from *x.x.x.x*" (UNIX) message appears. Verify the IP and subnet mask information. Check that the cables connecting the workstation to the ONS 15454 are securely attached. Check the link status by typing:

 # ndd -set /dev/*device* **instance 0**

 # ndd -get /dev/*device* **link_status**

For example:

 # ndd -set /dev/hme instance 0

 # ndd -get /dev/hme link_status

A result of "1" means the link is up. A result of "0" means the link is down.

Note Check the man page for ndd. For example, type: `# man ndd`.

Step 7 Return to your originating procedure (NTP).

DLP-A566 Install the CTC Launcher Application from a Release 9.1, 9.2, or 9.2.1 Software CD

Purpose	This task installs the CTC Launcher from a Release 9.1, 9.2, or 9.2.1 software CD.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Insert the Cisco ONS 15454 or Cisco ONS 15454 SDH or Cisco ONS 15310-CL or Cisco ONS 15310-MA Software Release 9.1, 9.2, or 9.2.1 CD into your CD drive.

Step 2 Navigate to the CtcLauncher directory.

Step 3 Save the StartCTC.exe file to a local hard drive.

Step 4 Return to your originating procedure (NTP).

DLP-A567 Install the CTC Launcher Application from a Release 9.1, 9.2, or 9.2.1 Node

Purpose	This task installs the CTC Launcher from an ONS 15454 node running Software R 9.1, 9.2, or 9.2.1.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Using a web browser, go to the following address, where *node-name* is the DNS name of a node you are going to access:

http://*node-name***/fs/StartCTC.exe**

The browser File Download dialog box appears.

Step 2 Click **Save**

Step 3 Navigate to the location where you want to save the StartCTC.exe file to a local hard drive.

Step 4 Click **Save**.

Step 5 Return to your originating procedure (NTP).

DLP-A568 Connect to ONS Nodes Using the CTC Launcher

Purpose	This task connects the CTC Launcher to ONS nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Start the CTC Launcher:

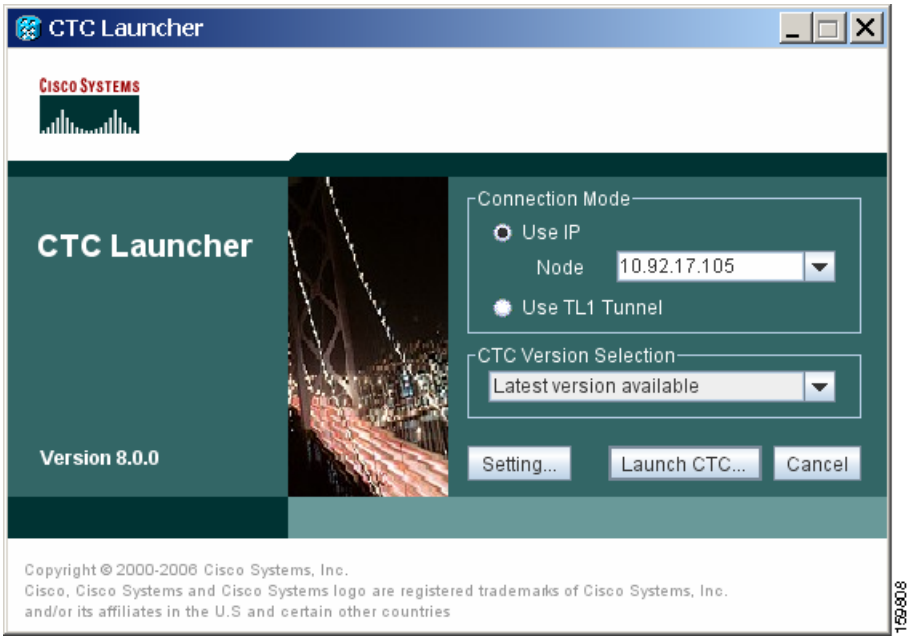
- Windows: navigate to the directory containing the StartCTC.exe file and double-click it. (You can also use the Windows Start menu Run command.)
- Solaris: assuming the StartCTC.exe file is accessible from the current shell path, navigate to the directory containing the StartCTC.exe file and type:

  % java -jar StartCTC.exe

Step 2 In the CTC Launcher dialog box, choose **Use IP**.

Figure 22-14 shows the CTC Launcher window.

Figure 22-14 CTC Launcher Window



Step 3 In the Login Node box, enter the ONS NE node name or IP address. (If the address was entered previously, you can choose it from the drop-down menu.)

Step 4 Select the CTC version you want to launch from the following choices in the drop-down menu:

- Same version as the login node: Select if you want to launch the same CTC version as the login node version, even if more recent versions of CTC are available in the cache.
- Latest version available: Select if you want to launch the latest CTC version available. If the cache has a newer CTC version than the login node, that CTC version will be used. Otherwise the same CTC version as the login node will be used.
- Version x.xx: Select if you want to launch a specific CTC version.

Note Cisco recommends that you always use the "Same version as the login node" unless the use of newer CTC versions is needed (for example, when CTC must manage a network containing mixed version NEs).

Step 5 Click **Launch CTC**. After the connection is made, the CTC Login dialog box appears.

Step 6 Log into the ONS node.

Note Because each CTC version requires particular JRE versions, the CTC Launcher will prompt the user for the location of a suitable JRE whenever a new CTC version is launched for the first time using a file chooser dialog (if a suitable JRE version is not known by the launcher yet). That JRE information is then saved in the user's preferences file. From the selection dialog, select any appropriate JRE directory.

After the JRE version is selected, the CTC will be launched. The required jar files will be downloaded into the new cache if they are missing. The CTC Login window will appear after a few seconds.

Step 7 Return to your originating procedure (NTP).

DLP-A569 Create a TL1 Tunnel Using the CTC Launcher

Purpose	This task creates a TL1 tunnel using the CTC Launcher, and the tunnel transports the TCP traffic to and from ONS ENEs through the OSI-based GNE.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Double-click the StartCTC.exe file.

Step 2 Click **Use TL1 Tunnel**.

Step 3 In the Open CTC TL1 Tunnel dialog box, enter the following:

- Far End TID—Enter the TID of the ONS ENE at the far end of the tunnel. The TID is the name entered in the Node Name field on the node view Provisioning > General tab.
- Host Name/IP Address—Enter the GNE DNS host name or IP address through which the tunnel will established. This is the third-party vendor GNE that is connected to an ONS node through an OSI DCC network. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.
- Choose a port option:
  - Use Default TL1 Port—Choose this option if you want to use the default TL1 port 3081 and 3082.
  - Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
- TL1 Encoding Mode—Choose the TL1 encoding:
  - LV + Binary Payload—TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient encoding mode. However, you must verify that the GNE supports LV + Binary Payload encoding.

  - LV + Base64 Payload—TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
  - Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
- GNE Login Required—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
- TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 4 Click **OK**.

Step 5 If the GNE Login Required box is checked, complete the following steps. If not, continue Step 6.

a. In the Login to Gateway NE dialog box UID field, enter the TL1 user name.

b. In the PID field, enter the TL1 user password.

c. Click **OK**.

Step 6 When the CTC Login dialog box appears, complete the CTC login.

Step 7 Return to your originating procedure (NTP).

DLP-A570 Create a TL1 Tunnel Using CTC

Purpose	This task creates a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 2 In the TL1 Tunnels window, click **Create**.

Step 3 In the Create CTC TL1 Tunnel dialog box, enter the following:

- Far End TID—Enter the TID of the ONS ENE at the far end of the tunnel. The ENE must be a Cisco ONS NE. The TID is the name entered in the Node Name field on the node view Provisioning > General tab.
- Host Name/IP Address—Enter the GNE DNS host name or IP address through which the tunnel will established. This is the third-party vendor GNE that is connected to an ONS NE with an OSI DCC. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.
- Choose a port option:
  - Use Default TL1 Port—Choose this option if you want to use the GNE default TL1 port. TL1 uses standard ports, such as 3081 and 3082, unless custom TL1 ports are defined.
  - Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
- TL1 Encoding Mode—Choose the TL1 encoding:

  - LV + Binary Payload—TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient. However, you must verify that the GNE supports LV + Binary Payload encoding.
  - LV + Base64 Payload—TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
  - Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
- GNE Login Required—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
- TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 4 Click **OK**.

Step 5 If the GNE Login Required box is checked, complete the following steps. If not, continue Step 6.

a. In the Login to Gateway NE dialog box UID field, enter the TL1 user name.

b. In the PID field, enter the TL1 user password.

c. Click **OK**.

Step 6 After the CTC Login dialog box appears, log into CTC.

Step 7 Return to your originating procedure (NTP).

DLP-A571 View TL1 Tunnel Information

Purpose	This task views a TL1 tunnel created using the CTC Launcher.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Log into CTC.

Step 2 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 3 In the TL1 Tunnels window, view the information shown in Table 22-8.

Table 22-8 TL1 Tunnels Window

Item	Description
Far End TID	The Target ID of the NE at the far end of the tunnel. This NE is an ONS NE. It is typically connected with an OSI DCC to a third-party vender GNE. CTC manages this NE.
GNE Host	The GNE host or IP address through which the tunnel is established. This is generally a third-party vendor GNE that is connected to an ONS NE with an OSI DCC. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.
Port	The TCP port number where the GNE accepts TL1 connections coming from the DCN. These port numbers are standard (such as 3081 and 3082) unless custom port numbers are provisioned on the GNE.

Table 22-8 TL1 Tunnels Window (continued)

Item	Description
TL1 Encoding	Defines the TL1 encoding used for the tunnel: • LV + Binary Payload—TL1 messages are delimited by an LV (length value) header. TCP traffic is encapsulated in binary form. • LV + Base64 Payload—TL1 messages are delimited by an LV header. TCP traffic is encapsulated using the base 64 encoding. • Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
GNE TID	The GNE TID is shown when the GNE requires a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs. If present, CTC asks the user for the ACT-USER user ID and password when the tunnel is opened.
State	Indicates the tunnel state: OPEN—A tunnel is currently open and carrying TCP traffic. RETRY PENDING—The TL1 connection carrying the tunnel has been disconnected and a retry to reconnect it is pending. (CTC automatically attempts to reconnect the tunnel at regular intervals. During that time all ENEs behind the tunnel are unreachable.) (empty)—No tunnel is currently open.
Far End IP	The IP address of the ONS NE that is at the far end of the TL1 tunnel. This information is retrieved from the NE when the tunnel is established.
Sockets	The number of active TCP sockets that are multiplexed in the tunnel. This information is automatically updated in real time.
Retries	Indicates the number of times CTC tried to reopen a tunnel. If a network problem causes a tunnel to go down, CTC automatically tries to reopen it at regular intervals. This information is automatically updated in real time.
Rx Bytes	Shows the number of bytes of management traffic that were received over the tunnel. This information is automatically updated in real time.
Tx Bytes	Shows the number of bytes of management traffic that were transmitted over the tunnel. This information is automatically updated in real time.

Step 4 Return to your originating procedure (NTP).

DLP-A572 Edit a TL1 Tunnel Using CTC

Purpose	This task edits a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 2 In the TL1 Tunnels window, click the tunnel you want to edit.

Step 3 Click **Edit**.

Step 4 In the Edit CTC TL1 Tunnel dialog box, edit the following:

- Use Default TL1 Port—Choose this option if you want to use the GNE default TL1 port. TL1 uses standard ports, such as 3081 and 3082, unless custom TL1 ports are defined.
- Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
- TL1 Encoding Mode—Choose the TL1 encoding:
  - LV + Binary Payload—TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient. However, you must verify that the GNE supports LV + Binary Payload encoding.
  - LV + Base64 Payload—TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
  - Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
- GNE Login Required—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
- TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 5 Click **OK**.

Step 6 If the GNE Login Required box is checked, complete login in the Login to Gateway NE dialog box. If not, continue Step 6.

a. In the UID field, enter the TL1 user name.

b. In the PID field, enter the TL1 user password.

c. Click **OK**.

Step 7 When the CTC Login dialog box appears, complete the CTC login. Refer to login procedures in the user documentation for the ONS ENE.

Step 8 Return to your originating procedure (NTP).

DLP-A573 Delete a TL1 Tunnel Using CTC

Purpose	This task deletes a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 2 In the TL1 Tunnels window, click the tunnel you want to delete.

Step 3 Click **Delete**.

Step 4 In the confirmation dialog box, click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-A574 Provision a PPM on the MRC-12 or MRC-2.5G-4 Card

Purpose	This task provisions single-rate and multirate pluggable port modules (PPMs) for the MRC-12 or MRC-2.5G-4 card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the MRC-12 or MRC-2.5G-4 card where you want to provision PPM settings.

Step 2 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 3 In the Pluggable Port Modules pane, click **Create**. The Create PPM dialog box appears.

Step 4 In the Create PPM dialog box, complete the following:

- PPM—Choose the slot number where the SFP is installed from the drop-down list.
- PPM Type—Choose the number of ports located on the SFP from the drop-down list. If only one port is supported, **PPM (1 port)** is the only option.

Step 5 Click **OK**. The newly created port appears on the Pluggable Port Modules pane. The row on the Pluggable Port Modules pane turns light blue and the Actual Equipment Type column lists the equipment name.

Step 6 Verify that the PPM appears in the list on the Pluggable Port Modules pane. If it does not, repeat Steps 4 through 5.

Step 7 Repeat the task to provision a second PPM.

Step 8 Click **OK**.

Step 9 Continue with the "DLP-A575 Provision the Optical Line Rate on the MRC-12 or MRC-2.5G-4 Card" task on page 22-89 to provision the line rate.

Step 10 Return to your originating procedure (NTP).

DLP-A575 Provision the Optical Line Rate on the MRC-12 or MRC-2.5G-4 Card

Purpose	This task provisions the optical line rate on a MRC-12 or MRC-2.5G-4 PPM. Regardless of whether a PPM on the MRC-12or MRC-2.5G-4 card is single-rate or multirate, you must provision the line rate on the PPM.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the MRC-12 or MRC-2.5G-4 card where you want to provision PPM settings.

Step 2 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 3 In the Pluggable Ports pane, click **Create**. The Create Port dialog box appears.

Step 4 In the Create Port dialog box, complete the following:

- Port—Click the PPM number and port number from the drop-down list. The first number indicates the PPM and the second number indicates the port number on the PPM. For example, the first PPM displays as 1-1 and the second PPM displays as 2-1.
- Port Type—Click the type of port from the drop-down list. The port type list displays the supported port rates on your PPM, which may differ based on PPM type and rate. See Table 22-9 for definitions of the supported rates on the MRC-12 and MRC-2.5G-4 cards.

Table 22-9 PPM Port Types

Card	Port Type
MRC-12 and MRC-2.5G-4	• OC-3—155 Mbps • OC-12—622 Mbps • OC-48—2.48 Gbps

Step 5 Click **OK**.

Step 6 Repeat Steps 3 through 5 to configure the port rates as needed.

Step 7 Click **OK**. The row on the Pluggable Ports pane is light blue until the actual SFP is installed and then the row turns white.

Step 8 Return to your originating procedure (NTP).

DLP-A576 Change the Optical Line Rate on the MRC-12 or MRC-2.5G-4 Card

Purpose	This task changes the optical line rate on a multirate PPM. Perform this task if you want to change the port rate on an SFP that is already provisioned.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the MRC-12 or MRC-2.5G-4 card where you want to provision PPM settings.

Step 2 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 3 Click the port with the port rate you want to change in the Pluggable Ports pane. The highlight changes to dark blue.

Step 4 Click **Edit**. The Edit Port Rate dialog box appears.

Step 5 In the Change To field, use the drop-down list to select the new port rate and click **OK**.

Step 6 Click **Yes** in the Confirm Port Rate Change dialog box.

Step 7 Return to your originating procedure (NTP).

DLP-A577 Delete a PPM from the MRC-12, MRC-2.5G-4, or OC192-XFP Card

Purpose	This task deletes PPM provisioning for SFPs on the MRC-12, MRC-2.5G-4, or OC192-XFP card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Before deleting a PPM, delete the PPM from the provisioning pane.

Step 1 Determine if the PPM can be deleted.

You cannot delete a port on a PPM if it is in service, part of a protection group, has a communications channel termination in use, is used as a timing source, has circuits, or has overhead circuits. As needed, complete the following procedures and task:

- DLP-A154 Modify a 1+1 Protection Group, page 18-23
- NTP-A85 Change Node Timing, page 11-6

- NTP-A292 Modify or Delete Communications Channel Terminations and Provisionable Patchcords, page 11-5
- NTP-A151 Modify and Delete Circuits, page 7-4
- NTP-A278 Modify and Delete Overhead Circuits and Server Trails, page 7-5
- DLP-A214 Change the Service State for a Port, page 19-9

Step 2 In node view, double-click the card where you want to delete PPM settings.

Step 3 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 4 To delete a PPM and the associated ports:

a. Click the PPM line that appears in the Pluggable Port Modules pane. The highlight changes to dark blue.

b. Click **Delete**. The Delete PPM dialog box appears.

c. Click **Yes**. The PPM provisioning is removed from the Pluggable Port Modules pane and the Pluggable Ports pane.

Step 5 Verify that the PPM provisioning is deleted:

- If the PPM was preprovisioned, CTC shows an empty slot in CTC after it is deleted.
- If the SFP (PPM) is physically present when you delete the PPM provisioning, CTC transitions to the deleted state; the ports (if any) are deleted, and the PPM is represented as a gray graphic in CTC. The SFP can be provisioned again in CTC or the equipment can be removed, in which case the removal causes the graphic to disappear.

Step 6 If you need to remove the SFP, see the "DLP-A470 Remove GBIC or SFP/XFP Devices" task on page 21-62.

Step 7 Return to your originating procedure (NTP).

DLP-A578 Configuring Windows Vista to Support CTC

Purpose	This task describes the configurations that must be done in Windows Vista operating system prior to launching CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Complete the following steps to disable Internet Explorer 7 protected mode:

Note Perform a full installation of Windows Vista operating system on your computer. If Windows Vista is installed through operating system upgrade, then CTC will not work. Refer to the manufacturer's user guide for instructions on how to install Windows Vista.

Note This procedure is needed only if CTC is launched from the Internet Explorer browser. If you start CTC by downloading the CTC Launcher application from the node, perform the See DLP-A567 Install the CTC Launcher Application from a Release 9.1, 9.2, or 9.2.1 Node, page 22-81.

a. Open Internet Explorer,
b. Click **Tools > Internet** Options.
c. Click **Security** tab.
d. Select the zone that is appropriate. Available options are: **Local Intranet**, **Internet**, and **Trusted Sites**.
e. Check the **Disable Protect Mode** check box.

Step 2 Complete the following steps to Disable TCP Autotuning:

a. From the Windows Start menu, click **Search > Search for Files and Folders.** The Search window appears.
b. On the right side of the window in the Search box, type **Command Prompt** and press **Enter**. Windows will search for the Command Prompt application and list it in the search results.
c. Right click **cmd** and select **Run as administrator**.
d. Enter the administrator user ID and password and click **OK**.
e. A Command prompt windows appears. At the command prompt enter the following text:

```
netsh interface tcp set global autotuninglevel=disabled
```

Autotuning can be enabled if desired using the following command:

```
netsh interface tcp set global autotuninglevel=normal
```

Step 3 Return to your originating procedure (NTP).

DLP-A579 Provision an Open VCAT Circuit Source and Destination

Purpose	This task provisions an open virtual concatenated (VCAT) circuit source and destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60 The Circuit Creation wizard Circuit Source page must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Node drop-down list, choose the node where the circuit will originate.

Step 2 From the Slot drop-down list, choose the slot containing the CE-Series, ML-Series, or FC_MR-4 card where the circuit originates. (If a card's capacity is fully utilized, it does not appear in the list.)

Step 3 Depending on the circuit origination card, choose the source port and/or STS and, if applicable, VT from the Port and STS drop-down lists. The Port drop-down list is only available if the card has multiple ports. STSs and VTs do not appear if they are already in use by other circuits. VTs do not appear for STS-V circuits.

Step 4 Click **Next**.

Step 5 Click the **Auto-ranged Destinations** check box to select the endpoints automatically. Only the first endpoint has to be selected, all of the other endpoints will be automatically created.

If you do not choose auto-ranged destinations; from the card selected in Step 2, choose the source port and/or STS and, if applicable, VT from the Port and STS drop-down lists. The Port drop-down list is only available if the card has multiple ports. STSs and VTs do not appear if they are already in use by other circuits. VTs do not appear for STS-V circuits.

Step 6 From the **Select Destinations For** drop-down list, choose the member number.

Step 7 From the Node drop-down list, choose the destination node.

Step 8 From the Slot drop-down list, choose the slot containing the card where the circuit will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the list.) Non-data cards may be used for open VCAT circuits.

Step 9 Click **Add Destinations**.

Step 10 Click **Next**.

Step 11 Return to your originating procedure (NTP).

DLP-A580 Create User Defined Alarm Types

Purpose	This task creates alarm types for external alarms on the AIC-I card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the AIC-I card.

Step 2 Click the **Provisioning > User Defined Alarms** tabs.

Step 3 Click **Add**.The Enter New Alarm Type dialog box appears.

Step 4 In the name field type the new alarm type name and click **OK**.

- The name can be up to 20 alphanumeric characters (upper case). No spaces, no special characters, hyphen (-) is allowed.
- Up to 50 different Alarm Types can be defined.

Step 5 Click the **External Alarms** tab.

Step 6 Verify that the defined name appears in the **Alarm Type** drop-down list.

Step 7 Return to your originating procedure (NTP).

DLP-A581 Configure Link Integrity Timer

Purpose	This task sets the link integrity soak timer for each port in the Ethernet cards (mapper cards).
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, double-click a card to open the card view.

Step 2 In the card view, click the **Provisioning > Ether Ports** tabs.

Step 3 Change the Admin State of the port to OOS,DSBLD or OOS,MT for the corresponding port number.

Step 4 In the Line area, enable the link integrity soak timer feature by unchecking the check box in the Link Integrity Disable column for the corresponding port number. The Link Integrity Disable option is available only for CE-1000 card.

Step 5 Enter the desired link integrity soak duration in the Link Integrity Timer column for the corresponding port number. Enter the link integrity soak duration in the range between 200 and 10000 ms, in multiples of 100 ms.

Note The default link integrity timer value is 200 ms.

Step 6 Click **Apply** to set the specified link integrity soak timer.

Step 7 Return to your originating procedure (NTP).

DLP-A584 Create an SNMPv3 User

Purpose	This procedure creates an SNMPv3 user.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP > SNMP V3 > User** tabs.

Step 2 Click **Create**.

Step 3 In the Create User dialog box, enter the following information:

- User Name—Specify the name of the user on the host that connects to the agent. The user name must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters. For TL1 compatibility, the user name must be of 6 to 10 characters.
- Group Name—Specify the group to which the user belongs.
- Authentication
  - Protocol—Select the authentication algorithm that you want to use. The options are NONE, MD5, and SHA.
  - Password—Enter a password if you select MD5 or SHA. By default, the password length is set to a minimum of eight characters.
- Privacy—Initiates a privacy authentication level setting session that enables the host to encrypt the contents of the message that is sent to the agent.
  - Protocol—Select NONE or DES as the privacy authentication algorithm.
  - Password—Enter a password if you select DES.

Step 4 Click **OK** to save the information.

Step 5 Return to your originating procedure (NTP).

DLP-A585 Create MIB Views

Purpose	This procedure creates an SNMPv3 MIB view.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP > SNMP V3 > MIB views** tabs.

Step 2 Click **Create**.

Step 3 In the Create Views dialog box, enter the following information:

- Name—Name of the view.
- Subtree OID—The MIB subtree which, when combined with the mask, defines the family of subtrees.
- Bit Mask—A family of view subtrees. Each bit in the bit mask corresponds to a sub-identifier of the subtree OID.
- Type—Select the view type. Options are Include and Exclude. Type defines whether the family of subtrees that are defined by the subtree OID and the bit mask combination are included or excluded from the notification filter.

Step 4 Click **OK** to save the information.

Step 5 Return to your originating procedure (NTP).

DLP-A586 Create Group Access

Purpose	This procedure creates a user group and configures the access parameters for the users in the group.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP > SNMP V3 > Group Access** tabs.

Step 2 Click **Create**.

Step 3 In the Create Group Access dialog box, enter the following information:

- Group Name—The name of the SNMP group, or collection of users, who share a common access policy.
- Security Level—The security level for which the access parameters are defined. Select from the following options:
  - noAuthNoPriv—Uses a user name match for authentication.
  - AuthNoPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
  - AuthPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption based on the CBC-DES (DES-56) standard, in addition to authentication.

  If you select authNoPriv or authPriv for a group, the corresponding user must be configured with an authentication protocol and password, with privacy protocol and password, or both.
- Views
  - Read View Name—Read view name for the group.
  - Notify View Name—Notify view name for the group.
- Allow SNMP Sets—Select this check box if you want the SNMP agent to accept SNMP SET requests. If this check box is not selected, SET requests are rejected.

Note SNMP SET request access is implemented for very few objects.

Step 4 Click **OK** to save the information.

Step 5 Return to your originating procedure (NTP).

DLP-A587 Configure SNMPv3 Trap Destination

Purpose	This procedure provisions SNMPv3 trap destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP > SNMP V3 > Trap Destinations (V3)** tabs.

Step 2 Click **Create**.

Step 3 In the Configure SNMPv3 Trap dialog box, enter the following information:

- Target Address—Target to which the traps should be sent. Use an IPv4 or an IPv6 address.
- UDP Port—UDP port number that the host uses. Default value is 162.
- User Name—Specify the name of the user on the host that connects to the agent.
- Security Level—Select one of the following options:
  - noAuthNoPriv—Uses a user name match for authentication.
  - AuthNoPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
  - AuthPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption based on the CBC-DES (DES-56) standard, in addition to authentication.
- Filter Profile—Select this check box and enter the filter profile name. Traps are sent when you provide a filter profile name and create a notification filter. This field is optional and traps can also be sent without providing a filter profile and create a notification filter. For more information, see "DLP-A589 Create Notification Filters" task on page 22-98.
- Proxy Traps Only—If selected, forwards only proxy traps from the ENE. Traps from this node are not sent to the trap destination identified by this entry.
- Proxy Tags—Specify a list of tags. The tag list is needed on a GNE only if an ENE needs to send traps to the trap destination identified by this entry, and wants to use the GNE as the proxy.

Step 4 Click **OK** to save the information.

Step 5 Return to your originating procedure (NTP).

DLP-A588 Delete SNMPv3 Trap Destination

Purpose	This procedure deletes an SNMPv3 trap destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP> SNMPv3 > Trap Destination** tabs.

Step 2 In the Trap Destinations area, select the trap destination you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-A589 Create Notification Filters

Purpose	This procedure creates SNMPv3 notification filters. The notification filters are used to filter the notifications or traps, which should or should not be transmitted to the management target.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP > SNMP V3 > Notification Filters** tabs.

Step 2 Click **Create**.

Step 3 In the Create Notify dialog box, enter the following information:

- Filter Profile Name—Specify a name for the filter.
- Subtree OID—The MIB subtree which, when combined with the mask, defines the family of subtrees.
- Bit Mask—A family of view subtrees. Each bit in the bit mask corresponds to a sub-identifier of the subtree OID.
- View Type—Select the view type. Options are Include and Exclude. Type defines whether the family of subtrees that are defined by the subtree OID and the bit mask combination are included or excluded from the notification filter.

Step 4 Click **OK** to save the information.

Step 5 Return to your originating procedure (NTP).

DLP-A590 Manually Configure the SNMPv3 Proxy Forwarder Table

Purpose	This procedure creates an entry in the SNMPv3 Proxy Forwarder Table.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In network view, click **Provisioning > SNMPv3**.

Step 2 In the SNMPv3 Proxy Server area, complete the following:

- Select the GNE to be used as the SNMPv3 proxy server from the drop-down list.
- Select the **Enable IPv6 Target/Trap** check box if the nodes and the NMS stations are on an IPv6 network.

Step 3 In the SNMPv3 Proxy Forwarder Table area, click **Manual Create**.

Step 4 In the Manual Configuration of SNMPv3 Proxy Forwarder dialog box, enter the following information:

- Target IP Address—Target to which the request should be forwarded. Use an IPv4 or an IPv6 address.
- Context Engine ID—The context engine ID of the ENE to which the request is to be forwarded. The context engine ID should be the same as the context engine ID of the incoming request.
- Proxy Type—Type of SNMP request that needs to be forwarded. The options are Read and Write.
- Local User Details—The details of the local user who proxies on behalf of the ENE user.
  - User Name—Specify the name of the user on the host that connects to the agent.
  - Local Security Level—Select the security level of the incoming requests that are to be forwarded. The options are noAuthNoPriv, AuthNoPriv, and AuthPriv.
- Remote User Details—User to which the request is forwarded.
  - User Name—Specify the user name of the remote user.
  - Remote Security Level—Select the security level of the outgoing requests. The options are noAuthNoPriv, AuthNoPriv, and AuthPriv.
- Authentication
  - Protocol—Select the authentication algorithm you want to use. The options are NONE, MD5, and SHA.
  - Password—Enter the password if you select MD5 or SHA.
- Privacy—Enables the host to encrypt the contents of the message that is sent to the agent.
  - Protocol—Select NONE or DES as the privacy authentication algorithm.
  - Password—Enter the password if you select DES. The password should not exceed 64 characters.

Step 5 Click **OK** to save the information.

Step 6 Return to your originating procedure (NTP).

DLP-A591 Automatically Configure the SNMPv3 Proxy Forwarder Table

Purpose	This procedure creates an entry in the SNMPv3 Proxy Forwarder Table.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In network view, click **Provisioning > SNMPv3** tabs.

Step 2 In the SNMPv3 Proxy Server area, complete the following:

- Select the GNE to be used as the SNMPv3 proxy server from the drop-down list.
- Select the **Enable IPv6 Target/Trap** check box if the nodes and the NMS stations are on an IPv6 network.

Step 3 In the SNMPv3 Proxy Forwarder Table area, click **Auto Create**.

Step 4 In the Automatic Configuration of SNMPv3 Proxy Forwarder dialog box, enter the following information:

- Proxy Type—Select the type of proxies to be forwarded. The options are Read and Write.
- Security Level—Select the security level for the incoming requests that are to be forwarded. The options are:
  - noAuthNoPriv—Uses a username match for authentication.
  - AuthNoPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
  - AuthPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption based on the CBC-DES (DES-56) standard, in addition to authentication.
- Target Address List—Select the proxy destination.
- Local User Name—Select the user name from the list of users.

Note When you configure SNMPv3 Proxy Forwarder Table automatically, the default_group is used on the ENE. The default_group does not have write access. To enable write access and allow SNMP sets, you need to edit the default_group on ENE.

Step 5 Click **OK** to save the settings.

Step 6 Return to your originating procedure (NTP).

DLP-A592 Manually Configure the SNMPv3 Proxy Trap Forwarder Table

Purpose	This procedure creates an entry in the SNMPv3 Proxy Trap Forwarder Table.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In network view, click **Provisioning > SNMPv3** tabs.

Step 2 In the SNMPv3 Proxy Server area, complete the following:

- Select the GNE to be used as the SNMPv3 proxy server from the drop-down list.
- Select the **Enable IPv6 Target/Trap** check box if the nodes and the NMS stations are on an IPv6 network.

Step 3 In the SNMPv3 Proxy Trap Forwarder Table area, click **Manual Create**.

Step 4 In the Manual Configuration of SNMPv3 Proxy Trap Forwarder dialog box, enter the following information:

- Remote Trap Source—Select the IP address from which the traps are sent. If the IP address is not listed, enter the IP address manually.
- Context Engine ID—Specify the context engine ID of the ENE from which traps need to be forwarded. This field is automatically populated if the source of trap is selected. If the source of trap is not specified, you need to manually enter the context engine ID.
- Target Tag—Specify the tag name. The tag identifies the list of NMS that should receive the forwarded traps. Traps are forwarded to all GNE Trap destinations whose proxy tags list contains this tag.
- Remote User Details
  - User Name—Specify the user name.
  - Security Level—Select the security level for the user. The options are noAuthNoPriv, AuthNoPriv, and AuthPriv.
- Authentication—Select the authentication algorithm.
  - Protocol—Select the authentication algorithm you want to use. The options are NONE, MD5, and SHA. Default is None.
  - Password—Enter the password if you select MD5 or SHA.
- Privacy—Enables the host to encrypt the contents of the message that is sent to the agent.
  - Protocol—Select NONE or DES as the privacy authentication algorithm. Encryption is disabled if NONE is selected.
  - Password—Enter the password if you select DES. The password should not exceed 64 characters.

Step 5 Click **OK** to save the information.

Step 6 Return to your originating procedure (NTP).

DLP-A593 Automatically Configure the SNMPv3 Proxy Trap Forwarder Table

Purpose	This procedure creates an entry in the SNMPv3 Proxy Trap Forwarder Table automatically.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In network view, click **Provisioning > SNMPv3** tabs.

Step 2 In the SNMPv3 Proxy Server area, complete the following:

- Select the GNE to be used as the SNMPv3 proxy server from the drop-down list.
- Select the Enable IPv6 Target/Trap check box if the nodes and the NMS stations are on an IPv6 network.

Step 3 In the **SNMPv3 Proxy Trap Forwarder Table** area, click **Auto Create**.

Step 4 In the Automatic Configuration of SNMPv3 Proxy Trap Forwarder dialog box, enter the following information:

- Target Tag—Specify the tag name. The tag identifies the list of NMS that should receive the forwarded traps. All GNE Trap destinations that have this tag in their proxy tags list are chosen.
- Source of Trap—The list of ENEs whose traps are forwarded to the SNMPv3 Trap destinations that are identified by the Target Tag.

Step 5 Click **OK** to save the information.

Step 6 Return to your originating procedure (NTP).

DLP-A594 Provision a Dual Source, Single Destination Circuit

Purpose	This task provisions a dual source, single destination circuit on an ML-MR-10 card having the card port protection (CPP) enabled.
Tools/Equipment	Two ML-MR-10 cards must be installed at one end of the circuit.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note After you have selected the circuit properties in the Circuit Source dialog box according to the specific circuit creation procedure, you are ready to provision the circuit source.

Step 1 From the Node drop-down list, choose the node where the source will originate.

Step 2 From the Slot drop-down list, choose the slot containing the ML-MR-10 card where the circuit will originate.

Step 3 Choose the POS port from the Port drop-down list.

Step 4 From the STS drop-down list, choose the source STS.

Note If the ML-MR-10 card is in automatic mode, the STS drop-down list will be unavailable.

Note Both the ML-MR-10 cards must be unique cards on the same chassis.

Step 5 Select the **Use Secondary Source** check box and repeat Steps 1 through 4 to define the secondary source. If you do not need to create a secondary source, continue with Step 6.

Step 6 Click **Next**.

Step 7 From the Node drop-down list, choose the destination (termination) node.

Step 8 Repeat Steps 1 through 4 to define the destination.

Step 9 If you are creating a dual source, dual destination circuit, create a dual/secondary destination circuit; for example, a path protection bridge/selector circuit exit point in a multivendor path protection configuration, click **Use Secondary Destination** and repeat Steps 7 through 8 to define the secondary destination.

Step 10 Click **Next**.

Step 11 Return to your originating procedure (NTP).

DLP-A595 Provision Card Mode for CE-MR-10 Card

Purpose	This task provisions the card mode for the CE-MR-10 card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note When you change the provisioning mode, the card should not have any circuits configured on it.

Step 1 In the node view, double-click the CE-MR-10 card.

Step 2 Click the **Provisioning > Card** tabs.

Step 3 In the Mode drop-down list, select one of the following:

- MANUAL—Allows the selection of STS during circuit creation.
- AUTOMATIC—Prevents the selection of STS during circuit creation.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A596 Provision the Ethernet Port of the ML-Series Card

Purpose	This task provisions the Ethernet ports of the ML-Series card to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, double-click the ML-Series card where you want to provision the Ethernet port.

Step 2 Click the **Provisioning > Ether Ports** tabs.
The Ether Ports pane appears.

Step 3 In the Ether Ports pane complete the following:

- Port—Displays a fixed number identifier for the specific port.
- Port Name—Enter a 12 character alphanumeric identifier for the port.

Note Circuit table displays port name of the POS port and not the Ethernet port. For information on viewing the circuit table, see DLP-A416 View Circuit Information, page 21-2.

- Admin State—Displays the state of the port. Allowed values are UP and DOWN. For the UP value to appear, the Ethernet port must be both administratively active and have a SONET/SDH circuit provisioned.
- PSAS (Pre Service Alarm Suppress)—Check the PSAS check box to enable alarm suppression on the port for a time interval set in the Soak Time column. Uncheck the PSAS checkbox to disable alarm suppression.
- Soak Time—Enter a desired soak time in hours and minutes (hh:mm) format. Use this column when you have checked PSAS to suppress alarms. Once the port detects a signal, the countdown begins for the designated soak time. Soak time hours can be set from 0 to 48. Soak time minutes can be set from 0 to 45 in 15 minute increments.
- Link State—Displays the status between signaling points at port and attached device. Allowed values are UP or DOWN.
- MTU (Maximum Transmission Unit)— Displays the largest acceptable packet size configured for the port.

- Speed—Displays the Ethernet port transmission speed.
- Duplex—Displays the duplex mode setting for the port.
- Flow Control—Displays the flow control mode negotiated with peer device.
- Optics— Displays the Small form-factor pluggable (SFP) physical media type.

Step 4 Click **Apply.**

Step 5 Reprovisioning an Ethernet port on the ML-Series card does not reset the ethernet statistics for that port. The Ethernet Statistics must be refreshed. To do so, do the following:

a. Click the **Performance** > **Ether Ports** > **Statistics** tabs.

b. Click **Refresh.**

Step 6 Return to your originating procedure (NTP).

DLP-A597 Provision the POS Port of the ML-Series Card

Purpose	This task provisions the POS ports of the ML-Series card to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, double-click the ML-Series card where you want to provision the POS port.

Step 2 Click the **Provisioning** > **POS Ports** tabs.
The POS Port pane appears.

Step 3 For each port, provision the following parameters:

- Port—Displays a fixed number identifier for the specific port.
- Port Name—Enter a 12 character alphanumeric identifier for the port.

Note Circuit table displays port name of the POS port and not the Ethernet port. For information on viewing the circuit table, see DLP-A416 View Circuit Information, page 21-2.

- Admin State—Displays the state of the port. Allowed values are UP or DOWN. For the UP value to appear, a POS port must be both administratively active and have a SONET/SDH circuit provisioned.
- PSAS—Check the PSAS checkbox enable alarm suppression on the port for a time interval set in the Soak Time column. Uncheck the PSAS checkbox to disable alarm suppression.
- Soak Time—Enter a desired soak time in hours and minutes (hh:mm) format. Use this column when you have checked PSAS to suppress alarms. Once the port detects a signal, the countdown begins for the designated soak time. Soak time hours can be set from 0 to 48. Soak time minutes can be set from 0 to 45 in 15 minute increments.
- Link State—Displays the status between signaling points at port and attached device. Allowed values are UP or DOWN.

- MTU—Displays the largest acceptable packet size configured for the port.
- Framing Type— Displays the POS framing mechanism employed on the port.

Step 4 Click **Apply.**

Step 5 Reprovisioning a POS port on the ML-Series card does not reset the POS statistics for that port. The POS Statistics must be refreshed. To do so, do the following:

a. Click the **Performance > POS Ports > Statistics** tabs.

b. Click **Refresh.**

Step 6 Return to your originating procedure (NTP).

DLP-A599 Repair Server Trails

Purpose	This procedure repairs Server Trail terminations in cases where IP address changes for a node connected by a Server Trail link.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-60
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The Server Trail Repair wizard can only fix the IP address changes and cannot fix Server Trail terminations when you migrate from IPv4 to IPv6 addresses.

Note The Server Trail Repair wizard cannot repair the Server Trails when IP address of nodes on both ends of the Server Trail are changed.

Note When Server Trails are created on an IPv4 or IPv6 node and the IP address of the node changes, make sure that the Server Trail Repair wizard is launched on the IP address of the node that changed. For example, if the IP address of Server Trails created on an IPv4 node changes, run the Server Trail Repair wizard on the IPv4 node and not on the IPv6 node.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will repair Server Trails. If you are already logged in, continue with Step 2.

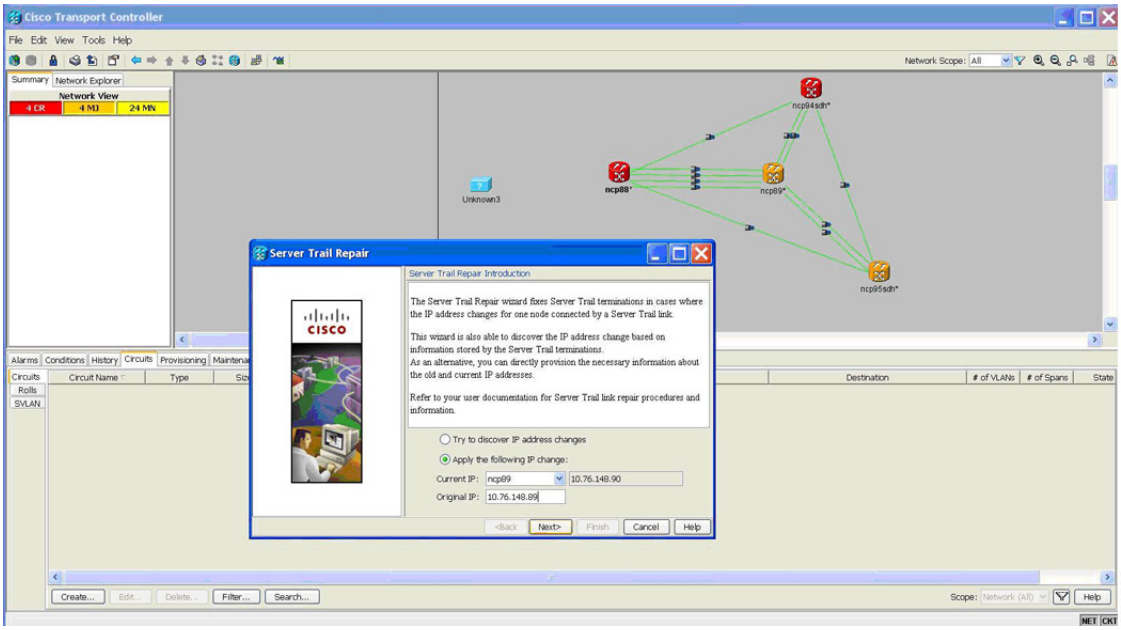
Note The Server Trail Repair wizard works only when nodes at both ends of the Server Trail are added in the CTC. If CTC is launched after the IP address is changed or if the node on any of the sides is not discovered automatically, then the node has to be added manually into the CTC.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Choose the **Tools > Links > Repair Server Trails** option from the tool bar.
The **Server Trail Repair** wizard appears.

Step 4 Specify the changed IP address.
The **Server Trail Repair** window provides the following options, as shown in Figure 22-15:

Figure 22-15 Server Trail Repair Wizard—Server Trail Repair Introduction



- **Try to discover IP address changes**—The wizard searches and displays the list of changed IP addresses.

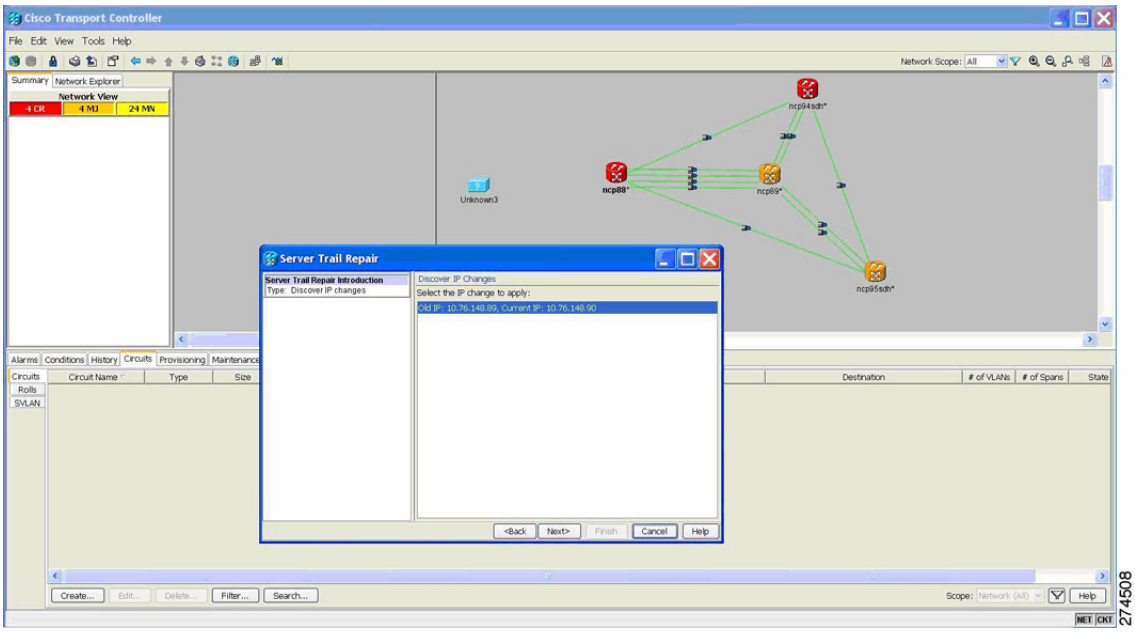
  Note The wizard can discover multiple IP address changes. However, the wizard can repair only one IP address change at a time. To repair multiple IP address changes, run the **Server Trail Repair** wizard multiple times.

- **Apply the following IP change**—Allows you to specify the changed IP address.

  Select the node with changed IP address and specify old IP address as Original IP Address. The wizard automatically displays the current IP address.

Step 5 Click **Next**.
If you selected "Try to discover IP address changes" option in Step 4, then the wizard displays all the IP address changes that will be fixed, as shown in Figure 22-16. Click **Next**.

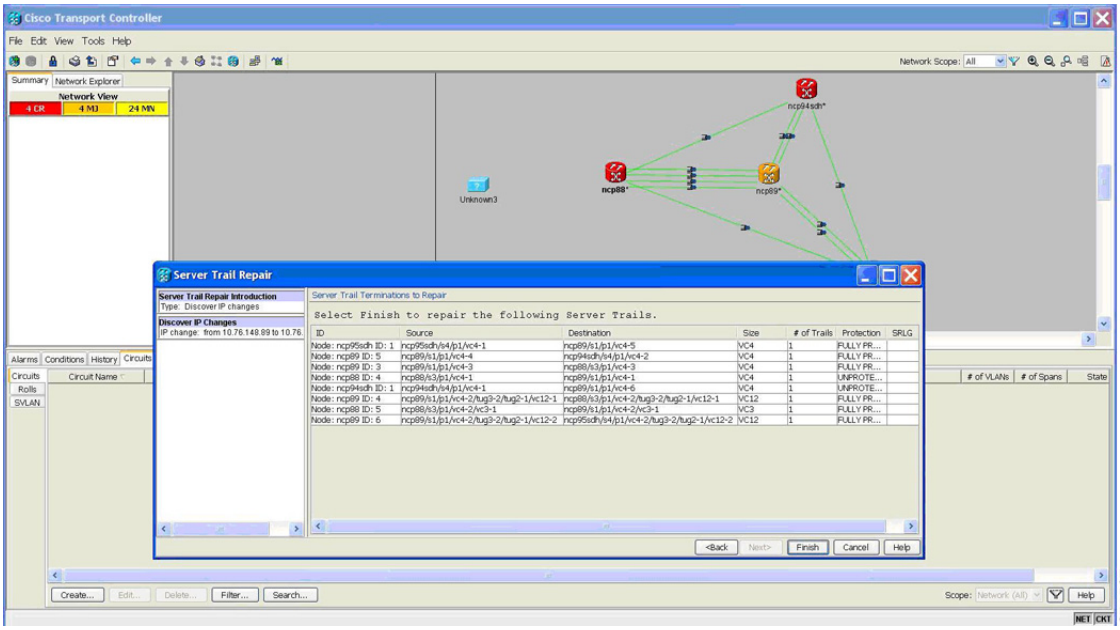
Figure 22-16 Server Trail Repair Wizard—Discover IP Change



If you selected "Apply the following IP change" option in Step 4, continue with Step 6.

Step 6 The Server Trail Terminations to Repair window appears, as shown in Figure 22-17. Click **Finish** to repair the Server Trails.

Figure 22-17 Server Trail Repair Wizard—Server Trail Terminations to Repair



Stop. You have completed this procedure.

CHAPTER 23

DLPs A600 to A699

Note The terms “Unidirectional Path Switched Ring” and “UPSR” may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as “Path Protected Mesh Network” and “PPMN,” refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

DLP-A600 Perform BLSR Lockout

Purpose	This task performs a BLSR lockout. If you have BLSR provisioned, you must perform this task before beginning the upgrade.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-A108 Back Up the Database, page 15-5
Required/As Needed	Required for BLSR only
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Maintenance

Note During the activation, BLSR spans are not protected. You must leave the BLSR in the lockout state until you have finished activating all nodes in the ring. Ensure that the lockout is removed after activation.

Note To prevent ring or span switching, perform the lockout on both the east and west spans of each node.

Step 1 According to local site practice, complete the “NTP-A108 Back Up the Database” procedure on page 15-5 for all the nodes in the ring.

Step 2 Complete the “DLP-A60 Log into CTC” task on page 17-60 at the node where you will perform BLSR lockout. If you are already logged in, continue with Step 3.

Step 3 In node view, click the **Maintenance** tab, then click **BLSR**.

Step 4 For each of the line cards, perform the following steps:

a. Next to the card row, click the **East Switch** column to access the drop-down list.

b. From the menu options, choose **Lockout Protect**.

c. Click **Apply**.

d. In the same row, click the **West Switch** column to access the drop-down list.

e. From the menu options, choose **Lockout Protect**.

f. Click **Apply**.

Note Ignore any Default K alarms that occur on the protect synchronous transport signal (STS) time slots during this lockout period.

Note Certain BLSR or Multiservice Switching Platform (MSSP)-related alarms might be raised following activation of the first node in the ring. The following alarms, if raised, are normal, and should not cause concern. They clear upon completion of the upgrade, after all nodes have been activated.

- BLSR-OOSYNC (MN)
- RING-MISMATCH (MJ)
- APSCDFLTK (MN)
- BLSR-RESYNC (NA)

Step 5 Return to your originating procedure (NTP).

DLP-A601 Remove BLSR Lockout

Purpose	This task removes a BLSR lockout.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-A600 Perform BLSR Lockout, page 23-1
Required/As Needed	Required for BLSR
Onsite/Remote	Onsite or remote (but in the presence of the workstation)
Security Level	Maintenance

Step 1 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 15-5 for all the nodes in the ring.

Step 2 Complete the "DLP-A60 Log into CTC" task on page 17-60 at the node where you will remove BLSR lockout. If you are already logged in, continue with Step 3.

Step 3 In node view, click the **Maintenance** tab, then click **BLSR**.

Step 4 For each of the line cards, perform the following steps:

a. Next to the card row, click the **West Switch** column to access the drop-down list.

b. From the shortcut menu, choose **Clear**.

c. Click **Apply**.

Note When removing a lockout, be sure to apply your changes each time you choose the Clear option. If you try to select Clear for more than one lockout at a time, you risk traffic loss on the first ring switch.

d. In the same row, click the **East Switch** column to access the drop-down list.

e. From the shortcut menu, choose **Clear**.

f. Click **Apply**.

Step 5 Repeat this task as many times as necessary to remove all BLSR span lockouts on the nodes.

Step 6 Return to your originating procedure (NTP).

APPENDIX A

CTC Information and Shortcuts

Note The terms “Unidirectional Path Switched Ring” and “UPSR” may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as “Path Protected Mesh Network” and “PPMN,” refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This appendix describes the Cisco Transport Controller (CTC) views, menus and tool options, shortcuts, and table display options. This appendix also describes the shelf inventory data presented in CTC. For more information about CTC, refer to the *Cisco ONS 15454 Reference Manual*.

Note If network discovery is enabled on the node, CTC searches each node in the network for more recent versions of the CTC software. If a more recent version is discovered, CTC gives you the option of downloading the Java archive (JAR) files to your PC.

Display Node, Card, and Network Views

CTC provides three views of the ONS 15454 and the ONS network:

- Node view appears when you first log into an ONS 15454. This view shows a graphic of the ONS 15454 shelf and provides access to tabs and subtabs that you use to manage the node.
- Card view provides access to individual ONS 15454 cards. This view provides a graphic of the card and provides access to tabs and subtabs that you use to manage the card.
- Network view shows all the nodes in a ring. A Superuser can set up this feature so each user will see the same network view, or the user can create a custom view with maps. This view provides access to tabs and subtabs that you use to manage the network. Network view can contain domains. A domain is used to isolate nodes or groups of nodes for easier maintenance. Double-clicking a domain shows all the nodes in the domain; nodes connected to the domain are grayed out.

Table A-1 lists different actions for changing CTC views.

Table A-1 Change CTC Views

To display:	Perform one of the following:
Node view	• Log into a node; node view is the default view. • In network view, double-click a node icon, or right-click the node and choose **Open Node** from the shortcut menu. • In network view, single-click a node icon, then choose **Go To Selected Object View** from the View menu. • From the View menu, choose **Go To Other Node**, then choose the node you want from the shortcut menu. • Use the arrows on the CTC toolbar to navigate up or down views. For example, in network view, click a node, then click the down arrow.
Home view (node view of the first node you logged into in a network)	• From the CTC View menu, choose **Go To Home View**.
Network view	• In node view, click the up arrow or the Network View tool on the CTC toolbar. • From the View menu, choose **Go To Network View**.
Card view	• In node view, double-click a card or right-click the card and choose **Open Card**. • In node view, single-click a card icon, then choose **Go To Selected Object View** from the View menu. • Use the arrows on the CTC toolbar to navigate up or down views. For example, in node view, click a card, then click the down arrow.

Table A-2 lists the node icons on the network view map.

Table A-2 Description of Node Icons on Network View Map

Node Name	Icon	Description
SONET Hybrid OADM Hybrid line amplifier Hybrid terminal Passive hybrid terminal Amplified TDM		A SONET, hybrid, or amplified time-division multiplexing (TDM) node icon is represented as a cylinder with crossed arrows. • A SONET or SDH node can include OC-N cards, electrical cards, cross-connects, Storage Access Management (SAM) cards, and Ethernet cards. • A hybrid optical add/drop multiplexing (OADM) node contains at least one AD-xC-xx.x card or one AD-xB-xx.x card and two TCC2/TCC2P cards. TDM cards can be installed in any available slot. • A hybrid line amplifier node contains amplifiers and both TDM and dense wavelength division multiplexing (DWDM) cards. • A hybrid terminal node contains at least one 32MUX-O card, one 32DMX-O card, amplifiers, two TCC2/TCC2P cards, and TDM cards. Alternatively, the node may contain at least one 40-MUX-C, one 40-DMX-C card, amplifiers, two TCC2/TCC2P cards, and TDM cards. • A passive hybrid terminal node has the same equipment as the hybrid terminal node, but does not contain amplifiers. • An amplified TDM node is a node that increases the span length between two ONS 15454 nodes that contain TDM cards and optical amplifiers. Amplified TDM nodes contain either OPT-BST amplifiers or AD-1C-xx.x cards. For DWDM node information, refer to the *Cisco ONS 15454 DWDM Reference Manual*.
Hub		A DWDM hub node icon is represented as a three-dimensional cylinder with amplifiers. A hub node contains at least two 32-channel demultiplexers and two 32-channel multiplexers. The hub node may alternatively contain at least two 40-DMX-C cards and two 40-MUX-C cards. No OADM cards are provisioned. For DWDM node information, refer to the *Cisco ONS 15454 DWDM Reference Manual*.
OADM		A DWDM OADM node icon is represented as a three-dimensional cylinder with arrows. An OADM node contains at least one channel OADM (AD-xC) or one band OADM (AD-xB). No 32MUX-O, 32DMX-O, 32DMX, 40-MUX-C, or 40-DMX-C cards are provisioned. For DWDM node information, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Table A-2 Description of Node Icons on Network View Map (continued)

Node Name	Icon	Description
ROADM		A reconfigurable OADM (ROADM) node icon is represented as a three-dimensional cylinder with two amplifier symbols that have arrows between them. An ROADM node contains at least one 32WSS or 40-WSS-C card. A single-slot 32DMX or double-slot 32DMX-O can be installed, but is not required. Alternatively, a 40-DMX-C can be installed, but is not required. Transponders (TXPs) and muxponders (MXPs) can be installed in Slots 6 and 12. If amplification is not used, TXPs or MXPs can be installed in Slots 1 and 17. If OPT-BST cards are not installed, OSC-CSM cards are installed in Slots 2 and 16 and Slots 8 and 10 are empty.
Terminal		A terminal node is represented as a three-dimensional cylinder with a white rectangle in the center. • A terminal node contains one 32DMX or 32DMX-O card and one 32-MUX-O card. Alternatively, a terminal node contains one 40-DMX-C card and one 40-MUX-C card. No OADM cards are provisioned. • A flexible terminal node contains a series of OADM and amplifier cards. For DWDM node information, refer to the *Cisco ONS 15454 DWDM Reference Manual*.
Line Amplifier OSC regeneration		Line amplifier and optical service channel (OSC) regeneration nodes are represented as a three-dimensional cylinder with one arrow pointing west and another arrow pointing east. • A line amplifier node only has OPT-PRE or OPT-BST amplifiers provisioned. • An OSC regeneration node contains two OSC-CSM cards. For DWDM node information, refer to the *Cisco ONS 15454 DWDM Reference Manual*.
Unknown		An unknown DWDM node icon is represented as a three-dimensional cylinder with one arrow pointing north. An unknown node means that the provisioned cards do not allow the node to fit any of the defined DWDM node categories. For DWDM node information, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Manage the CTC Window

Different navigational methods are available within the CTC window to access views and perform management actions. You can double-click and right-click objects in the graphic area and move the mouse over nodes, cards, and ports to view popup status information.

CTC Menu and Toolbar Options

The CTC window menu bar and toolbar provide primary CTC functions. Table A-3 shows the actions that are available from the CTC menu and toolbar.

Table A-3 CTC Menu and Toolbar Options

Menu	Menu Option	Toolbar	Description
File	Add Node		Adds a node to the current session. See the "DLP-A62 Add a Node to the Current Session or Login Group" task on page 17-64.
	Delete Selected Node		Deletes a node from the current session.
	Lock CTC		Locks CTC without closing the CTC session. A user name and password are required to open CTC.
	Print		Prints CTC data. See the "DLP-A531 Print CTC Data" task on page 22-32.
	Export		Exports CTC data. See the "DLP-A532 Export CTC Data" task on page 22-34.
	Exit	—	Closes the CTC session.
Edit	Preferences		Displays the Preferences dialog box, which shows the following tabs: • General—Allows you to change event defaults and manage preferences. • Login Node Groups—Allows you to create login node groups. See the "DLP-A61 Create Login Node Groups" task on page 17-63. • Map—Allows you to customize the network view. See the "DLP-A145 Change the Network View Background Color" task on page 18-18 and the "DLP-A268 Apply a Custom Network View Background Map" task on page 19-52. • Circuit—Allows you to change the color of circuit spans. See the "DLP-A232 Change Active and Standby Span Color" task on page 19-21. • Firewall—Sets the Internet Inter-ORB Protocol (IIOP) listener ports and the Secure Sockets Layer Inter-ORB Protocol (SSLIOP) for access to the ONS 15454 through a firewall. See the "NTP-A27 Set Up the ONS 15454 for Firewall Access" procedure on page 4-10. • JRE—Allows you to select another Java Runtime Environment (JRE) version. See the "DLP-A431 Change the JRE Version" task on page 21-9.

Table A-3 CTC Menu and Toolbar Options (continued)

Menu	Menu Option	Toolbar	Description
View	Go To Previous View		Displays the previous CTC view.
	Go To Next View		Displays the next CTC view. Available only after you navigate to a previous view. Go to Previous View and Go to Next View are similar to forward and backward navigation in a web browser.
	Go To Parent View		References the CTC view hierarchy: network view, node view, and card view. In card view, this command displays the node view; in node view, the command displays network view. Not available in network view.
	Go To Selected Object View		Displays the object selected in the CTC window.
	Go To Home View		Displays the login node in node view.
	Go To Network View		Displays the network view.
	Go To Other Node		Displays a dialog box allowing you to type in the node name or IP address of a a network node that you want to view.
	Show Status Bar	—	Click this item to display or hide the status bar at the bottom of the CTC window.
	Show Tool Bar	—	Click this item to display or hide the CTC toolbar.
—	—		Zooms out the network view area (toolbar only).
—	—		Zooms in the network view area (toolbar only).
—	—		Zooms in a selected network view area (toolbar only).

Table A-3 CTC Menu and Toolbar Options (continued)

Menu	Menu Option	Toolbar	Description
Tools	Circuits	—	Displays the following options: • Repair Circuits—Repairs incomplete circuits following replacement of the ONS 15454 alarm interface panel (AIP). Refer to the *Cisco ONS 15454 Troubleshooting Guide* for more information. • Reconfigure Circuits—Allows you to reconfigure circuits. See the "NTP-A298 Reconfigure Circuits" procedure on page 7-12 for more information. • Set Path Selector Attributes—Allows you to edit path protection circuit path selector attributes. See the "DLP-A233 Edit Path Protection Circuit Path Selectors" task on page 19-22. • Set Circuit State—Allows you to change a circuit state. See the "DLP-A230 Change a Circuit Service State" task on page 19-19. • Roll Circuit—Allows you to reroute live traffic without interrupting service. See the "NTP-A334 Bridge and Roll Traffic" section on page 7-11. • Delete Rolls—Removes rolls that are not deleted by CTC after a roll has been completed. See the "DLP-A468 Delete a Roll" task on page 21-59. • Upgrade OCHNC—(ONS 15454 only) Upgrades OCHNCs created in earlier software releases to OCHCCs. Refer to the *Cisco ONS 15454 DWDM Procedure Guide* for more information. • Show RPR Circuit Ring—Shows the RPR ring for the circuit selected on the Circuits window. See the "NTP-A348 Display IEEE 802.17 RPR Circuits" procedure on page 7-14.

Table A-3 CTC Menu and Toolbar Options (continued)

Menu	Menu Option	Toolbar	Description
Tools	Overhead Circuits	—	Displays the Repair IP Tunnels option, which fixes circuits that are in the INCOMPLETE state as a result of node IP address changes. See the "DLP-A336 Repair an IP Tunnel" task on page 20-24.
	Topology Upgrade	—	Displays the following options: • Convert Path Protection to BLSR—Converts a path protection configuration to a bidirectional line switch ring (BLSR). See the "NTP-A267 Convert a Path Protection Configuration to a Two-Fiber BLSR Automatically" procedure on page 13-13. • Convert Unprotected to Path Protection—Converts a point-to-point or linear add/drop multiplexer (ADM) to a path protection configuration. See the "NTP-A342 Convert a Point-to-Point or Linear ADM to a Path Protection Configuration Automatically" procedure on page 13-11.
	Manage VLANs	—	Displays a list of VLANs that have been created and allows you to create and delete VLANS. See the "NTP-A325 Manage VLANs" procedure on page 7-13.
	Open TL1 Connection		Displays the TL1 session dialog box so you can create a TL1 session to a specific node. Refer to the *Cisco ONS SONET TL1 Command Guide* and the *Cisco ONS SONET TL1 Reference Guide*.
	Open IOS Connection		Displays the Cisco IOS command line interface dialog box if a Cisco IOS capable card (any ML-Series card) is installed in the node. Refer to the *Ethernet Card Software Feature and Configuration Guide*.
	Update CTC	—	Allows you to update CTC to a newer version if a newer version was found during network discovery.
Help	Contents and Index	—	Displays the online help window.
	User Manuals	—	Displays the Cisco ONS 15454 documentation.
	About CTC	—	Displays the software version and the nodes in the CTC session.
—	Network Scope	—	Displays the selected network scope. The network scope drop-down list has three options: DWDM, TDM, or All. If you choose DWDM, DWDM and hybrid nodes appear on the network view map. If you choose TDM, TDM and hybrid nodes appear on the network view map. If you choose All, every node on the network appears on the network view map.
—	Link Filter		Opens the Link Filter dialog box, which allows you to choose which link classes appear on the non-detail network map. The available classes vary according to the selected network scope. • ALL—DCC, GCC, OTS, PPC, server trail • DWDM—GCC, OTS, PPC • TDM—DCC, PPC, server trail

Table A-3 CTC Menu and Toolbar Options (continued)

Menu	Menu Option	Toolbar	Description
—	—		Opens the Collapse/Expand Links dialog box, which allows you to globally expand or consolidate network view links based on link type.
—	—	 	Opens the CTC Alerts dialog box, which shows the status of certain CTC background tasks. When the CTC Alerts toolbar icon contains a red triangle, unread notifications exist. When there are no unread notifications, the CTC Alerts toolbar icon contains a gray triangle. Notifications include: • Network disconnection • Send-PDIP inconsistency—CTC discovers a new node that does not have a SEND-PDIP setting consistent with the login node. • Circuit deletion status—Reports when the circuit deletion process completes if you choose "Notify when complete" as described in the "NTP-A278 Modify and Delete Overhead Circuits and Server Trails" procedure on page 7-5. The CTC Alerts window always reports circuit deletion errors. • Conditions retrieval error • Software download failure You can save a notification by clicking the Save button in the CTC Alerts dialog box and navigating to the directory where you want to save the text file. By default, the CTC Alerts dialog box opens automatically. To disable automatic popup, see the "DLP-A327 Configure the CTC Alerts Dialog Box for Automatic Popup" task on page 20-16.

CTC Mouse Options

In addition to the CTC menu bar and toolbar, you can invoke actions by double-clicking CTC window items with your mouse, or by right-clicking an item and selecting actions from shortcut menus. Table A-4 lists the CTC window mouse shortcuts.

Table A-4 CTC Window Mouse Shortcuts

Technique	Description
Double-click	• Node in network view—Displays the node view. • Domain in network view—Displays the domain view. • Card in node view—Displays the card view. • Alarm/Event—Displays the object that raised the alarm or event. • Circuits—Displays the Edit Circuit window.
Right-click	• Network view graphic area—Displays a menu that you can use to create a new domain; change the position and zoom level of the graphic image; save the map layout (if you have a Superuser security level); reset the default layout of the network view; set, change, or remove the background image and color; collapse and expand links; and save or reset the node position. • Domain in network view—Displays a menu that you can use to open a domain, show the domain overview, rename the domain, and delete the domain. • Node in network view—Displays a menu that you can use to open the node, reset the node icon position to the longitude and latitude set on the Provisioning > General tab, delete the node, fix the node position for auto layout, provision circuits, provision channels, and update circuits or channels with a new node. • Span in network view—Displays a menu that you can use to view information about the span's source and destination ports, the protection scheme, and the optical or electrical level. You can display the Circuits on Spans dialog box, which displays additional span information and allows you to perform path protection switching. If a BLSR is provisioned, you can display the PCA circuits. You can also perform span upgrades from this menu, and expand and collapse links. • Card in node view—Displays a menu that you can use to open, delete, reset, and change cards. The card that you choose determines the commands that appear. • Card in card view—Displays a menu that you can use to reset the card, or go to the parent view (node view). • Empty slot in node view—Displays a menu with cards that you can choose to preprovision the slot.

Table A-4 CTC Window Mouse Shortcuts (continued)

Technique	Description
Move mouse cursor	• Over node in network view—Displays a summary of node alarms and provides a warning if the node icon has been moved out of the map range. • Over span in network view—Displays circuit (node, slot, port) bandwidth and protection information. For DWDM spans, the optical direction and optical ring ID appear. If the span terminates on the trunk port of a TXP/MXP, the associated DWDM wavelength also appears. • Over card in node view—Displays card type, card status, and alarm profile status. For DWDM cards, the number of bands or channels also appear, depending on the card type. • Over domain in network view—Displays domain name and the number of nodes in the domain. • Over card port in node view—Displays port number and/or name, port service state, and alarm profile status. • Over card port in card view—Displays port name (if applicable), port service state, protection status (if applicable), and alarm profile status. For DWDM cards, the port number is labeled as channel, band, or line depending on the card type along with the port state and alarm profile status.

Node View Shortcuts

Table A-5 shows actions on ONS 15454 cards that you can perform by moving your mouse over the CTC window.

Table A-5 Node View Card-Related Shortcuts

Action	Shortcut
Display card information	In node view, move your mouse over cards in the graphic to display tooltips with the card type, card status (active or standby), the highest level of alarm (if any), and the alarm profile used by the card.
Open, reset, or delete a card	In node view, right-click a card. Choose **Open Card** to display the card in card view, **Delete Card** to delete it, or **Reset Card** to reset the card.
Preprovision a slot	In node view, right-click an empty slot. Choose the card type for which you want to provision the slot from the shortcut menu.
Change a card	In node view, right-click an OC-N card or a DS3 card, and choose **Change Card**. In the Change Card dialog box, choose the card type. Change Card retains all card provisioning, including data communications channel (DCC) terminations, protection, circuits, and ring.
Change view	Right-click on the area outside the node to display a menu that allows you to return to the parent view.

Network View Shortcuts

Right-click the network view graphic area or a node, span, or domain to display shortcut menus. Table A-6 lists the actions that are available from the network view.

Table A-6 Network Management Tasks in Network View

Action	Task
Open a node	Any of the following: • Double-click a node icon. • Right-click a node icon and choose **Open Node** from the shortcut menu. • Click a node and choose **Go To Selected Object View** from the View menu. • From the View menu, choose **Go To Other Node**. Choose a node from the Select Node dialog box. • Double-click a node alarm or event in the Alarms or History tab.
Move a node icon	Press the **Ctrl** key and the left mouse button simultaneously and drag the node icon to a new location.
Consolidate links	Right-click on a link and choose **Consolidate/Expand** from the shortcut menu. For more detailed instructions, refer to Chapter 11, "Change Node Settings."
Reset node icon position	Right-click a node and choose **Reset Node Position** from the shortcut menu. The node icon moves to the position defined by the longitude and latitude fields on the Provisioning > General tab in node view.
Provision a circuit	Right-click a node. From the shortcut menu, choose **Provision Circuit To** and choose the node where you want to provision the circuit. For circuit creation procedures, see Chapter 6, "Create Circuits and VT Tunnels."
Update circuits with new node	Right-click a node and choose **Update Circuits With New Node** from the shortcut menu. Use this command when you add a new node and want to pass circuits through it.
Display a link end point	Right-click a span. From the shortcut menu, choose **Go To** [<node> | <port> | <slot>] for the drop port you want to view. CTC displays the card in card view.
Display span properties	Do any of the following: • Move the mouse over a span; the properties appear near the span. • Click a span; the properties appear in the upper left corner of the window. • Right-click a span; the properties appear at the top of the shortcut menu.
Perform a path protection switch for an entire span	Right-click a network span and click **Circuits**. In the Circuits on Span dialog box, switch options appear in the Path Protection Span Switching field.
Display DWDM span properties	Right-click a DWDM network span and click **Circuits**. The optical channel network connection (OCHNC), optical direction, and circuit appear.

Table A-6 Network Management Tasks in Network View (continued)

Action	Task
Upgrade a span	Right-click a span and choose **Upgrade Span** from the shortcut menu. **Note** For detailed span upgrade information and instructions, see Chapter 12, "Upgrade Cards and Spans."
Upgrade terminal to linear	Right-click a span and choose **Upgrade Protection > Terminal to Linear** from the shortcut menu. See the "NTP-A335 Convert a 1+1 Point-to-Point to a Linear ADM Automatically" task on page 13-2.

Table Display Options

Right-clicking a table column displays a menu. Table A-7 shows table display options, which include rearranging or hiding CTC table columns and sorting table columns by primary or secondary keys.

Table A-7 Table Display Options

Task	Click	Right-Click Shortcut Menu
Resize column	Click while dragging the column separator to the right or left.	—
Rearrange column order	Click while dragging the column header to the right or left.	—
Reset column order	—	Choose **Reset Columns Order/Visibility**.
Hide column	—	Choose **Hide Column**.
Show column	—	Choose **Show Column >** *column_name*.
Display all hidden columns	—	Choose **Reset Columns Order/Visibility**.
Sort table (primary)	Click a column header; each click changes sort order (ascending or descending).	Choose **Sort Column**.
Sort table (secondary sorting keys)	Press the **Shift** key and simultaneously click the column header.	Choose **Sort Column (incremental)**.
Reset sorting	—	Choose **Reset Sorting**.
View table row count	—	View the number after **Row count=**; it is the last item on the shortcut menu.

Equipment Inventory

In node view, the Inventory tab displays information about the ONS 15454 equipment, including:

- Delete button—After highlighting a card with your mouse, use this button to delete the card from node view.
- Reset button—After highlighting a card with your mouse, use this button to reset the card.

- Location—Identifies where the equipment is installed, either chassis or slot number.
- Eqpt Type—Displays the type of equipment but not the specific card name, for example, OC-12 or DS-1.
- Actual Eqpt Type—Displays the specific card name, for example, OC12 IR/STM4 SH 1310.
- Admin State—Changes the card service state unless network conditions prevent the change. For more information about card states, refer to the "Administrative and Service States" appendix of the *Cisco ONS 15454 Reference Manual.*
  - IS—Puts the card in the In-Service and Normal (IS-NR) service state.
  - OOS,MA—Puts the card in the Out-of-Service and Autonomous, Maintenance (OOS-AU,MT) service state.
- Service State—Displays the current card service state, which is an autonomously generated state that gives the overall condition of the card. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State. For more information about card states, refer to the "Administrative and Service States" appendix of the *Cisco ONS 15454 Reference Manual.*
- HW Part #—Displays the hardware part number; this number is printed on the top of the card or equipment piece.
- HW Rev—Displays the hardware revision number.
- Serial #—Displays the equipment serial number; this number is unique to each card.
- CLEI Code—Displays the Common Language Equipment Identifier code.
- Bootroom Rev—Displays the boot read-only memory (ROM) revision number.
- Product ID—Displays the manufacturing product identifier for a hardware component, such as a fan tray, chassis, or card. The Product ID column displays "N/A" for equipment existing before Software Release 4.6.
- Version ID—Displays the manufacturing version identifier for a fan tray, chassis, or card. The Version ID column displays "N/A" for equipment existing before Software Release 4.6.