Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide

Product and Documentation Release 8.5.4
Last Updated: July 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: 78-18130-01

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco’s installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco’s written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.

- Move the equipment to one side or the other of the television or radio.

- Move the equipment farther away from the television or radio.

- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide, Release 8.5.4

CONTENTS

APPENDIX A

INDEX

FIGURES

TABLES

PROCEDURES

TASKS

Preface

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
- Document Objectives
- Audience
- Document Organization
- Related Documentation
- Document Conventions
- Obtaining Optical Networking Information
- Obtaining Documentation and Submitting a Service Request

Revision History

The following Revision History tables record technical changes, additions, and corrections to this document. The table shows the date of the change and summary of the change.

Date	Notes
March 2008	• Added a Warning under Before You Begin section in Install the Cisco ONS 15310-CL chapter. • Added a Note under NTP-C2 Install the Shelf Assembly section in Install the Cisco ONS 15310-CL chapter. • Added a Warning under NTP-C3 Install the Power and Ground section in Install the Cisco ONS 15310-CL chapter. • Added a Warning under NTP-C4 Install an Ethernet Card section in Install the Cisco ONS 15310-CL chapter. • Added a Warning under section NTP-C5 Install Wires to Alarm, Timing, LAN, Craft, and UDC Pin Connections section in Install the Cisco ONS 15310-CL chapter. • Added a Warning under the NTP-C6 Install the Electrical Cables section in Install the Cisco ONS 15310-CL chapter. • Added a Warning under the NTP-C7 Install and Remove SFPs section in Install the Cisco ONS 15310-CL chapter. • Added a Warning under Before You Begin section in Install the Cisco ONS 15310-MA chapter. • Added a Note under NTP-C150 Install the Shelf Assembly section in Install the Cisco ONS 15310-MA chapter. • Added a Warning under the NTP-C151 Install the Power and Ground section in Install the Cisco ONS 15310-MA chapter. • Added a Warning under the NTP-C152 Install the Fan-Tray Assembly section in Install the Cisco ONS 15310-MA chapter. • Added two Warnings under NTP-C153 Install the CTX2500 Cards section in Install the Cisco ONS 15310-MA chapter. • Added a Warning under NTP-C154 Install the Ethernet Cards section inInstall the Cisco ONS 15310-MA chapter. • Added a Warning under the NTP-C155 Install the Electrical Cards section in Install the Cisco ONS 15310-MA chapter. • Updated Table for NTP-C157 Install Wires to Alarm, Timing, Craft, LAN, and UDC Pin Connections section in Install the Cisco ONS 15310-MA chapter. • Added a Warning under section NTP-C157 Install Wires to Alarm, Timing, Craft, LAN, and UDC Pin Connections section in Install the Cisco ONS 15310-MA chapter. • Added a Warning under the NTP-C159 Install and Remove SFPs section in Install the Cisco ONS 15310-MA chapter.

Date	Notes
	• Added a Note under Step 1 under DLP-C5 Connect the Office Ground to the ONS 15310-CL section in DLPs C1 to C99 chapter. • Added Step 2under DLP-C5 Connect the Office Ground to the ONS 15310-CL section in DLPs C1 to C99 chapter. • Updated Note under DLP-C7 Connect DC Office Power to the ONS 15310-CL section in DLPs C1 to C99 chapter. • Updated Step 2 under DLP-C8 Turn On and Verify DC Office Power on the ONS 15310-CL section inDLPs C1 to C99 chapter. • Added Note under DLP-C250 Connect the Office Ground to the ONS 15310-MA section in DLPs C200 to C299 chapter. • Added Step 2 under DLP-C250 Connect the Office Ground to the ONS 15310-MA section in DLPs C200 to C299 chapter. • Added Note under DLP-C251 Connect Office Power to the ONS 15310-MA section in DLPs C200 to C299 chapter. • Updated Step 1 under DLP-C252 Turn On and Verify Office Power to the ONS 15310-MA section in DLPs C200 to C299 chapter.
April 2008	• Added steps and images under DLP-C249 Mount Dual ONS 15310-MA Shelf Assemblies in a Rack section in DLPs C200 to C299 chapter. • Added a note in the NTP-C20 Set Up Name, Date, Time, and Contact Information section of Turn Up a Node chapter.
November 2008	• Updated Server Trail documentation in Chapter 6, Create Circuits and VT Tunnels and Chapter 19, DLPs C200 to C299. • Added Notes under NTP-C51 Create an Automatically Routed VCAT Circuit and NTP-C52 Create a Manually Routed VCAT Circuit procedures in Chapter 6, Create Circuits and VT Tunnels.
December 2008	• Added a new procedure DLP-C289 Enable Node Secure Mode in Chapter 19. • Updated the NTP-C177 procedure title to read as Set Up the ONS 15310 in EMS Secure Access.
April 2009	• Updated the reinitialization tool options in DLP-C169 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows) and DLP-C170 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX) sections of Chapter 18, DLPs C100 to C199.
June 2009	• Updated the note in DLP-C138 in the chapter, DLPs C100 to C199.
August 2009	• Updated the “Add a Path Protection Node” procedure in Chapter 14, “Add and Remove Nodes”.
October 2009	• Updated the Clean Fiber Connectors procedure in Chapter 15, “Maintain the Node”. • Added the “Clean Multi Fiber-Optic Cable Connectors” procedure in Chapter 18, DLPs C100 to C199.
November 2009	Updated the section “NTP-C140 Create a Server Trail” in the chapter, “Create Circuits and VT Tunnels”.
December 2009	• Updated the fan tray caution in the section “NTP-C152 Install the Fan-Tray Assembly” in the chapter “Install the Cisco ONS 15310-MA”.

Date	Notes
January 2010	Updated the “Add a Path Protection Node” procedure in Chapter 14, “Add and Remove Nodes”.
February 2010	Added NTP: C191 “Install the Rear Cover” in Chapter 2 “Install the Cisco ONS 15310-MA”.

Document Objectives

The *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* explains how to install, turn up, configure, and maintain Cisco ONS 15310-CL and Cisco ONS 15310-MA nodes and networks. Use this document 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

This guide provides procedures for installation, turn up, provisioning and acceptance of ONS 15310 nodes and ONS 15310 designed 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.

Verification procedures are provided, where necessary, to allow contract vendors to complete the physical installation and then turn the site over to craft personnel for verification, provisioning, turn up and acceptance. The front matter of the book is present 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. 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).

Non-Trouble Procedure (NTP)

Each NTP (procedure) 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, a trouble clearing reference is provided.

Related Documentation

Use the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* in conjunction with the following referenced publications:

- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*
  Provides detailed card specifications, hardware and software feature descriptions, network topology information, and network element defaults.
- *Cisco ONS 15310-CL and Cisco ONS 15310-MA 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 Cisco 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 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*
  Provides software feature and operation information for Ethernet cards in the Cisco ONS 15310-CL and Cisco ONS 15310-MA.
- *Release Notes for the Cisco ONS 15310-CL Release 8.5*
  Provides caveats, closed issues, and new feature and functionality information.
- *Release Notes for the Cisco ONS 15310-MA Release 8.5*
  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://cisco.com/en/US/products/hw/optical/ps2001/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 **IMPORTANT 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 15310 system. It also includes translations of the safety warnings that appear in the ONS 15310 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.

CHAPTER 1

Install the Cisco ONS 15310-CL

This chapter provides procedures for installing the Cisco ONS 15310-CL shelf, cards, and fiber-optic cable. To view 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-C1 Unpack and Inspect the Shelf Assembly, page 1-4—Complete this procedure before continuing with the "NTP-C2 Install the Shelf Assembly" procedure on page 1-4.
2. NTP-C2 Install the Shelf Assembly, page 1-4—Complete this procedure to install the shelf assembly in a rack before continuing with the "NTP-C3 Install the Power and Ground" procedure on page 1-5.
3. NTP-C3 Install the Power and Ground, page 1-5—Complete this procedure before continuing with the "NTP-C4 Install an Ethernet Card" procedure on page 1-7.
4. NTP-C4 Install an Ethernet Card, page 1-7—As needed, complete this procedure to install an Ethernet card (CE-100T-8 or ML-100T-8).
5. NTP-C121 Install a Filler Card, page 1-9—As needed, complete this procedure to install a filler card (blank faceplate) in the expansion slot. If no Ethernet card is installed in the expansion slot, you must install a filler card.
6. NTP-C5 Install Wires to Alarm, Timing, LAN, Craft, and UDC Pin Connections, page 1-9—Complete this procedure to install cables for alarms, timing, LAN, and craft connections.
7. NTP-C6 Install the Electrical Cables, page 1-10—Complete this procedure to connect and route cables that will carry electrical traffic.
8. NTP-C7 Install and Remove SFPs, page 1-11—As needed, complete this procedure to install small form-factor pluggables (SFPs) so you can attach fiber-optic cables and determine the rate of the optical ports.
9. NTP-C8 Install Optical Cables, page 1-12—Complete this procedure to connect and route cables that will carry optical traffic.
10. NTP-C9 Preprovision an SFP Slot, page 1-14—As needed, complete this procedure to provision SFPs, known as pluggable port modules (PPMs) in Cisco Transport Controller (CTC).
11. NTP-C10 Preprovision a Card Slot, page 1-15—As needed, complete this procedure to preprovision an empty card slot with a card that will be installed later.

12. NTP-C11 Remove and Replace an Ethernet Card, page 1-16—As needed, complete this procedure to remove and replace an Ethernet card.
13. NTP-C12 Perform the Shelf Installation Acceptance Test, page 1-16—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 can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Warning **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Note The ONS 15310-CL is designed to comply with GR-1089-CORE Type 2 and Type 4 telecommunication port equipment. Install and operate the ONS 15310-CL only in environments that do not expose wiring or cabling to the outside plant. Acceptable applications include Central Office Environments (COEs), Electronic Equipment Enclosures (EEEs), Controlled Environment Vaults (CEVs), huts, and Customer Premise Environments (CPEs).

Note The Cisco ONS 15310-CL is intended for use with telecommunications equipment only.

Warning **The intra-building ports of the ONS15310-CL are suitable only for connecting to intra-building or unexposed wiring or cabling. The intra-building ports of ONS15310-CL 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.**

Required Tools and Equipment

You will need the following tools and equipment to install and test the ONS 15310-CL.

Included Materials

These materials are shipped with the ONS 15310-CL. The number in parentheses provides the quantity of the item included in the package.

- #12-24 x 1/2 pan head Phillips mounting screws (4)
- #10-32 x 3/8 pan head Phillips power lug screws (2)
- #6 AWG dual-hole, 5/8 in.-spaced grounding lug
- Electrostatic discharge (ESD) wrist strap with 1.8 m (6 ft.) coil cable

User-Supplied Materials

These materials and tools are required but are not supplied with the ONS 15310-CL.

- Equipment rack (22 inches total width for a 19-inch rack; 26 inches total width for a 23-inch rack)
- Fuse and alarm panel (DC-powered shelf)
- Copper power cable (DC-powered shelf, only; from fuse and alarm panel to assembly), #14 AWG
- Ground cable, #6 AWG stranded (minimum)
- Alarm cable, CAT-5 terminated with RJ-45 for all alarm connections
- Craft port serial cable, CAT-5 terminated with RJ-45
- BITS timing port cable, CAT-5 terminated with RJ-45
- UDC/RS-232 port cable, CAT-5 terminated with RJ-45
- Management LAN cable, CAT-5 terminated with RJ-45
- Single-mode LC fiber jumpers with UPC polish (55 dB or better) for optical interfaces
- DS1 cabling, 96-pin LFH connector, terminated to a 21-pair #26AWG cable, with dual 64-pin CHAMP connectors at far end with separate transmit and receive, straight termination (optional)
- Shielded coaxial cable terminated with miniBNC connectors at the ONS 15310-CL end (BNC connectors at other end) for DS-3/EC-1 ports
- Tie wraps and/or lacing cord
- Labels

Tools Needed

- #2 Phillips screw driver
- Medium slot head screw driver
- Small slot head screw driver
- Wire cutters
- Wire strippers
- Hand crimper, Molex p/n 63811-1100 or equivalent

Test Equipment

- Volt meter

- Power meter (for use with fiber optics only)
- Bit Error Rate (BER) tester, DS-1 and DS-3/EC-1

Note In this chapter, the terms "ONS 15310-CL" and "shelf assembly" are used interchangeably. In the installation context, these terms have the same meaning. Otherwise, shelf assembly refers to the physical steel enclosure that holds cards and connects power, and ONS 15310-CL refers to the entire system, both hardware and software.

NTP-C1 Unpack and Inspect the Shelf Assembly

Purpose	This procedure describes how to unpack the ONS 15310-CL and verify the contents.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Complete the "DLP-C1 Unpack and Verify the Shelf Assembly" task on page 17-1.

Step 2 Complete the "DLP-C2 Inspect the Shelf Assembly" task on page 17-1.

Step 3 Continue with the "NTP-C2 Install the Shelf Assembly" procedure on page 1-4.

Stop. You have completed this procedure.

NTP-C2 Install the Shelf Assembly

Purpose	This procedure describes how to mount shelf assemblies in a rack. You can also place the ONS 15310-CL on a flat surface, using the rubber feet mounted on the shelf assembly.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Two set screws (48-1003-XX)
Prerequisite Procedures	NTP-C1 Unpack and Inspect the 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) for AC power, or 149°F (65°C) for DC power.** Statement 1047

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 **To prevent airflow restriction, allow clearance around the ventilation openings to be at least 1 inch (2.54 cm).** Statement 1076

Note The ONS 15310-CL installations are suitable for Network Telecommunication facilities and locations where NEC are applicable.

Step 1 Complete the necessary rack mount task:

- DLP-C3 Mount the ONS 15310-CL in a Rack, page 17-2
- DLP-C4 Mount Multiple ONS 15310-CL Shelf Assemblies in a Rack, page 17-4

Step 2 Continue with the "NTP-C3 Install the Power and Ground" procedure on page 1-5.

Stop. You have completed this procedure.

NTP-C3 Install the Power and Ground

Purpose	This procedure describes how to install power feeds and ground the ONS 15310-CL.
Tools/Equipment	Ground cable, #6 AWG stranded copper conductors, minimum 90 degrees C Copper power cable (from fuse and alarm panel to assembly), #14 AWG stranded copper conductors, minimum 90 degrees C
Prerequisite Procedures	NTP-C2 Install the Shelf Assembly, page 1-4
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

⚠ **Warning** **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** **Read the installation instructions before connecting the system to the power source.** Statement 1004

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

⚠ **Warning** **This equipment must be grounded. Never defeat the ground conductor or operate 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

The following warnings apply to shelf assemblies that connect to DC office power:

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

⚠ **Warning** **When installing or replacing the unit, the ground connection must always be made first and disconnected last.** Statement 1046

⚠ **Warning** **Connect the unit only to DC power source that complies with the safety extra-low voltage (SELV) requirements under IEC 60950-1 based safety standards.** Statement 1033

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

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

⚠ **Caution** Always use the supplied ESD wristband when working with a powered ONS 15310-CL. Plug the wristband cable into the ESD jack located to the left of the expansion slot.

Step 1 Verify that the proper fuse panel is installed (20-amp fuse per shelf minimum). If not, install one according to manufacturer instructions.

Step 2 Complete the "DLP-C5 Connect the Office Ground to the ONS 15310-CL" task on page 17-5.

Step 3 As needed, complete one of the following tasks:

- DLP-C6 Connect AC Office Power to the ONS 15310-CL, page 17-6
- DLP-C7 Connect DC Office Power to the ONS 15310-CL, page 17-8

Step 4 As needed, complete one of the following tasks:

- DLP-C8 Turn On and Verify DC Office Power on the ONS 15310-CL, page 17-11
- DLP-C182 Turn On and Verify AC Office Power, page 18-75

Step 5 As needed, continue with the "NTP-C4 Install an Ethernet Card" procedure on page 1-7 or the "NTP-C121 Install a Filler Card" procedure on page 1-9.

Stop. You have completed this procedure.

NTP-C4 Install an Ethernet Card

Purpose	This procedure installs an Ethernet card (CE-100T-8 or ML-100T-8) in the ONS 15310-CL expansion slot.
Tools/Equipment	None
Prerequisite Procedures	DLP-C8 Turn On and Verify DC Office Power on the ONS 15310-CL, page 17-11
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Warning **Blank faceplates and cover panels 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, faceplates, front covers, and rear covers are in place.** Statement 1029

Warning **To comply with the Telcordia GR-1089 Network Equipment Building Systems (NEBS) standard for electromagnetic compatibility and safety, connect the copper Ethernet ports to intrabuilding or nonexposed wiring and cabling only. Also refer to the Intra-building Ports Warning for more information.**

Warning **The Ethernet ports of ONS15310-CL are intra-building ports and are suitable only for connecting to cat-5 shielded (STP) cabling grounded at both ends.** Statement 1084

Caution Do not install an Ethernet card in an ONS 15310-CL if the ambient temperature exceeds 131 degrees Fahrenheit (55 degrees Celsius).

Step 1 Install an Ethernet card (CE-100T-8 or ML-100T-8) in the expansion slot (Figure 1-1):

a. Open the card ejector.

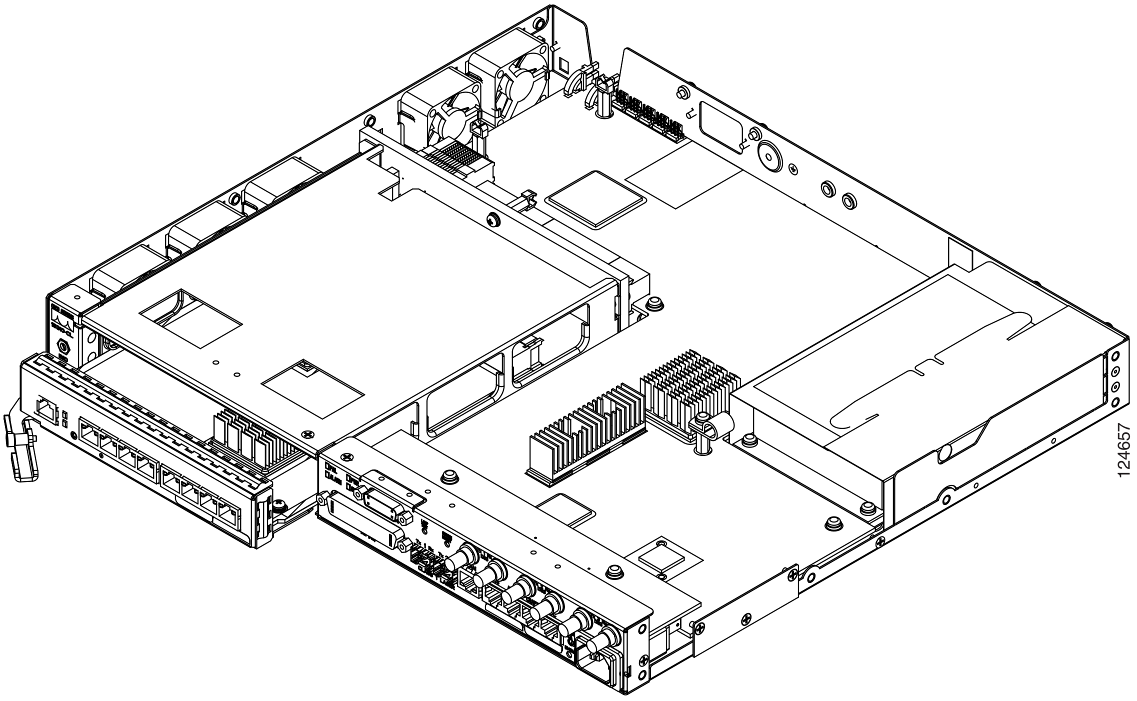
b. Slide the card along the guide rails into the slot.

c. Close the ejector by pushing it to the right.

d. Lock the cards into place by tightening the ejector locking screws.

Note The Ethernet cards are hot-pluggable, meaning they can be inserted or removed without turning off the power to the ONS 15310-CL.

Figure 1-1 Installing an Ethernet Card



Step 2 Verify the Ethernet card LED activity:

a. Verify that the red FAIL LED is off

b. Verify that the green ACT LED is on.

Step 3 If you remove power from the ONS 15310-CL chassis and then restore the power, check the chassis LED activity:

a. Verify that the chassis red FAIL LED blinks for 20 to 30 seconds, then turns off.

b. Verify that the chassis ALARM LED is off.

c. Verify the chassis green PWR LED is on. (It is amber only if one DC power source is on and operating.)

d. Verify that the chassis green SYNC LED is on.

Step 4 When you log into CTC, verify that the card appears properly on the CTC node view screen.

Stop. You have completed this procedure.

NTP-C121 Install a Filler Card

Purpose	This procedure installs a filler card (blank faceplate) in the ONS 15310-CL expansion slot. The filler cards are detectable in CTC.
Tools/Equipment	Filler card (15310-CL-FILLER)
Prerequisite Procedures	DLP-C8 Turn On and Verify DC Office Power on the ONS 15310-CL, page 17-11
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Warning **Blank faceplates and cover panels 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, faceplates, front covers, and rear covers are in place.** Statement 1029

Step 1 Open the card ejector.

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

Step 3 Close the ejector by pushing it to the right.

Step 4 Lock the cards into place by tightening the ejector locking screws.

Note The filler cards are hot-pluggable, which means they can be inserted or removed without turning off the power to the ONS 15310-CL.

Step 5 When you log into CTC, verify that the card appears properly in CTC node view.

Stop. You have completed this procedure.

NTP-C5 Install Wires to Alarm, Timing, LAN, Craft, and UDC Pin Connections

Purpose	This procedure installs alarm, timing, craft, UDC, and LAN wires.
Tools/Equipment	CAT-5 cables, terminated with RJ-45 for all alarm, timing, craft, UDC, and LAN connections
Prerequisite Procedures	NTP-C2 Install the Shelf Assembly, page 1-4
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **The Alarm, Timing (BITS), Craft, LAN and, UDC ports of ONS15310-MA are intra-building ports. The BITS and LAN ports are suitable only for connecting to shielded cabling grounded at both ends.**

Caution Always use the supplied ESD wristband when working with a powered ONS 15310-CL. Plug the wristband cable into the ESD jack located to the left of the expansion slot.

Step 1 Complete the "DLP-C9 Install External Alarm Cables on the ONS 15310-CL" task on page 17-12 as necessary. An alarm cable is necessary to provision external alarms and external controls.

Step 2 Complete the "DLP-C10 Install Timing Cables on the ONS 15310-CL" task on page 17-13 as needed. Timing cables are necessary to provision external timing.

Step 3 Complete the "DLP-C11 Install the Serial Cable for an ONS 15310-CL TL1 Craft Interface" task on page 17-15 as needed. A craft cable is required to access TL1 using the craft interface.

Step 4 Complete the "DLP-C12 Install the UDC Cable on the ONS 15310-CL" task on page 17-15 to enable UDC circuits; UDC circuits are dedicated data channels between nodes.

Step 5 Complete the "DLP-C181 Install the LAN Cable for CTC Interface" task on page 18-74 to provide access to the CTC.

Step 6 Continue with the "NTP-C6 Install the Electrical Cables" procedure on page 1-10.

Stop. You have completed this procedure.

NTP-C6 Install the Electrical Cables

Purpose	This procedure describes how to install the electrical DS-1 (96-pin D-sub) and DS-3/EC-1 (coaxial) cables. To carry electrical traffic on the ONS 15310-CL, you must install electrical cables.
Tools/Equipment	Shielded coaxial cable terminated with miniBNC connectors for DS-3/EC-1 ports 96-pin LFH connector terminated to a 21-pair #26AWG cable
Prerequisite Procedures	NTP-C5 Install Wires to Alarm, Timing, LAN, Craft, and UDC Pin Connections, page 1-9
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **The DS-1 and DS-3 ports of ONS15310-CL are intra-building ports and are suitable only for connecting to shielded cabling grounded at both ends.**

Caution Always use the supplied ESD wristband when working with a powered ONS 15310-CL. Plug the wristband cable into the ESD jack located to the left of the expansion slot.

Step 1 Complete the "DLP-C13 Install LFH Cables for ONS 15310-CL DS-1 Connections" task on page 17-16 as needed.

Step 2 Complete the "DLP-C14 Install DS-3/EC-1 Cables With MiniBNC Connectors on the ONS 15310-CL" task on page 17-19 as needed.

Step 3 Complete the "DLP-C15 Route Cables on the ONS 15310-CL" task on page 17-20 as needed.

Step 4 Continue with the "NTP-C7 Install and Remove SFPs" procedure on page 1-11.

Stop. You have completed this procedure.

NTP-C7 Install and Remove SFPs

Purpose	This procedure installs and removes Small Form-factor Pluggables (SFPs). SFPs are hot-swappable input/output devices that plug into SFP slots on the ONS 15310-CL front panel to link the port with the fiber-optic network. You can preprovision the multirate SFPs using the "DLP-C192 Provision a Multirate Pluggable Port Module" task on page 18-92. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for more information on SFP specifications.
Tools/Equipment	SFPs: For OC-3/STM-1 port use only: • ONS-SI-155-L1: 1310-nm, long reach • ONS-SI-155-L2: 1550-nm, long reach • ONS-SI-155-I1: 1310-nm, intermediate reach • ONS-SE-155-1470 through ONS-SE-155-1610: 1470 nm through 1610 nm, long-reach For OC-3/STM-1 or OC-12/STM-4 use: • ONS-SI-622-I1: 1310-nm, intermediate reach For OC-12/STM-4 use only: • ONS-SI-622-L1: 1310-nm, long reach • ONS-SI-622-L2: 1550-nm, long reach • ONS-SE-622-1470 through ONS-SE-622-1610: 1470 nm through 1610 nm, long-reach
Prerequisite Procedures	NTP-C3 Install the Power and Ground, page 1-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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

Warning **For copper SFPs, the Ethernet ports of ONS15310-CL are intra-building ports and are suitable only for connecting to cat-5 shielded (STP) cabling grounded at both ends.** Statement 1084

Step 1 Complete the "DLP-C16 Install SFP Connectors" task on page 17-22 as needed.

Step 2 Complete the "DLP-C17 Remove SFP Connectors" task on page 17-23 as needed.

Step 3 Continue with the "NTP-C8 Install Optical Cables" procedure on page 1-12.

Stop. You have completed this procedure.

NTP-C8 Install Optical Cables

Purpose	This procedure describes how to install fiber-optic cables in SFPs on the ONS 15310-CL.
Tools/Equipment	Single-mode fiber jumpers with LC connectors Fiber boot Optical power meter Optical attenuators, as necessary
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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

Caution Always use the supplied ESD wristband when working with a powered ONS 15310-CL. Plug the wristband cable into the ESD jack located to the left of the expansion slot.

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

Note Inspect and clean all fiber connectors thoroughly. See the "NTP-C109 Clean Fiber Connectors" procedure on page 15-10 for instructions. Dust particles can degrade performance. Put caps on any fiber connectors that are not used.

Note To install fiber-optic cables in the ONS 15310-CL, a fiber cable with the corresponding connector type must be connected to the transmit and receive ports on the SFPs.

Step 1 Measure the optical receive levels using an optical power meter, compare with the allowable optical power levels for the installed SFPs, and attenuate accordingly. See Table 1-1 for the minimum and maximum levels for each SFP type.

Table 1-1 Optical Transmit and Receive Levels

SFP	Interface	Transmitter Output Power Min/Max (dBm)	Receiver Input Power Min/Max (dBm)
ONS-SI-155-L1	OC-3	–5.0 to 0	–34 to –10
ONS-SI-155-L2	OC3	–5.0 to 0	–34 to –10
ONS-SI-155-I1	OC-3	–15 to –8.0	–28 to –8
ONS-SI-622-L1	OC-12	–3.0 to 2.0	–28 to –8
ONS-SI-622-L2	OC-12	–3.0 to 2.0	–28 to –8
ONS-SI-622-I1	OC-12/OC-3	–15 to –8.0	–28 to–8
ONS-SE-155-1470 through ONS-SE-155-1610	OC-3	0 to +5	–7
ONS-SE-622-1470 through ONS-SE-622-1610	OC-12	0 to +5	–7

Step 2 As needed, complete the "DLP-C18 Install Fiber-Optic Cables in a 1+1 Configuration" task on page 17-24.

Step 3 As needed, complete the "DLP-C19 Install Fiber-Optic Cables for Path Protection Configurations" task on page 17-25.

Step 4 As needed, gently route the fiber cables away from the shelf. You may want to use the optional tie-down bar.

Step 5 Continue with the "NTP-C12 Perform the Shelf Installation Acceptance Test" procedure on page 1-16.

Stop. You have completed this procedure.

NTP-C9 Preprovision an SFP Slot

Purpose	This procedure preprovisions SFPs, which are referred to as pluggable port modules (PPMs) in CTC. OC-3, OC-12, and multirate (OC-3/OC-12) PPMs are compatible with the ONS 15310-CL.
Tools/Equipment	None
Prerequisite Procedures	Chapter 3, "Connect the PC and Log into the GUI"
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The 15310-CL-CTX card does not have a faceplate because it is located inside the chassis; the 15310-CL-CTX LED indicators and connectors (including the SFP slot) are located on the ONS 15310-CL front panel.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 to log into an ONS 15310-CL on the network.

Step 2 Click the **Alarms** tab:

a. Verify that the alarm filter is not turned on. See the "DLP-C88 Disable Alarm Filtering" task on page 17-109 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 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* as necessary.

c. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export alarm and condition information.

Step 3 In node view, double-click the 15310-CL-CTX card.

Step 4 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 5 In the Pluggable Port Modules pane, click **Create**. The Create PPM dialog box appears.

Step 6 In the Create PPM dialog box, complete the following:

- PPM—Click the slot number where the SFP is installed from the drop-down list.
- PPM Type—Click the number of ports supported by your SFP from the drop-down list. If only one port is supported, **PPM (1 port)** is the only menu option.

Step 7 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 is installed. After the SFP is installed, the row on the pane turns white and the column lists the equipment name.

Step 8 Verify that the PPM appears in the list on the Pluggable Port Modules pane. If it does not, repeat Steps 5 through 7.

Step 9 Click the **Provisioning > Line** tabs. If applicable for the PPM you are preprovisioning, use the **Reach** and **Wavelength** columns to configure these parameters as desired.

Note Only the SFPs that can be configured for Reach and Wavelength are displayed and settable for a given card or PIM. Only the parameters that are editable for the PPMs on a particular platform type are provisionable. For instance, some platforms may not have PPMs with configurable wavelengths or reaches. In that case wavelength is not provisionable.

Step 10 Repeat the task to provision a second PPM.

Step 11 Click **OK**.

Step 12 When you are ready to install the SFP, complete the "DLP-C16 Install SFP Connectors" task on page 17-22. If you installed a multirate SFP, you must select the line rate using the "DLP-C193 Provision the Optical Line Rate" task on page 18-92.

Stop. You have completed this procedure.

NTP-C10 Preprovision a Card Slot

Purpose	This procedure describes how to preprovision a slot in the software before physical card installation.
Tools/Equipment	None
Prerequisite Procedures	Chapter 3, "Connect the PC and Log into the GUI"
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node where you want to preprovision the slot. If you are already logged in, continue with Step 2.

Step 2 Right-click the empty slot where you will later install a card.

Step 3 From the Add Card popup menu, navigate to Ethernet and choose the card type you want (CE-100T-8 or ML-100T-8).

Note When you preprovision a slot, the card appears purple in the CTC shelf display, rather than white when a card is physically in the slot.

Stop. You have completed this procedure.

NTP-C11 Remove and Replace an Ethernet Card

Purpose	This procedure describes how to remove and replace Ethernet cards in the ONS 15310-CL shelf.
Tools/Equipment	None
Prerequisite Procedures	NTP-C4 Install an Ethernet Card, page 1-7
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **Blank faceplates and cover panels 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, faceplates, front covers, and rear covers are in place.** Statement 1029

Step 1 If you are not logged into CTC and you need to remove a card, continue with Step 3. When you log into CTC, troubleshoot the mismatched equipment (MEA) alarm with the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

Step 2 If you are logged into CTC, on the node view shelf graphic right-click the Ethernet card that you want to remove and choose **Delete Card**.

Note If you do not remove a card from the shelf after you delete it in CTC, it will reboot and reappear in CTC.

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 "NTP-C4 Install an Ethernet Card" procedure on page 1-7.

Stop. You have completed this procedure.

NTP-C12 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, "Install the Cisco ONS 15310-CL"
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Complete Table 1-2 on page 1-17 by verifying that each procedure was completed.

Table 1-2 ONS 15310-CL Shelf Installation Task Summary

Description	Completed
NTP-C1 Unpack and Inspect the Shelf Assembly, page 1-4	
NTP-C2 Install the Shelf Assembly, page 1-4	
NTP-C3 Install the Power and Ground, page 1-5	
NTP-C4 Install an Ethernet Card, page 1-7	
NTP-C121 Install a Filler Card, page 1-9	
NTP-C5 Install Wires to Alarm, Timing, LAN, Craft, and UDC Pin Connections, page 1-9	
NTP-C6 Install the Electrical Cables, page 1-10	
NTP-C7 Install and Remove SFPs, page 1-11	
NTP-C8 Install Optical Cables, page 1-12	

Step 2 Check each wire and cable connection to make sure all cables are locked securely. If a wire or cable is loose, return to the appropriate procedure in this chapter to correct it.

Step 3 Complete the "DLP-C20 Measure Voltage" task on page 17-28.

Stop. You have completed this procedure.

CHAPTER 2

Install the Cisco ONS 15310-MA

This chapter provides procedures for installing the Cisco ONS 15310-MA shelf, cards, and fiber-optic cable. To view a summary of the tools and equipment required for installation, see the "Required Tools and Equipment" section on page 2-3.

Before You Begin

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

1. NTP-C149 Unpack and Inspect the ONS 15310-MA Shelf Assembly, page 2-5—Complete this procedure before continuing with the "NTP-C150 Install the Shelf Assembly" procedure on page 2-5.
2. NTP-C150 Install the Shelf Assembly, page 2-5—Complete this procedure to install the shelf assembly in a rack before continuing with the "NTP-C151 Install the Power and Ground" procedure on page 2-12 or before completing one of the following optional procedures.
3. NTP-C169 Install the Cable Management Bracket, page 2-6—As needed, complete this procedure to install the cable management bracket.
4. NTP-C166 Remove the Blank Sheet Metal Covers, page 2-9—As needed, complete this procedure to access the backplane.
5. NTP-C167 Install the EIAs, page 2-10—As needed, complete this procedure to install the electrical interface assemblies (EIAs) before continuing with the "NTP-C151 Install the Power and Ground" procedure on page 2-12.
6. NTP-C151 Install the Power and Ground, page 2-12—Complete this procedure before continuing with the "NTP-C152 Install the Fan-Tray Assembly" procedure on page 2-14.
7. NTP-C152 Install the Fan-Tray Assembly, page 2-14—Complete this procedure before continuing with the "NTP-C153 Install the CTX2500 Cards" procedure on page 2-16.
8. NTP-C153 Install the CTX2500 Cards, page 2-16—Complete this procedure to install the common-control/cross-connect cards.
9. NTP-C154 Install the Ethernet Cards, page 2-19—As needed, complete this procedure to install an Ethernet card.
10. NTP-C155 Install the Electrical Cards, page 2-20—As needed, complete this procedure to install an electrical card.
11. NTP-C156 Install the Filler Cards, page 2-21—As needed, complete this procedure to install a filler card (blank faceplate) in the expansion slot. If no Ethernet or electrical card is installed in the expansion slot, you must install a filler card.

12. NTP-C157 Install Wires to Alarm, Timing, Craft, LAN, and UDC Pin Connections, page 2-23—Complete this procedure to install cables for alarms, timing, LAN, craft, and user data channel (UDC) connections.
13. NTP-C158 Install the Electrical Cables, page 2-24—Complete this procedure to connect and route cables that will carry electrical traffic.
14. NTP-C173 Install the TST-DSX Card, page 2-25—As needed, complete this procedure to test the DS-1 and DS-3 wiring integrity between an ONS 15310-MA shelf and the associated digital signal cross-connect (DSX) wiring panel.
15. NTP-C159 Install and Remove SFPs, page 2-27—As needed, complete this procedure to install Small Form-factor Pluggables (SFPs) that provide a fiber-optic interface to the CTX2500 card.
16. NTP-C160 Install Optical Cables, page 2-28—Complete this procedure to connect and route cables that will carry optical traffic.
17. NTP-C164 Perform the Shelf Installation Acceptance Test, page 2-29—Complete this procedure to determine if you have correctly completed all other procedures in the chapter.
18. NTP-C161 Preprovision an SFP Slot, page 2-30—As needed, complete this procedure to preprovision SFPs, which provide a fiber-optic interface to the ONS 15310-MA and can be provisioned for various line rates.
19. NTP-C162 Preprovision a Card Slot, page 2-31—As needed, complete this procedure to preprovision an empty card slot with a card that will be installed later.
20. NTP-C163 Remove and Replace a Card, page 2-32—As needed, complete this procedure to remove and replace an ONS 15310-MA card.
21. NTP-C168 Install the Front Door, page 2-33—As needed, complete this procedure to install the front door.
22. NTP-C191 Install the Rear Cover, page 2-35—As needed, complete this procedure to install the rear cover.

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 can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Warning **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Note The ONS 15310-MA is designed to comply with Telcordia GR-1089-CORE Type 2 and Type 4. Acceptable applications include Central Office Environments (COEs), Electronic Equipment Enclosures (EEEs), Controlled Environment Vaults (CEVs), huts, and Customer Premise Environments (CPEs).

Note The Cisco ONS 15310-MA is intended for use with telecommunications equipment only.

Warning **The intra-building ports of the ONS15310-MA are suitable only for connecting to intrabuilding or unexposed wiring or cabling. The intra-building ports of ONS15310-MA 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.**

Required Tools and Equipment

You will need the following tools and equipment to install and test the ONS 15310-MA.

Included Materials

These materials are shipped with the ONS 15310-MA. The number in parentheses provides the quantity of the item included in the package.

- Ground lug (1)
- Screws: panhead, 10-32 x 0.375 (10)
- Screws: panhead, 10-32 x 0.37, green zinc (2)
- Screws: panhead, 12-24 x 0.75 (8)
- Screws: panhead, 10-32 x 0.31 (2)
- Screws: panhead, 8-32 x 0.31 (3)
- Kep nut: 10-32 x 0.170
- Rack mount bracket
- Interconnect plate
- Rack mount bracket for 19-inch rack
- Rack mount bracket for 23-inch rack
- Cable routing bracket

User-Supplied Materials

These materials and tools are required but are not supplied with the ONS 15310-MA.

- Equipment rack (26 inches total width for a 23-inch rack)
- Fuse and alarm panel
- Copper power cable (from fuse and alarm panel to assembly), #12 AWG
- Ground cable, #6 AWG stranded (minimum)
- Alarm In cable, unshielded cable terminated with a DB-37 connector

- Alarm Out cable, shielded cable terminated with a DB-25 connector
- Craft port serial cable, CAT-5 terminated with RJ-45
- BITS timing port cable, CAT-3/CAT-5 terminated with DB-9 connector
- User data channel (UDC) cable: EIA/TIA-232 port cable, CAT-5 terminated with RJ-45
- Management LAN cable, CAT-5 terminated with RJ-45
- Single-mode LC fiber jumpers with UPC polish (55 dB or better) for optical interfaces
- DS1 cabling, shielded, terminated to a 21-pair #26AWG cable, with dual 64-pin CHAMP connectors at far end with separate transmit and receive, straight termination (optional)
- Shielded coaxial cable terminated with BNC connectors for DS-3/EC-1 ports
- Tie wraps and/or lacing cord
- Labels

Tools Needed

The following tools are needed to complete the procedures in this chapter:

- #2 Phillips screw driver
- Medium slot head screw driver
- Small slot head screw driver
- Wire cutters
- Wire strippers

Test Equipment

The following test equipment is needed to complete the procedures in this chapter:

- Volt meter
- Power meter (for use with fiber optics only)
- Bit error rate (BER) tester, DS-1 and DS-3/EC-1

Note In this chapter, the terms “ONS 15310-MA” and “shelf assembly” are used interchangeably. In the installation context, these terms have the same meaning. Otherwise, shelf assembly refers to the physical steel enclosure that holds cards and connects power, and ONS 15310-MA refers to the entire system, both hardware and software.

NTP-C149 Unpack and Inspect the ONS 15310-MA Shelf Assembly

Purpose	This procedure describes how to unpack the ONS 15310-MA and verify the contents.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Complete the "DLP-C1 Unpack and Verify the Shelf Assembly" task on page 17-1.

Step 2 Complete the "DLP-C2 Inspect the Shelf Assembly" task on page 17-1.

Step 3 Continue with the "NTP-C150 Install the Shelf Assembly" procedure on page 2-5.

Stop. You have completed this procedure.

NTP-C150 Install the Shelf Assembly

Purpose	This procedure describes how to mount ONS 15310-MA shelf assemblies in a rack.
Tools/Equipment	#2 Phillips screwdriver #12-24 mounting screws (4) #10-32 ear mounting screws (8) Universal mounting ears (2) Dual-assembly plate 19-inch-rack mounting ear 23-inch-rack mounting ear Fuse and alarm panel, if not installed
Prerequisite Procedures	NTP-C149 Unpack and Inspect the ONS 15310-MA Shelf Assembly, page 2-5
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note The ONS 15310-MA installations are suitable for Network Telecommunication facilities and locations where NEC are applicable.

Warning **To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 149°F (65°C).** Statement 1047

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

Step 1 Complete the necessary rack mount task:

- DLP-C248 Mount a Single ONS 15310-MA in a Rack, page 19-58
- DLP-C249 Mount Dual ONS 15310-MA Shelf Assemblies in a Rack, page 19-61

Step 2 Continue with the "NTP-C169 Install the Cable Management Bracket" procedure on page 2-6.

Stop. You have completed this procedure.

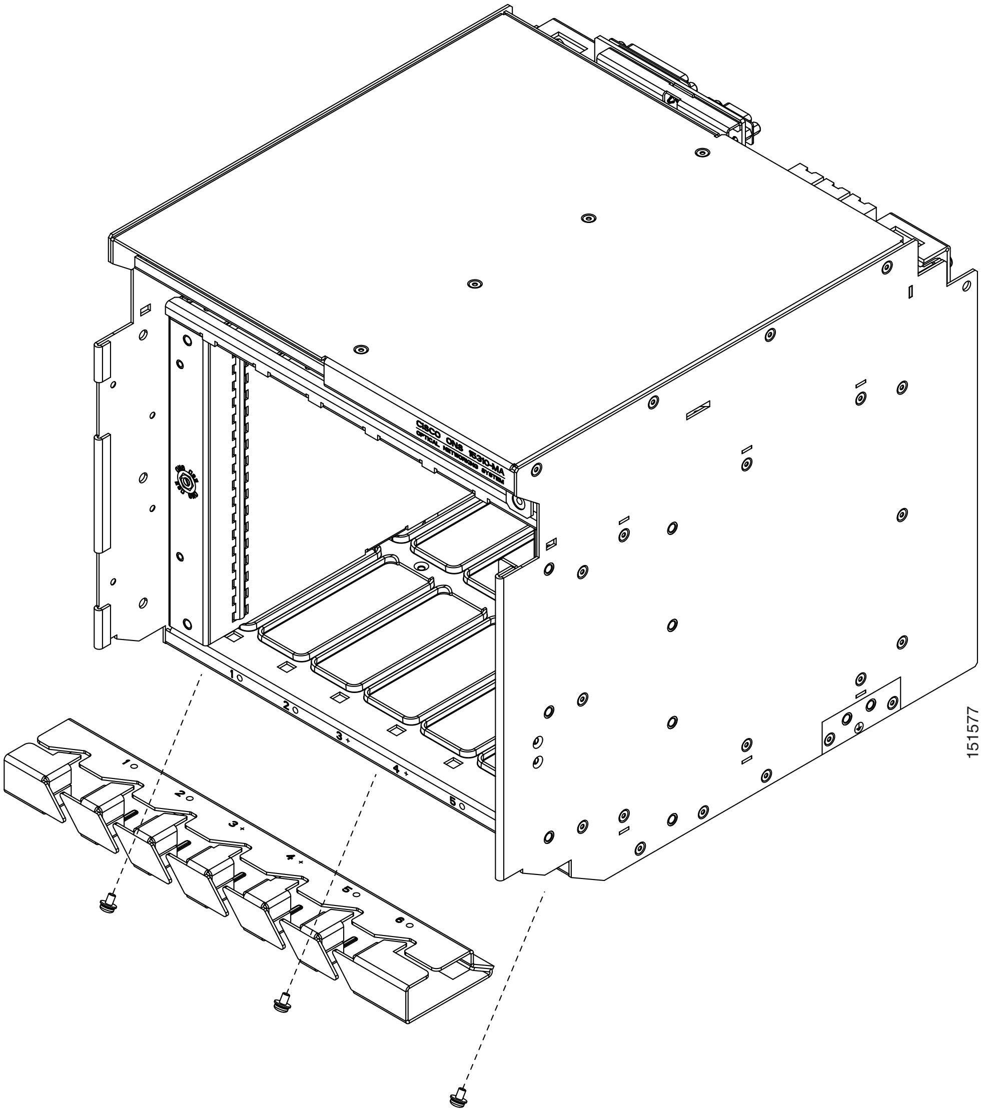
NTP-C169 Install the Cable Management Bracket

Purpose	This procedure describes how to install the cable management bracket, which is used for routing optical and Ethernet cables.
Tools/Equipment	#2 Phillips screwdriver Standard cable management bracket and three #8-32 x 0.31 inch (0.79 cm) screws (included with the ship kit) or Extended cable management bracket (15310-CBLMGT) and five 8-32 x 0.31 inch (0.79 cm) screws
Prerequisite Procedures	NTP-C150 Install the Shelf Assembly, page 2-5
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.** Statement 1077

Step 1 Line up the three screw holes on the rear of the bracket with the screw holes at the bottom of the ONS 15310-MA shelf assembly (Figure 2-1).

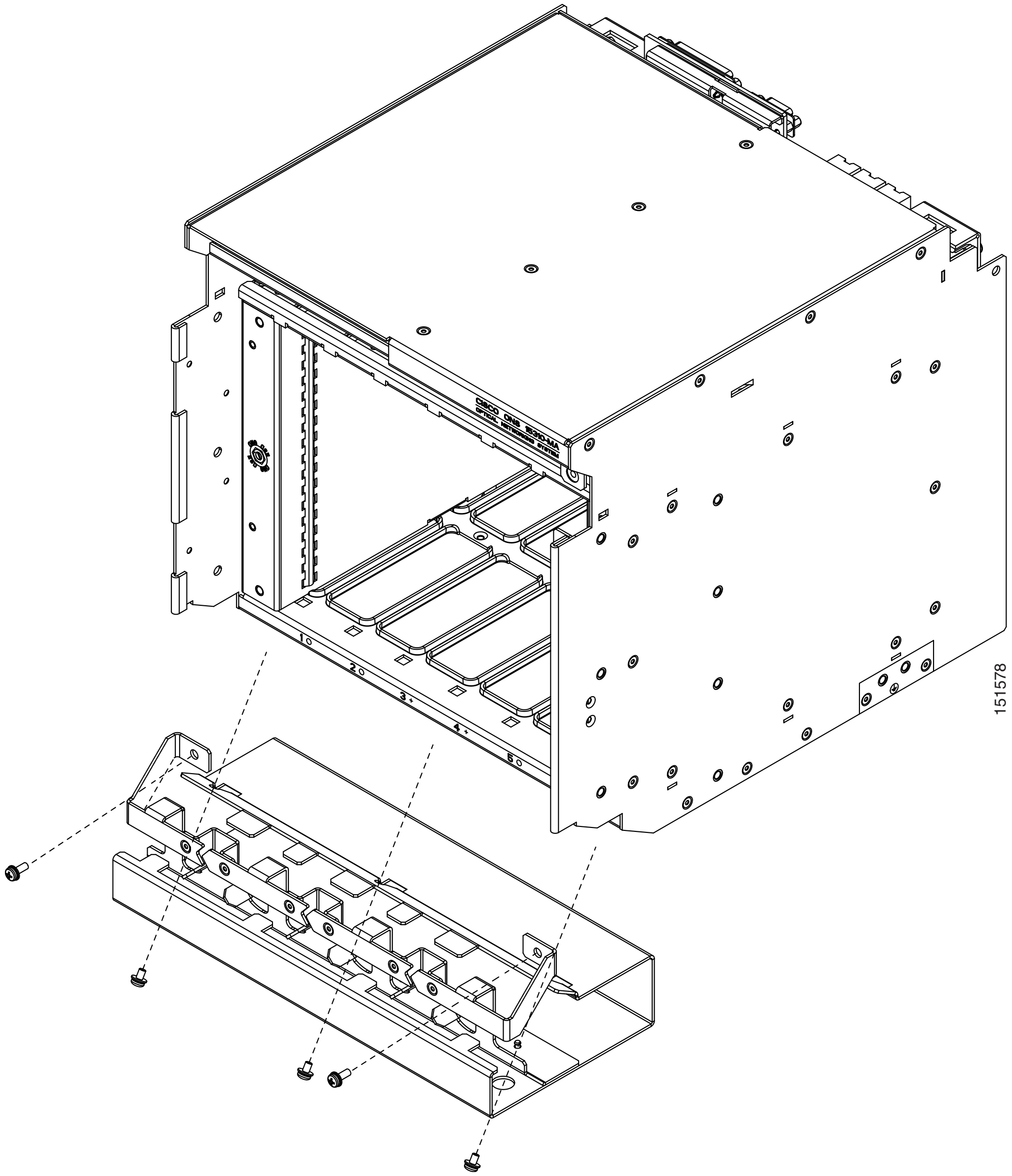
Figure 2-1 Installing the Standard Cable Management Bracket



Step 2 To secure the bracket to the shelf, use the screwdriver to install three 8-32 x 0.31 inch (0.79 cm) screws, torqued to 15 to 18 inch-lbs.

Step 3 If you are installing the extended bracket, install two 8-32 x 0.31 inch (0.79 cm) screws, torqued to 15 to 18 inch-lbs, through the top of the bracket directly into the ESD faceplates adjacent to Slots 1 and 6 on either side of shelf (Figure 2-2).

Figure 2-2 Installing the Extended Cable Management Bracket



Step 4 If you plan to install electrical interface assemblies (EIAs), continue with the "NTP-C166 Remove the Blank Sheet Metal Covers" procedure on page 2-9 to access the backplane. If not, continue with the "NTP-C151 Install the Power and Ground" procedure on page 2-12.

Stop. You have completed this procedure.

NTP-C166 Remove the Blank Sheet Metal Covers

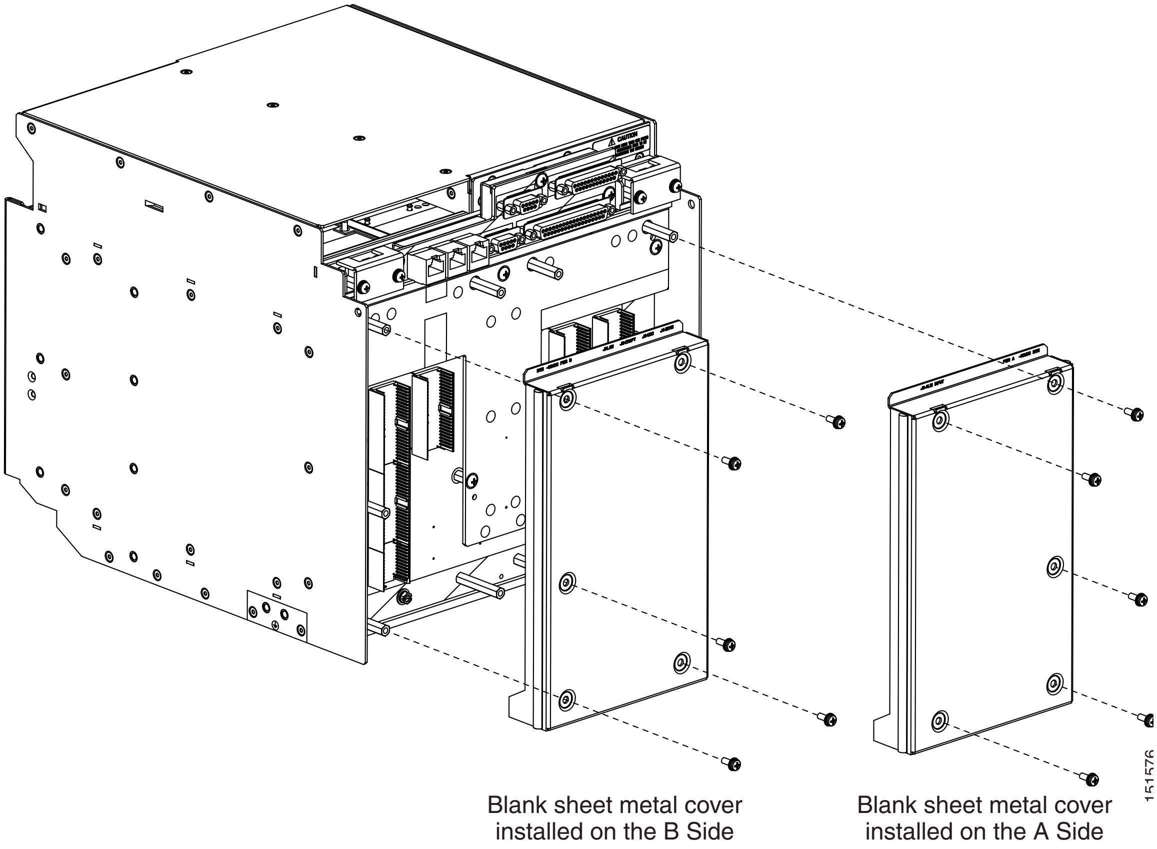
Purpose	This procedure describes how to access the backplane by removing the blank sheet metal covers. The backplane has two sheet metal covers (one on either side).
Tools/Equipment	#2 Phillips screwdriver
Prerequisite Procedures	NTP-C150 Install the Shelf Assembly, page 2-5
Required/As Needed	Required
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.** Statement 1077

Step 1 Use a Phillips screwdriver to remove the five screws holding each sheet metal cover in place.

Figure 2-3 shows the screw locations of the sheet metal covers installed on the A-side and B-side of the ONS 15310-MA.

Figure 2-3 Blank Sheet Metal Covers


Blank sheet metal cover installed on the B Side
Blank sheet metal cover installed on the A Side
151576

Step 2 Store the panels for later use. Attach the backplane cover(s) whenever EIA(s) are not installed.

Step 3 If you plan to install electrical interface assemblies (EIAs), continue with the "NTP-C167 Install the EIAs" procedure on page 2-10. If not, continue with the "NTP-C151 Install the Power and Ground" procedure on page 2-12.

Stop. You have completed this procedure.

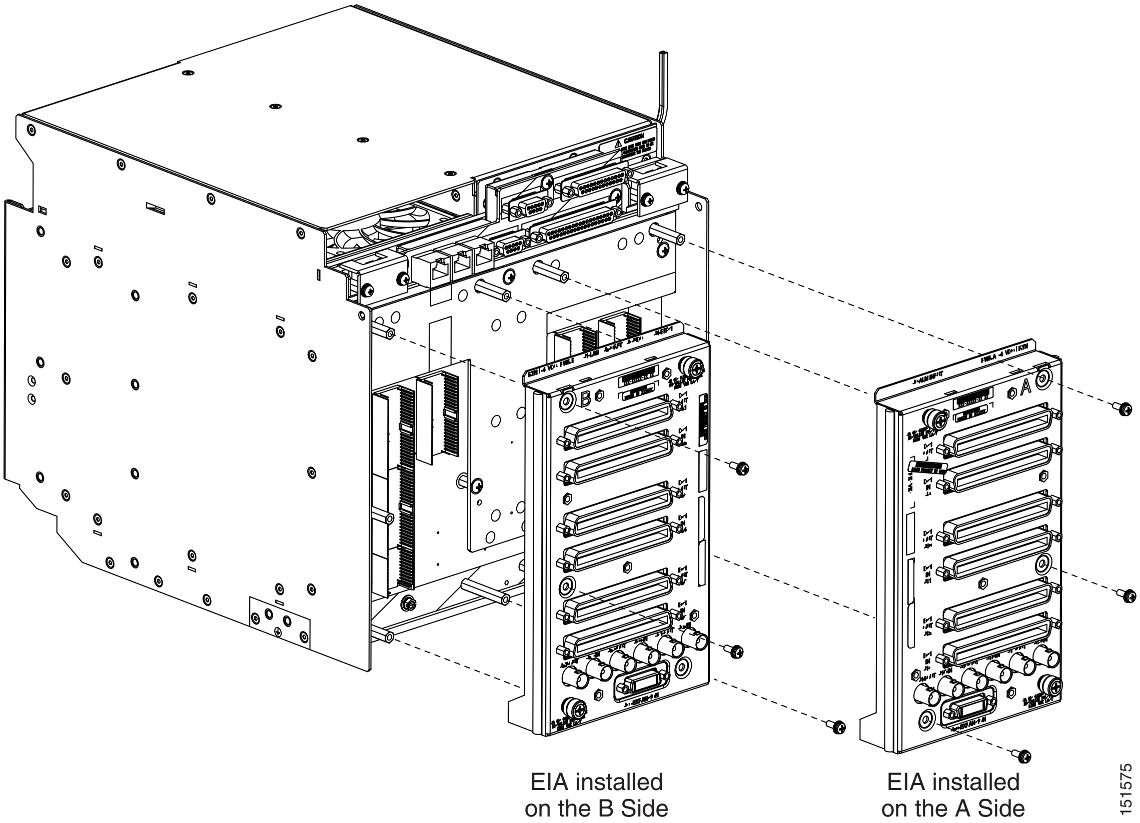
NTP-C167 Install the EIAs

Purpose	This procedure describes how to install electrical interface assemblies (EIAs). Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for descriptions of the EIAs.
Tools/Equipment	#2 Phillips screwdriver High-density EIA(s) 6-32 x 5/16-inch pan head screws (3, included with EIA)
Prerequisite Procedures	NTP-C169 Install the Cable Management Bracket, page 2-6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

⚠ **Caution** Connect only SELV services to the high-density EIAs on the ONS 15310-MA.

Step 1 Determine which high-density EIA is designed for installation on the B Side and which is designed for installation on the A Side (Figure 2-4).

Figure 2-4 ***High-Density EIA Installation***



Step 2 Align the connectors on the EIA you want to install with the mating connectors on the backplane, using the plastic guide posts on the connectors.

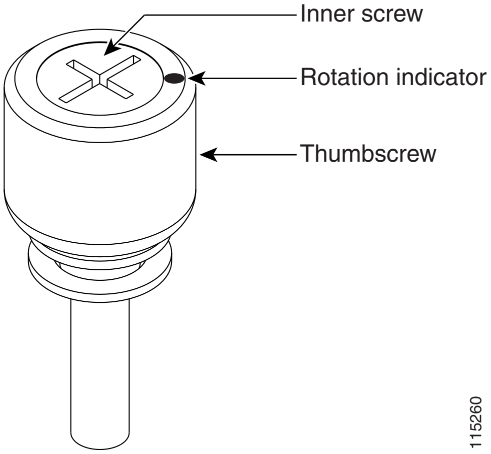
Caution Do not firmly apply pressure to the EIA; this could damage the EIA and backplane connectors.

Step 3 Seat the EIA as flat as possible by gently exerting enough pressure with your hands to only partially seat the connectors. Do not try and fully insert the EIA.

Step 4 Locate the two jack screws on the EIA, which are found on the opposite corners (Figure 2-4 on page 2-11). (For example, on the B-side EIA, the screws are located in the top right and bottom left corners.)

Step 5 Starting with either jack screw, tighten the thumb screw turn five full turns, then turn the other thumb screw five full turns (Figure 2-5). Alternate between the jack screws until the EIA is full seated onto the chassis and the jack screws are hand tight. The EIA is fully mated when both jack screws are fully threaded into the chassis.

Figure 2-5 EIA Jack Screw



Caution Threading one jack screw completely before threading the other jack screw might result in connector misalignment and damage to the EIA. Do not overtighten the jack screws.

Step 6 Install the remaining three 6-32 x 5/16-inch pan head screws onto the EIA and torque to 8 to 10 in-lbs.

Step 7 Repeat Steps 2 through 6 to install the other EIA, as necessary.

Step 8 Continue with the "NTP-C151 Install the Power and Ground" procedure on page 2-12.

Stop. You have completed this procedure.

NTP-C151 Install the Power and Ground

Purpose	This procedure describes how to install power feeds and how to ground the ONS 15310-MA.
Tools/Equipment	Ground cable, #6 AWG stranded copper conductors, minimum 90 degrees C (194 degrees F) Copper power cable (from fuse and alarm panel to assembly), #12 AWG stranded copper conductors, minimum 90 degrees C (194 degrees F)
Prerequisite Procedures	NTP-C150 Install the Shelf Assembly, page 2-5
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

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 **Read the installation instructions before connecting the system to the power source.** Statement 1004

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

Warning **This equipment must be grounded. Never defeat the ground conductor or operate 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

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

Warning **When installing or replacing the unit, the ground connection must always be made first and disconnected last.** Statement 1046

Warning **Connect the unit only to DC power source that complies with the safety extra-low voltage (SELV) requirements under IEC 60950-1 based safety standards.** Statement 1033

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

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

Caution Always use the supplied ESD wristband when working with a powered ONS 15310-MA. Plug the wristband cable into either of the ESD jacks, on the far left and right faceplates in the shelf.

Step 1 Verify that the proper fuse panel is installed (20-amp fuse per shelf minimum). If not, install one according to manufacturer instructions.

Step 2 Complete the "DLP-C250 Connect the Office Ground to the ONS 15310-MA" task on page 19-65.

Step 3 Complete the "DLP-C251 Connect Office Power to the ONS 15310-MA" task on page 19-68.

Step 4 Complete the "DLP-C252 Turn On and Verify Office Power to the ONS 15310-MA" task on page 19-69.

Step 5 Continue with the "NTP-C152 Install the Fan-Tray Assembly" procedure on page 2-14.

Stop. You have completed this procedure.

NTP-C152 Install the Fan-Tray Assembly

Purpose	This procedure installs the air filter and fan-tray assembly in the ONS 15310-MA.
Tools/Equipment	#2 Phillips screwdriver Fan-tray assembly Fan filter
Prerequisite Procedures	NTP-C151 Install the Power and Ground, page 2-12
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Caution Do not operate an ONS 15310-MA without a fan-tray air filter. A fan-tray air filter is mandatory in order to comply with Telcordia GR-63-CORE.

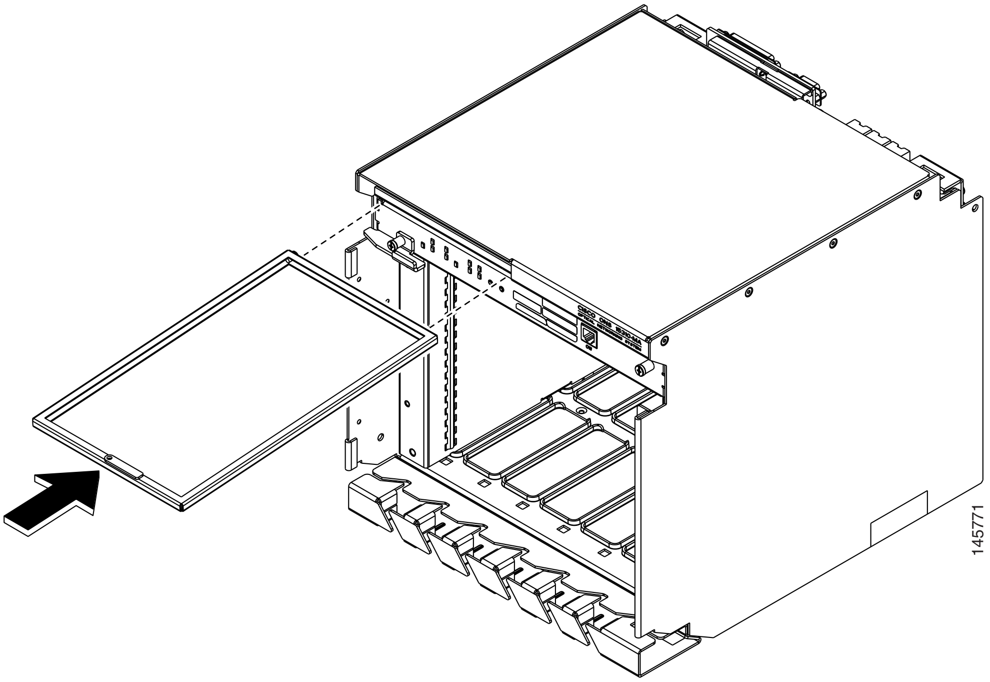
Caution You must place the edge of the air filter flush against the front of the fan-tray assembly compartment when installing the fan tray on top of the filter. Failure to do so could result in damage to the filter, the fan tray, or both.

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.

Warning **Order Wire (OW) port is an intra-building wiring port used only for maintenance purposes and is not connected during normal operation. This port must NOT be connected to any telecommunication network.**

Step 1 Install the air filter. The air filter is installed internally in the slot at the top left of the shelf assembly (Figure 2-6). Pull the tab, located at the center of the front of the fan filter, toward you. Make sure the tab is facing up before you install the fan filter.

Figure 2-6 Installing the Fan-Tray Air Filter



Step 2 Slide the air filter into the bracket, and push the tab closed

Step 3 Pull the fan tray ejector all the way out.

Step 4 Use the ejector to slide the fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.

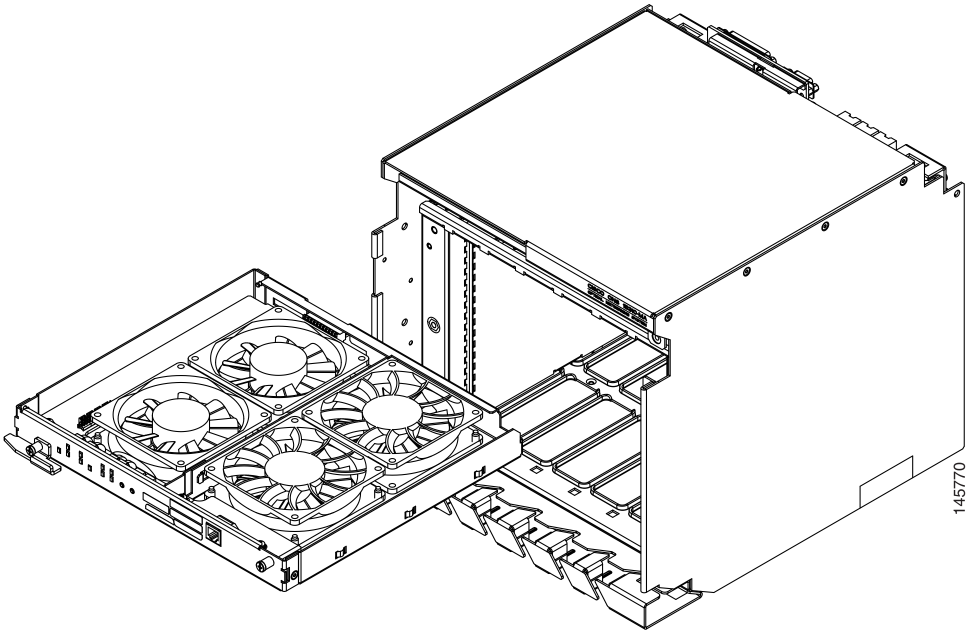
Step 5 Close the ejector.

Step 6 Use a Phillips screwdriver to tighten the screws at either end of the fan-tray assembly.

Step 7 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 2-7 shows the location of the fan-tray assembly.

Figure 2-7 Installing the Fan-Tray Assembly



Step 8 Continue with the "NTP-C153 Install the CTX2500 Cards" procedure on page 2-16.

Stop. You have completed this procedure.

NTP-C153 Install the CTX2500 Cards

Purpose	This procedure installs CTX2500 cards in the ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C8 Turn On and Verify DC Office Power on the ONS 15310-CL, page 17-11
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Warning **Blank faceplates and cover panels 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, faceplates, front covers, and rear covers are in place.** Statement 1029

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

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

Warning **The Ethernet ports and the LAN port on CTX2500 cards of ONS15310-MA are intra-building ports and are suitable only for connecting to cat-5 shielded (STP) cabling grounded at both ends.** Statement 1084

Warning **The CRAFT ports of ONS15310-MA are intra-building ports used only for setup and maintenance purposes by trained personnel and are not connected during normal operation.** Statement 1085

Caution Do not install a CTX2500 card in an ONS 15310-MA if the ambient temperature exceeds 149 degrees F (65 degrees C).

Caution Always use the supplied ESD wristband when working with a powered ONS 15310-MA. Plug the wristband cable into either of the ESD jacks, on the far left and right faceplates in the shelf.

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

Step 1 Install a CTX2500 card in Slot 3 or 4 (Figure 2-8):

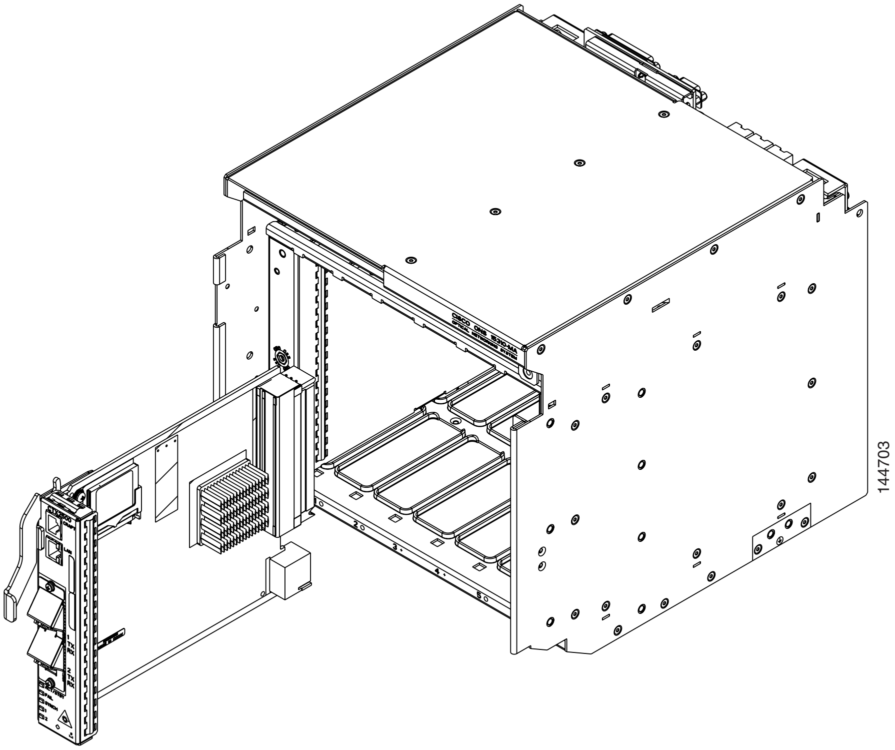
a. Open the card ejector.

b. Use the ejector at the top of the card and firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot.

c. Verify that the card is inserted correctly and close the ejector on the card.

Note The CTX2500 cards are hot-pluggable, which means they can be inserted or removed without turning off the power to the ONS 15310-MA.

Figure 2-8 Installing a CTX2500 Card



Step 2 Verify the CTX2500 card LED activity:

- **a.** The red FAIL LED turns on for 30 to 45 seconds. It then turns off for 5 seconds, and turns back on for 30 seconds.
- **b.** The red FAIL LED blinks for 20 seconds, and turns off for 5 seconds.
- **c.** All LEDs turn on for 2 seconds.
- **d.** The ACT/STBY LED turns on. It is green if the card is active, or amber if the card is standby.

Step 3 When you log into CTC, verify that the card appears properly in CTC node view.

Step 4 As necessary, continue with the "NTP-C154 Install the Ethernet Cards" procedure on page 2-19.

Stop. You have completed this procedure.

NTP-C154 Install the Ethernet Cards

Purpose	This procedure installs the Ethernet cards (CE-100T-8 or ML-100T-8) in the ONS 15310-MA. Ethernet cards can be installed in any traffic card slot (Slot 1, 2, 5, or 6).
Tools/Equipment	None
Prerequisite Procedures	DLP-C8 Turn On and Verify DC Office Power on the ONS 15310-CL, page 17-11
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Warning **Blank faceplates and cover panels 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, faceplates, front covers, and rear covers are in place.** Statement 1029

Warning **To comply with the Telcordia GR-1089 Network Equipment Building Systems (NEBS) standard for electromagnetic compatibility and safety, connect the copper Ethernet ports to intrabuilding or nonexposed wiring and cabling only.**

Warning **The Ethernet ports and the LAN port on CTX2500 cards of ONS15310-MA are intra-building ports and are suitable only for connecting to cat-5 shielded (STP) cabling grounded at both ends.** Statement 1084

Warning **The CRAFT ports of ONS15310-MA are intra-building ports used only for setup and maintenance purposes by trained personnel and are not connected during normal operation.** Statement 1085

Caution Do not install an Ethernet card in an ONS 15310-MA if the ambient temperature exceeds 149 degrees F (65 degrees C).

Caution Always use the supplied ESD wristband when working with a powered ONS 15310-MA. Plug the wristband cable into either of the ESD jacks, on the far left and right faceplates in the shelf.

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

Step 1 Install an Ethernet card (CE-100T-8 or ML-100T-8) in a traffic card slot:

a. Open the card ejector.

b. Use the ejector at the top of the card and firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot.

c. Verify that the card is inserted correctly and close the ejector on the card.

Note The Ethernet cards are hot-pluggable, which means they can be inserted or removed without turning off the power to the ONS 15310-MA.

Step 2 Verify the Ethernet card LED activity:

a. Verify that the red FAIL LED is off.

b. Verify that the green ACT LED is on.

Step 3 When you log into CTC, verify that the card appears properly in CTC node view.

Step 4 As necessary, continue with the "NTP-C155 Install the Electrical Cards" procedure on page 2-20.

Stop. You have completed this procedure.

NTP-C155 Install the Electrical Cards

Purpose	This procedure installs electrical cards (DS1-28/DS3-EC1-3 or DS1-84/DS3-EC1-3) in the ONS 15310-MA. Electrical cards can be installed in any traffic card slot (Slot 1, 2, 5, or 6).
Tools/Equipment	None
Prerequisite Procedures	DLP-C8 Turn On and Verify DC Office Power on the ONS 15310-CL, page 17-11
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Warning **Blank faceplates and cover panels 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, faceplates, front covers, and rear covers are in place.** Statement 1029

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 DS1/DS3 ports on the ONS15310-MA are intra-building ports and are suitable for connection only to shielded cabling grounded at both ends.** Statement 1084

See Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual, Release 8.5.

Caution Always use the supplied ESD wristband when working with a powered ONS 15310-MA. Plug the wristband cable into either of the ESD jacks, on the far left and right faceplates in the shelf.

Caution Do not install an electrical card in an ONS 15310-MA if the ambient temperature exceeds 149 degrees F (65 degrees C).

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

Step 1 Install an electrical card (DS1-28/DS3-EC1-3 or DS1-84/DS3-EC1-3) in a traffic card slot:

a. Open the card ejector.

b. Use the ejector at the top of the card and firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot.

c. Verify that the card is inserted correctly and close the ejector on the card.

Note The electrical cards are hot-pluggable, which means they can be inserted or removed without turning off the power to the ONS 15310-MA.

Step 2 Verify the electrical card LED activity:

a. All LEDs (FAIL, ACT/STBY, DS1 SF, DS3 SF) turn on for 5 seconds, then turn off.

b. The green ACT/STBY and red FAIL LED turn on for 15 seconds.

c. The red FAIL LED flashes for 10 seconds, then becomes steady red for 30 seconds.

d. While the red FAIL LED is on, the ACT/STBY LED turns green for three seconds, then turns amber. During this time, the DS1 SF and DS3 SF LEDs are amber.

e. All LEDs turn off.

f. The ACT/STBY LED turns green (active) or amber (standby).

Step 3 When you log into CTC, verify that the card appears properly in CTC node view.

Step 4 As necessary, continue with the "NTP-C156 Install the Filler Cards" procedure on page 2-21.

Stop. You have completed this procedure.

NTP-C156 Install the Filler Cards

Purpose	This procedure installs the filler cards (blank faceplates) in any unused ONS 15310-MA traffic or CTX2500 card slot. The filler cards are detectable in CTC.
Tools/Equipment	Filler card(s) for empty traffic card slots (15310-EXP-FILLER) and/or a filler card for empty CTX2500 card slots (15310-CTX-FILLER)

Prerequisite Procedures	DLP-C8 Turn On and Verify DC Office Power on the ONS 15310-CL, page 17-11
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Warning **Blank faceplates and cover panels 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, faceplates, front covers, and rear covers are in place.** Statement 1029

Caution Make sure you install the appropriate filler card for the slot where you are installing the card. Filler card(s) for empty traffic card slots have the product ID 15310-EXP-FILLER, and filler cards for empty CTX2500 card slots have the product ID 15310-CTX-FILLER.

Step 1 Open the card ejector at the top of the card.

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

Step 3 Close the ejector by firmly pushing it downward.

Note The filler cards are hot-pluggable, so they can be inserted or removed without turning off the power to the ONS 15310-MA.

Step 4 When you log into CTC, verify that the card appears properly in CTC node view.

Step 5 Continue with the "NTP-C157 Install Wires to Alarm, Timing, Craft, LAN, and UDC Pin Connections" procedure on page 2-23.

Stop. You have completed this procedure.

NTP-C157 Install Wires to Alarm, Timing, Craft, LAN, and UDC Pin Connections

Purpose	This procedure installs alarm, timing, craft (for TL1), LAN (for CTC), and UDC wires.
Tools/Equipment	Alarm In cable, unshielded cable terminated with a DB-37 connector Alarm Out cable, unshielded cable terminated with a DB-25 connector Craft port serial cable, CAT-5 terminated with RJ-45 BITS timing port cable, CAT-3/CAT-5 terminated with DB-9 connector BITS timing port cable, CAT-3/CAT-5 terminated with DB9BIT=BB9 to wire wrap adapter **Note** The cable shield must be wire-wrapped to the GND pin of the wire wrap adapter. User data channel (UDC) cable: EIA/TIA-232 port cable, CAT-5 terminated with RJ-45 Management LAN cable, CAT-5 terminated with RJ-45
Prerequisite Procedures	NTP-C150 Install the Shelf Assembly, page 2-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **The Alarm, Timing (BITS), Craft, LAN and UDC ports of ONS15310-MA are intra-building ports. The CRAFT and LAN ports (rear side) of ONS15310-MA are intra-building ports used only for setup and maintenance purposes by trained personnel and are not connected during normal operation. The BITS ports are suitable only for connecting to shielded cabling grounded at both ends.**

Caution Always use the supplied ESD wristband when working with a powered ONS 15310-MA. Plug the wristband cable into either of the ESD jacks, on the far left and right faceplates in the shelf.

Step 1 Complete the "DLP-C253 Install External Alarm Cables on the ONS 15310-MA" task on page 19-70 as needed. An alarm cable is necessary to provision external alarms and external controls.

Step 2 Complete the "DLP-C254 Install Timing Cables on the ONS 15310-MA" task on page 19-72 as needed. Timing cables are necessary to provision external timing.

Step 3 Complete the "DLP-C255 Install the Serial Cable for TL1 Craft Interface on the ONS 15310-MA" task on page 19-73 as needed. A craft cable is required to use Transaction Language One (TL1) through the craft interface.

Step 4 Complete the "DLP-C256 Install the UDC Cable on the ONS 15310-MA" task on page 19-73 to enable UDC circuits. A UDC circuit allows you to create a dedicated data channel between nodes.

Step 5 Complete the "DLP-C257 Install the LAN Cable for the CTC Interface on the ONS 15310-MA" task on page 19-74 to provide access to the CTC graphical user interface (GUI).

Step 6 Continue with the "NTP-C158 Install the Electrical Cables" procedure on page 2-24.

Stop. You have completed this procedure.

NTP-C158 Install the Electrical Cables

Purpose	This procedure describes how to install the electrical DS-1 (64-pin Champ) and DS-3/EC-1 (coaxial) cables. To carry electrical traffic on the ONS 15310-MA, you must install electrical cables.
Tools/Equipment	Shielded coaxial cable terminated with BNC connectors for DS-3/EC-1 ports 64-pin Champ connector terminated to shielded, twisted-pair cable
Prerequisite Procedures	NTP-C157 Install Wires to Alarm, Timing, Craft, LAN, and UDC Pin Connections, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

⚠ **Caution** Always use the supplied ESD wristband when working with a powered ONS 15310-MA. Plug the wristband cable into either of the ESD jacks, on the far left and right faceplates in the shelf.

Step 1 Complete the "DLP-C258 Install CHAMP Cables for DS-1 Connection" task on page 19-75 as needed.

Step 2 Complete the "DLP-C259 Install DS-3/EC-1 Cables" task on page 19-78 as needed.

Step 3 Complete the "DLP-C260 Route Cables" task on page 19-79 as needed.

Step 4 If you need to verify the wiring continuity of DS-1 or DS-3 connections between the node and the DSX panel, continue with the "NTP-C173 Install the TST-DSX Card" procedure on page 2-25. Otherwise, continue with the "NTP-C159 Install and Remove SFPs" procedure on page 2-27.

Stop. You have completed this procedure.

NTP-C173 Install the TST-DSX Card

Purpose	Use this procedure to install the TXT-DSX card and associated equipment. The TST-DSX test card enables you to verify the wiring continuity of DS-1 and DS-3/EC-1 electrical connections between the ONS 15310-MA and the external frame or DSX panel.
Tools/Equipment	Cisco ONS 15310-MA DSX Wiring Verification kit • TXT-DSX card • Handheld Receiver • AC to DC power supply • DS3 patch cords – 75-ohm male BNC connector to male WECo 440A male connector – 75-ohm male BNC connector to WECo 358 male connector – 75-ohm male BNC connector to 75-ohm male BNC connector – 75-ohm male BNC connector to LCP connector • DS1 patch cords – 100-ohm male Bantam connector to 100-ohm male Bantam connector – 100-ohm male Bantam connector to 100-ohm 310 connector • 9-pin, EIA-232 female connector to 9-pin, EIA-232 female connector
Prerequisite Procedures	NTP-C158 Install the Electrical Cables, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Used with a remote receiver, the TST-DSX card indicates whether the wiring connections are valid, which allows users to take corrective action prior to turning up service. The TST-DSX card is normally used in systems where there are no working services and likely no power applied. A hand-held remote receiver module is used with the TST-DSX card and is plugged into the DSX panel during testing using the provided cables. The receiver allows the user to initiate tests, display test status and errors, and store test results that can be transferred to a PC over an EIA-232 connection.

Caution The goal of this procedure is to test the wiring between the DSX and an empty Cisco ONS 15310-MA shelf assembly. The wiring type is DS-1 or DS-3. There must be no DS-1 or DS-3 traffic on the side of the shelf being tested. The TST-DSX card disrupts service if it is plugged into a shelf side where a DS-1 or DS-3 card is carrying traffic.

Step 1 Insert the TST-DSX card into one of the expansion slots on the shelf (either Side A, Slot 1 or 2, or Side B, Slot 5 or 6).

Step 2 If the shelf power is on, continue with Step 3. If the shelf power is not on, plug the supplied AC-to-DC adaptor into a wall outlet and plug the barrel connector of the power cable into the 48 VDC jack on the TST-DSX card faceplate.

Step 3 Set the TST-DSX card faceplate switch to the NORMAL position.

Step 4 Verify the state of the LEDs on the faceplate:

- POWER is steady on.
- ACTIVE blinks slowly, indicating that the TST-DSX is functional.
- LOOP is off.

Step 5 Verify that the backplane wiring and connectors have been installed.

Note If the ACTIVE LED is blinking rapidly, the Backplane Interface Connector (BIC) is not present.

Step 6 Turn on the power switch of the handheld receiver and observe the display.

The first display shows the receiver version number. The next display shows the following:
MANUAL TEST MODE
DS3; A; 310

The last display shows either the DS-1 or DS-3 test mode and the status of the test.

Step 7 If the display indicates 454 instead of 310 as the shelf mode, press the **MENU** key six times, press **DISPLAY** to change from 454 to 310 shelf mode, and then press the **ENTER/ACCEPT** key to save the setting.

Step 8 To change from one cable type to another (DS-1 or DS-3), press the **MENU** key once, press **DISPLAY** to change the setting, and then press **ENTER/ACCEPT** to store the setting.

Step 9 At the DSX wiring panel, insert an appropriate patch cord into the handheld receiver.

Step 10 Insert the other end of the patch cord into a port on the DSX wiring panel. The control unit's screen continuously shows the test result of any detected signal.

Note For more detailed information on using the TST-DSX card to verify and troubleshoot wiring between the ONS 15310-MA shelf and the DSX wiring panel, see the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

Stop. You have completed this procedure.

NTP-C159 Install and Remove SFPs

Purpose	This procedure installs and removes SFPs. SFPs are hot-swappable input/output devices that plug into SFP slots on the ONS 15310-MA faceplate to link the port with the fiber-optic network. SFPs are known as pluggable port modules (PPMs) in CTC. You can preprovision the multirate SFPs using the "DLP-C192 Provision a Multirate Pluggable Port Module" task on page 18-92.
Tools/Equipment	SFPs appropriate to the ONS 15310-MA. SFP types include OC-3, OC-12, OC-48, Ethernet, Gigabit Ethernet, and Fast Ethernet. Refer to the "Card Reference" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for SFP compatibility.
Prerequisite Procedures	NTP-C151 Install the Power and Ground, page 2-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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

Warning **For copper SFPs, the Ethernet ports of ONS15310-MA are intra-building ports and are suitable only for connecting to cat-5 shielded (STP) cabling grounded at both ends.**

Step 1 Complete the "DLP-C16 Install SFP Connectors" task on page 17-22 as needed.

Step 2 Complete the "DLP-C17 Remove SFP Connectors" task on page 17-23 as needed.

Step 3 Continue with the "NTP-C160 Install Optical Cables" procedure on page 2-28.

Stop. You have completed this procedure.

NTP-C160 Install Optical Cables

Purpose	This procedure describes how to install fiber-optic cables in SFPs on the ONS 15310-MA.
Tools/Equipment	Single-mode fiber jumpers with LC connectors Fiber boot Optical power meter Optical attenuators, as necessary
Prerequisite Procedures	DLP-C16 Install SFP Connectors, page 17-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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

Caution Always use the supplied ESD wristband when working with a powered ONS 15310-MA. Plug the wristband cable into either of the ESD jacks, on the far left and right faceplates in the shelf.

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

Note Inspect and clean all fiber connectors thoroughly. See the "NTP-C109 Clean Fiber Connectors" procedure on page 15-10 for instructions. Dust particles can degrade performance. Put caps on any fiber connectors that are not used.

Note To install fiber-optic cables in the ONS 15310-MA, a fiber cable with the corresponding connector type must be connected to the transmit and receive ports on the SFPs. On ONS 15310-MA ports, the transmit and receive fiber for each optical signal are contained within a single SFP port.

Step 1 Measure the optical receive levels using an optical power meter, compare the results with the allowable optical power levels for the installed SFPs, and attenuate accordingly. See Table 2-1 for the minimum and maximum levels for each SFP type.

Table 2-1 Optical Transmit and Receive Levels

SFP	Interface	Transmitter Output Power Min/Max (dBm)	Receiver Input Power Min/Max (dBm)
ONS-SI-155-L1	OC-3	–5.0 to 0	–34 to –10
ONS-SI-155-L2	OC3	–5.0 to 0	–34 to –10
ONS-SI-155-I1	OC-3	–15 to –8.0	–28 to –8
ONS-SI-622-L1	OC-12	–3.0 to 2.0	–28 to –8
ONS-SI-622-L2	OC-12	–3.0 to 2.0	–28 to –8
ONS-SI-622-I1	OC-12/OC-3	–15 to –8.0	–28 to–8
ONS-SE-155-1470 through ONS-SE-155-1610	OC-3	0 to +5	–34 to –3 (at BER 10^{-10})
ONS-SE-622-1470 through ONS-SE-622-1610	OC-12	0 to +5	–28 to –3 (at BER 10^{-10})
ONS-SI-2G-I1=	OC-48	–5.0 to 0	–18 to –0
ONS-SI-2G-L1=	OC-48	–3 to +2	–27 to –9
ONS-SI-2G-L2=	OC-48	–3 to +2	–28 to –9
ONS-SI-2G-S1=	OC-48	–10 to -3	–18 to –3
ONS-SC-2G-30.3= through ONS-SC-2G-60.6=	OC-48	0 to +4	–28 to –9

Step 2 As needed, complete the "DLP-C18 Install Fiber-Optic Cables in a 1+1 Configuration" task on page 17-24.

Step 3 As needed, complete the "DLP-C19 Install Fiber-Optic Cables for Path Protection Configurations" task on page 17-25.

Step 4 As needed, gently route the fiber cables away from the shelf. You might want to use the optional tie-down bar.

Step 5 Continue with the "NTP-C164 Perform the Shelf Installation Acceptance Test" procedure on page 2-29.

Stop. You have completed this procedure.

NTP-C164 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 2, "Install the Cisco ONS 15310-MA"
Required/As Needed	Required

Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Complete Table 2-2 on page 2-30 by verifying that each procedure was completed.

Table 2-2 ONS 15310-MA Shelf Installation Task Summary

Description	Completed
NTP-C149 Unpack and Inspect the ONS 15310-MA Shelf Assembly, page 2-5	
NTP-C150 Install the Shelf Assembly, page 2-5	
NTP-C169 Install the Cable Management Bracket, page 2-6	
NTP-C167 Install the EIAs, page 2-10	
NTP-C151 Install the Power and Ground, page 2-12	
NTP-C152 Install the Fan-Tray Assembly, page 2-14	
NTP-C153 Install the CTX2500 Cards, page 2-16	
NTP-C154 Install the Ethernet Cards, page 2-19	
NTP-C155 Install the Electrical Cards, page 2-20	
NTP-C156 Install the Filler Cards, page 2-21	
NTP-C157 Install Wires to Alarm, Timing, Craft, LAN, and UDC Pin Connections, page 2-23	
NTP-C158 Install the Electrical Cables, page 2-24	
NTP-C173 Install the TST-DSX Card, page 2-25	
NTP-C159 Install and Remove SFPs, page 2-27	
NTP-C160 Install Optical Cables, page 2-28	

Step 2 Check each wire and cable connection to make sure all cables are locked securely. If a wire or cable is loose, return to the appropriate procedure in this chapter to correct it.

Step 3 Complete the "DLP-C20 Measure Voltage" task on page 17-28.

Stop. You have completed this procedure.

NTP-C161 Preprovision an SFP Slot

Purpose	This procedure preprovisions SFPs, which are referred to as pluggable port modules (PPMs) in CTC. OC-3, OC-12, OC-48, and multirate (OC-3/OC-12) PPMs are compatible with the ONS 15310-MA. The SFP slots are located on the CTX2500 card.
Tools/Equipment	None
Prerequisite Procedures	Chapter 3, "Connect the PC and Log into the GUI"
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 to log into an ONS 15310-MA on the network.

Step 2 Click the **Alarms** tab:

a. Verify that the alarm filter is not turned on. See the "DLP-C88 Disable Alarm Filtering" task on page 17-109 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 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

c. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export alarm and condition information.

Step 3 In node view, double-click the CTX2500 card.

Step 4 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 5 In the Pluggable Port Modules pane, click **Create**. The Create PPM dialog box appears.

Step 6 In the Create PPM dialog box, complete the following:

- PPM—Click the slot number where the SFP is installed from the drop-down list.
- PPM Type—Click the number of ports supported by your SFP from the drop-down list. If only one port is supported, **PPM (1 port)** is the only option.

Step 7 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 is installed. After the SFP is installed, the row on the pane turns white and the column lists the equipment name.

Step 8 Verify that the PPM appears in the list on the Pluggable Port Modules pane. If it does not, repeat Steps 5 through 7.

Step 9 Repeat Steps 5 through 8 to provision a second PPM.

Step 10 Click **OK**.

Step 11 When you are ready to install the SFP, complete the "DLP-C16 Install SFP Connectors" task on page 17-22. If you preprovisioned a multirate SFP, you must select the line rate using the "DLP-C193 Provision the Optical Line Rate" task on page 18-92.

Stop. You have completed this procedure.

NTP-C162 Preprovision a Card Slot

Purpose	This procedure describes how to preprovision a slot in the software before physical card installation.
Tools/Equipment	None
Prerequisite Procedures	Chapter 3, "Connect the PC and Log into the GUI"
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node where you want to preprovision the slot. If you are already logged in, continue with Step 2.

Step 2 Right-click the empty slot where you will later install a card.

Step 3 From the Add Card shortcut menu, navigate to Ethernet or DSn and choose the card type you want (CE-100T-8 or ML-100T-8 for Ethernet; DS1-28/DS3-EC1-3 or DS1-84/DS3-EC1-3 for DSn).

Note When you preprovision a slot, the card appears purple in the CTC shelf display. When you physically install a card in the slot, the card appears white in the CTC shelf display.

Stop. You have completed this procedure.

NTP-C163 Remove and Replace a Card

Purpose	This procedure describes how to remove and replace cards in the ONS 15310-MA shelf.
Tools/Equipment	None
Prerequisite Procedures	NTP-C154 Install the Ethernet Cards, page 2-19 NTP-C158 Install the Electrical Cables, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **Blank faceplates and cover panels 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, faceplates, front covers, and rear covers are in place.** Statement 1029

Step 1 If you are not logged into CTC and you need to remove a card, continue with Step 3. When you log into CTC, troubleshoot the mismatched equipment (MEA) or Improper Removal (IMPRMVL) alarm using the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

Step 2 If you are logged into CTC, on the node view shelf graphic 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 CTX2500 card. To replace a CTX2500 card, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.
- The card is part of an optical protection group; see the "DLP-C138 Delete a Protection Group" task on page 18-43.

Note 1:1 electrical protection groups are created automatically in the ONS 15310-MA and can only be deleted after the protect card of a 1:1 protection group is deleted.

- The card has circuits; see the "DLP-C120 Delete Overhead Circuits" task on page 18-28 and the "DLP-C115 Delete Circuits" task on page 18-21.
- The card is being used for timing; see the "DLP-C139 Change the Node Timing Source" task on page 18-44.
- The card has a data communications channel (DCC) termination; see the "DLP-C154 Delete a Section DCC Termination" task on page 18-56 or the "DLP-C155 Delete a Line DCC Termination" task on page 18-57.

Note If you do not remove a card from the shelf after you delete it in CTC, it will reboot and reappear in CTC.

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:

- NTP-C153 Install the CTX2500 Cards, page 2-16
- NTP-C154 Install the Ethernet Cards, page 2-19
- NTP-C155 Install the Electrical Cards, page 2-20

Stop. You have completed this procedure.

NTP-C168 Install the Front Door

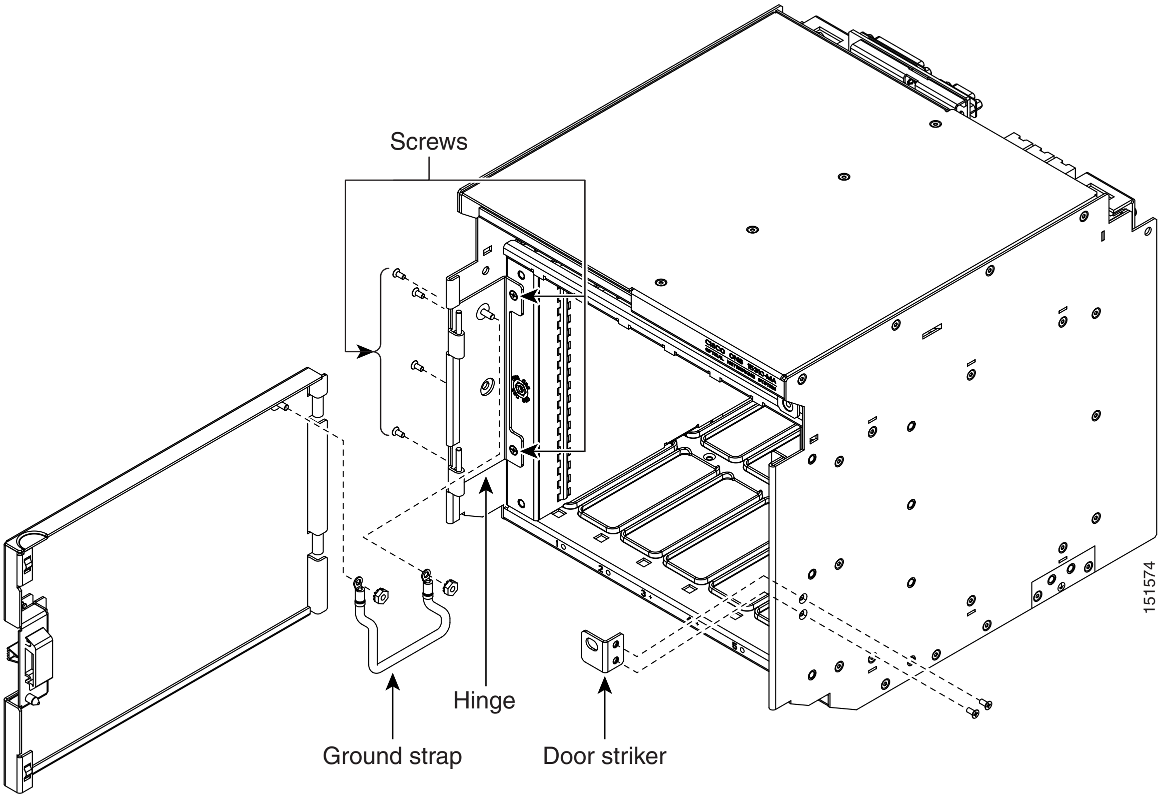
Purpose	This procedure replaces the front door and door ground strap after installing cards and fiber-optic cables.
Tools/Equipment	Front-door kit (53-2617-XX) • Door hinge • Door striker • 4-40 screws (8) • Ground cable • Hex nuts (2)
Prerequisite Procedures	NTP-C150 Install the Shelf Assembly, page 2-5
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

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

Caution Always use the supplied ESD wristband when working with a powered ONS 15310-MA. Plug the wristband cable into either of the ESD jacks, on the far left and right faceplates in the shelf.

Step 1 Place the door hinge flush against the inside of the ONS 15310-MA chassis flange on the left (Figure 2-9).

Figure 2-9 Installing the Front Door



Step 2 Line up the four screw holes on the door hinge with the corresponding screw holes on the flange of the shelf assembly. Make sure the other two holes on the hinge line up with the two holes on the ESD faceplate on the left side of the shelf.

Step 3 Approaching the shelf assembly from the left side, install four 4-40 screws to attach the door hinge to the chassis flange.

Step 4 Install two 4-40 screws through the hinge into the ESD faceplate.

Step 5 Attach the door striker to the right side of the chassis using the remaining two 4-40 screws.

Step 6 Slide the front door downward onto the hinge pins.

Step 7 Using the 5/16-inch nut driver, attach the ground cable to the threaded studs on the door and hinge with two hex nuts. Ensure the ground cable is looped or bent downward to avoid being pinched or caught when the door is closed.

Step 8 Close the front door.

⚠ **Caution** Be careful not to crimp any cables that are connected to the installed cards.

Stop. You have completed this procedure.

NTP-C191 Install the Rear Cover

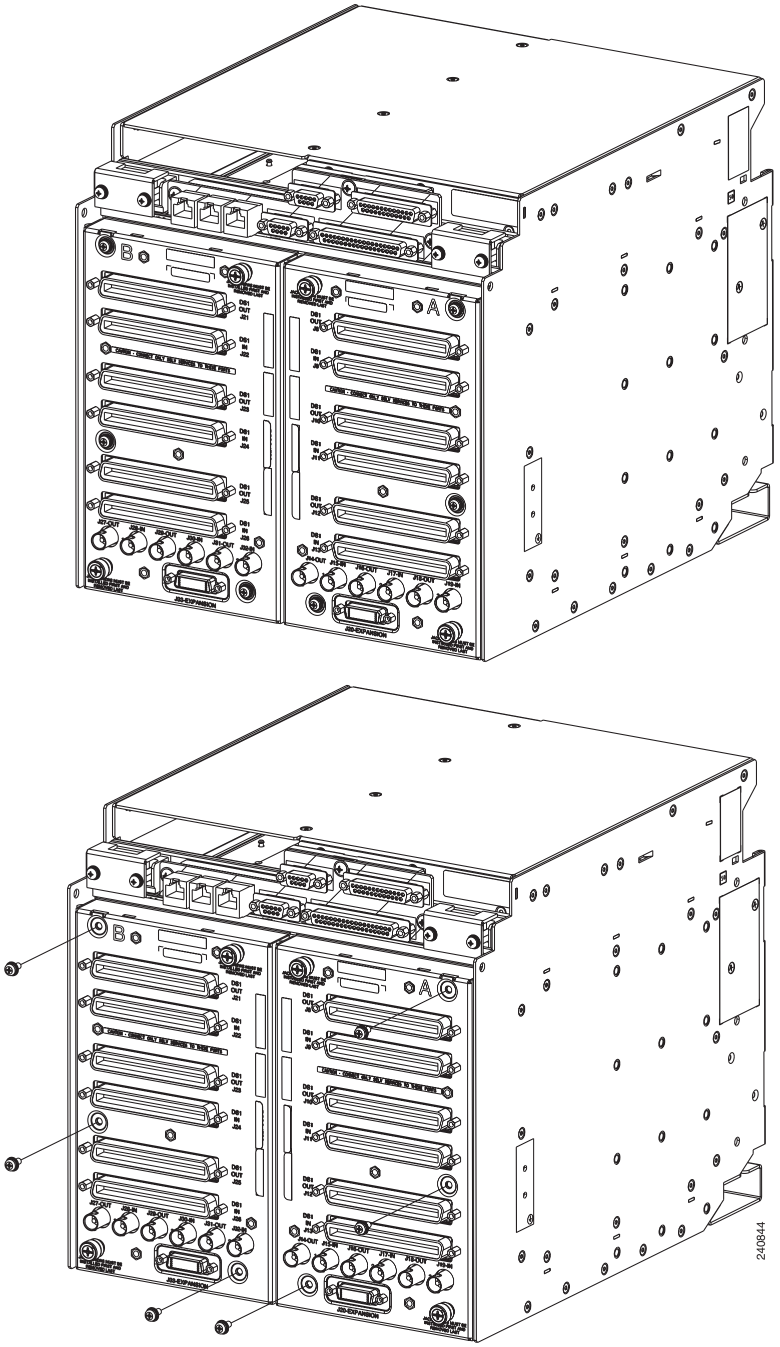
Purpose	This procedure explains how to install the rear cover on an ONS 15310-MA shelf.
Tools/Equipment	• #2 Phillips screwdriver • 1/4-inch nut driver • Six 1/4-inch hexagonal standoffs 6-32 x 3.3.25
Prerequisite Procedures	NTP-C158 Install the Electrical Cables, page 2-24
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

⚠ **Caution** Always use the supplied ESD wristband when working with a powered ONS 15310-MA. For detailed instructions on how to wear the ESD wristband, refer to the Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide.

Note Connect all cables on the backplane before installing the rear cover.

Step 1 Using a #2 Phillips screw driver, remove the six panhead screws from the Electrical Interface Assemblies (EIAs) located on the A-side and B-side of the backplane Figure 2-10.

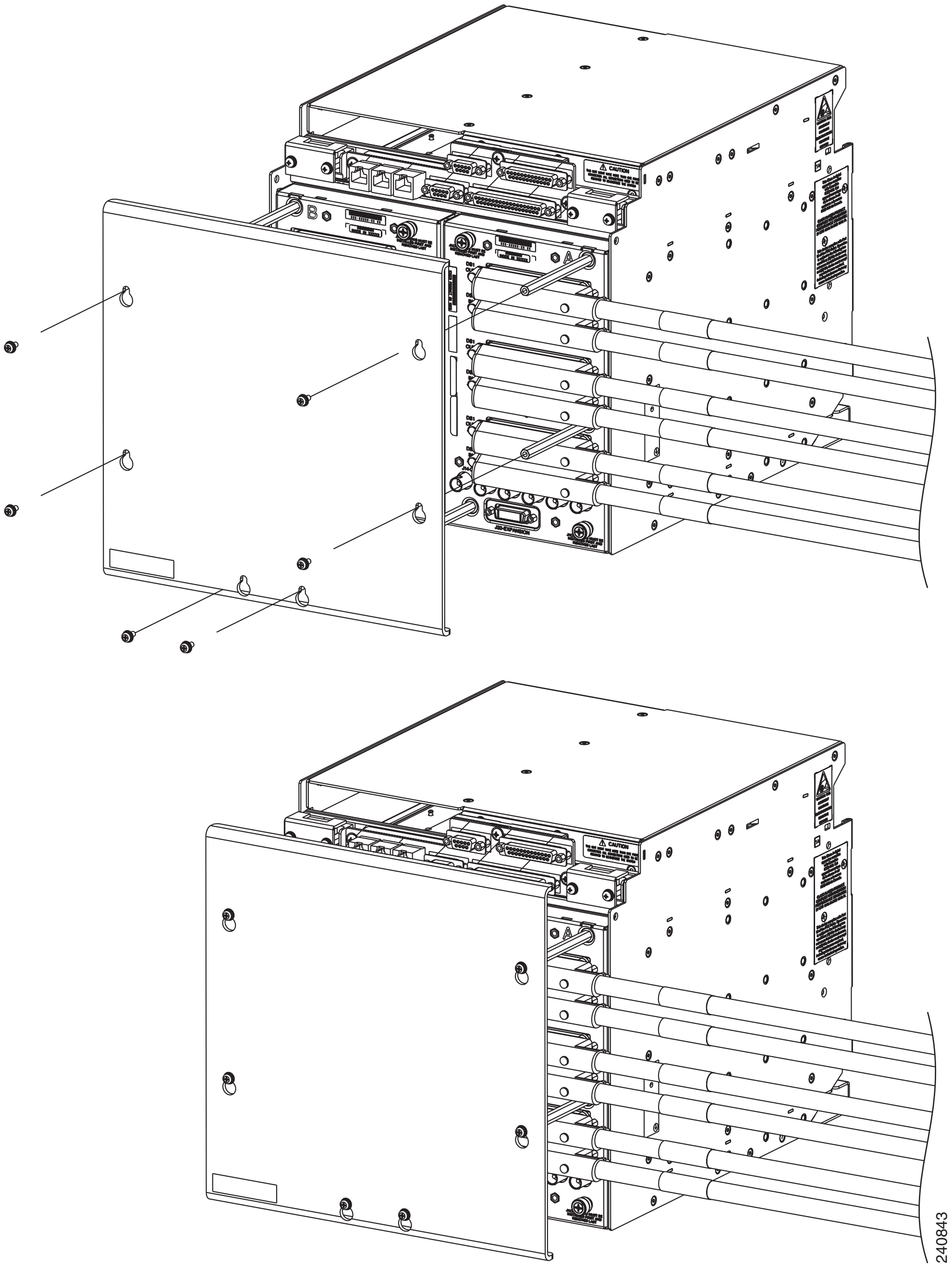
Figure 2-10 Removing the Panhead Screws



Step 2 Using the 1/4-inch nut driver, install the six hexagonal standoffs onto the mounting holes that held the six panhead screws.

Step 3 Align the holes on the rear cover with the hexagonal standoffs.

Figure 2-11 Installing the Rear Cover



Step 4 Install and tighten the six panhead screws onto the holes on the hexagonal standoffs.

Note You can also reverse the order of the procedure, and install the panhead screws onto the hexagonal standoffs first, place the rear cover on the standoffs, and finally tighten the panhead screws. The rear cover has oval cut-outs to allow this operation.

Stop. You have completed this procedure.

CHAPTER 3

Connect the PC and Log into the GUI

This chapter explains how to connect Windows PCs and Solaris workstations to the Cisco ONS 15310-CL and Cisco ONS 15310-MA, and how to log into Cisco Transport Controller (CTC) software. CTC is the Cisco ONS 15310-CL and Cisco ONS 15310-MA Operation, Administration, Maintenance and Provisioning (OAM&P) user interface. Procedures for connecting to the ONS 15310-CL and ONS 15310-MA using Transaction Language 1 (TL1) are provided in the *Cisco ONS SONET TL1 Command Guide*.

Before You Begin

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

1. NTP-C13 Set Up Computer for CTC, page 3-2—Complete this procedure if your PC or workstation has never been connected to an ONS 15310-CL.
2. NTP-C14 Set Up CTC Computer for Local Craft Connection to the Node, page 3-3—Complete this procedure to set up your computer for an onsite craft connection to the ONS 15310-CL and ONS 15310-MA.
3. NTP-C15 Set Up a CTC Computer for a Corporate LAN Connection to the Node, page 3-5—Complete this procedure to set up your computer to connect to the ONS 15310-CL and ONS 15310-MA using a corporate LAN.
4. NTP-C16 Set Up a Remote Access Connection to the Node, page 3-6—Complete this procedure to set up your computer for remote modem access to the ONS 15310-CL and ONS 15310-MA.
5. NTP-C17 Log into the GUI, page 3-7—Complete this procedure to log into CTC.
6. NTP-C147 Use the CTC Launcher Application to Manage Multiple ONS Nodes, page 3-8—Complete this procedure to use the CTC Launcher Application.

NTP-C13 Set Up Computer for CTC

Purpose	This procedure explains how to configure your Windows PC or Solaris workstation to run CTC.
Tools/Equipment	Cisco ONS 15310-CL Release 8.5 software CD or Cisco ONS 15310-MA Release 8.5 software CD
Prerequisite Procedures	Chapter 1, "Install the Cisco ONS 15310-CL" or Chapter 2, "Install the Cisco ONS 15310-MA"
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. To log into nodes running Software R4.5 or earlier, you must uninstall JRE 1.4.2 or 5.0 and install JRE 1.3.1. JRE 5.0 is provided on the Software R8.5 software CD. Complete the "DLP-C35 Change the JRE Version" task on page 17-50 as needed.

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

- To install Netscape 7.x on a Windows PC, download the browser from the following site: http://channels.netscape.com/ns/browsers/default.jsp
- To install Internet Explorer 6.x on a PC, download the browser at the following site: http://www.microsoft.com/windows/ie/default.mspx
- To install Mozilla 1.7 on a Solaris 9 or 10 workstation, download the browser from the following site: http://www.mozilla.org/releases/#1.7.12

Note For Windows PCs, only Internet Explorer 6.x and Netscape 7.x are supported. For Solaris workstations, Mozilla 1.7 is the only supported browser.

Step 2 Complete the "DLP-C231 Adjust the Java Virtual Memory Heap Size" task on page 19-31 to increase the size of the JVM heap in order to improve the CTC performance.

Step 3 Complete one of the following:

- If your computer is a Windows PC, complete the "DLP-C21 Run the CTC Installation Wizard for Windows" task on page 17-29, then go to Step 4.
- If your computer is a UNIX workstation, complete the "DLP-C22 Run the CTC Installation Wizard for UNIX" task on page 17-32.

Step 4 When your PC or workstation is set up, continue with one of the following procedures:

- NTP-C14 Set Up CTC Computer for Local Craft Connection to the Node, page 3-3
- NTP-C15 Set Up a CTC Computer for a Corporate LAN Connection to the Node, page 3-5
- NTP-C16 Set Up a Remote Access Connection to the Node, 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.

Stop. You have completed this procedure.

NTP-C14 Set Up CTC Computer for Local Craft Connection to the Node

Purpose	This procedure sets up a PC running Windows or a UNIX/Solaris workstation for an onsite local craft connection to the node.
Tools/Equipment	Network interface card (NIC), also referred to as an Ethernet card Straight-through (CAT-5) LAN cable
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
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 on your CTC connection environment. For initial setup, use Option 1 or 3 if you are setting up a Windows PC. Use Option 4 if you are setting up a Solaris workstation.

Table 3-1 CTC Computer Setup for Local Craft Connections to the ONS 15310-CL and ONS 15310-MA

Option	CTC Connection Environment	CTC Computer Setup Task
1	• You are connecting from a Windows PC. • You will connect to one ONS 15310-CL or ONS 15310-MA. If you connect to multiple nodes, you might need to configure your computer's IP settings each time you connect to the node. • You need to access non-ONS applications such as ping and tracert (trace route).	DLP-C23 Set Up a Windows PC for Craft Connection to an ONS 15310-CL or ONS 15310-MA on the Same Subnet Using Static IP Addresses, page 17-35
2	• You are connecting from a Windows PC. • Your network uses Dynamic Host Configuration Protocol (DHCP) for assignment of host IP addresses. • The CTC computer is provisioned for DHCP. • The ONS 15310-MA or ONS 15310-CL has DHCP forwarding enabled. • The ONS 15310-CL or ONS 15310-MA is connected to a DHCP server. **Note** The ONS 15310-CL and ONS 15310-MA do not provide IP addresses. If DHCP is enabled, it passes DHCP requests to an external DHCP server.	DLP-C24 Set Up a Windows PC for Craft Connection to an ONS 15310-CL or ONS 15310-CL Using Dynamic Host Configuration Protocol, page 17-37 **Note** Do not use this task for initial node turn-up. Use the task only if DHCP forwarding is enabled on the ONS 15310-CL or ONS 15310-MA. By default, DHCP is not enabled. To enable it, see the "NTP-C21 Set Up CTC Network Access" procedure on page 4-6.
3	• You are connecting from a Windows PC. • You will connect to ONS 15310-CL or ONS 15310-MA nodes 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 applications such as ping and tracert (trace route). • You will connect to the ONS 15310-CL or ONS 15310-MA LAN port either directly or through a hub.	DLP-C25 Set Up a Windows PC for Craft Connection to an ONS 15310-CL or ONS 15310-MA Using Automatic Host Detection, page 17-40
4	• You are connecting from a Solaris Workstation. • You will connect to one ONS 15310-CL or ONS 15310-MA. If you connect to multiple nodes, you might need to configure your computer's IP settings each time you connect to an ONS 15310-CL or ONS 15310-MA. • You need to access non-ONS applications such as ping and tracert (trace route).	DLP-C265 Set Up a Solaris Workstation for a Craft Connection to an ONS 15310-CL or ONS 15310-MA, page 19-80

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

- RJ-45 (CRAFT) port on the ONS 15310-CL or ONS 15310-MA
- RJ-45 (LAN) port on a hub or switch to which the ONS 15310-CL or ONS 15310-MA is physically connected

Note For instructions on crimping your own straight-through (CAT-5) LAN cables, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

Note For initial shelf turn-up, you should connect your PC directly to the CRAFT port on the ONS 15310-CL or ONS 15310-MA. On the ONS 15310-CL, the CRAFT port is located on the front of the node. On the ONS 15310-MA, the CRAFT port is located on the CTX2500 card.

Step 3 After setting up the CTC computer, continue with the "NTP-C17 Log into the GUI" procedure on page 3-7, as applicable.

Stop. You have completed this procedure.

NTP-C15 Set Up a CTC Computer for a Corporate LAN Connection to the Node

Purpose	This procedure sets up your computer to access the ONS 15310-CL or ONS 15310-MA through a corporate LAN.
Tools/Equipment	NIC, also referred to as an Ethernet card Straight-through (CAT-5) LAN cable
Prerequisite Procedures	• NTP-C13 Set Up Computer for CTC, page 3-2 • The ONS 15310-CL or ONS 15310-MA must be provisioned for LAN connectivity, including IP address, subnet mask, and default gateway. • The ONS 15310-CL or ONS 15310-MA must be physically connected to the corporate LAN.
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 15310-CL or ONS 15310-MA, 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 2000 and XP) or **Obtain an IP address from a DHCP server** (Windows NT 4.0).
- If your LAN requires that DNS or 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 15310-CL/ONS 15310-MA nodes as exceptions. To disable proxy service, complete one of the following tasks, depending on the web browser that you use:

- DLP-C27 Disable Proxy Service Using Internet Explorer (Windows), page 17-42
- DLP-C28 Disable Proxy Service Using Netscape (Windows), page 17-43

Step 4 Continue with the "NTP-C17 Log into the GUI" procedure on page 3-7.

Stop. You have completed this procedure.

NTP-C16 Set Up a Remote Access Connection to the Node

Purpose	This procedure connects an ONS 15310-CL or ONS 15310-MA using a LAN modem. To complete this procedure: • A LAN modem must be connected to the ONS 15310-CL or ONS 15310-MA. • The LAN modem must be provisioned for the ONS 15310-CL or ONS 15310-MA. To run CTC, the modem must be provisioned for Ethernet access.
Tools/Equipment	Modem and modem documentation
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Connect the modem to the ONS 15310-CL or ONS 15310-MA RJ-45 (CRAFT) port. On the 15310-CL, the CRAFT port is located on the front of the node. On the 15310-MA, the CRAFT port is located on the CTX2500 card faceplate.

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

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

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 xlviii for more information.

Step 3 Continue with the "NTP-C17 Log into the GUI" procedure on page 3-7

Stop. You have completed this procedure.

NTP-C17 Log into the GUI

Purpose	This procedure logs into CTC, the graphical user interface software used to manage the ONS 15310-CL and ONS 15310-MA. This procedure includes optional node login tasks.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2 One of the following procedures: • NTP-C14 Set Up CTC Computer for Local Craft Connection to the Node, page 3-3. or • NTP-C15 Set Up a CTC Computer for a Corporate LAN Connection to the Node, page 3-5, or • NTP-C16 Set Up a Remote Access Connection to the Node, page 3-6
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44.

If a Java Plug-in Security Warning dialog box appears during log in, complete the "DLP-C30 Install Public-Key Security Certificate" task on page 17-47 to install the public-key security certificate required by Software Release 4.1 and later.

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 the CTC has been found in the network and offers to install the CTC software upgrade JAR files. 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-C31 Create Login Node Groups" task on page 17-47. Login node groups allow you to view and manage nodes that have an IP connection but no data communications channel (DCC) connection to the login node.

Step 3 As needed, complete the "DLP-C32 Add a Node to the Current Session or Login Group" task on page 17-48.

Step 4 As needed, complete the "DLP-C33 Delete a Node from the Current Session or Login Group" task on page 17-49.

Step 5 As needed, complete the "DLP-C36 Configure the CTC Alerts Dialog for Automatic Popup" task on page 17-51.

Stop. You have completed this procedure.

NTP-C147 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-C13 Set Up Computer for CTC, page 3-2 One of the following procedures: • NTP-C14 Set Up CTC Computer for Local Craft Connection to the Node, page 3-3 • NTP-C15 Set Up a CTC Computer for a Corporate LAN Connection to the Node, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note JRE 1.5 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-C266 Install the CTC Launcher Application from a Release 8.5 Software CD, page 19-82
- DLP-C267 Install the CTC Launcher Application from a Release 8.5 Node, page 19-82

Step 2 As needed, complete the "DLP-C268 Connect to ONS Nodes Using the CTC Launcher" task on page 19-83 to connect to an ONS network element with direct IP connectivity.

Step 3 As needed, complete the "DLP-C275 Install or Reinstall the CTC JAR Files" task on page 19-91 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-C269 Create a TL1 Tunnel Using the CTC Launcher, page 19-84
- DLP-C270 Create a TL1 Tunnel Using CTC, page 19-85

Step 5 As needed, complete the "DLP-C271 View TL1 Tunnel Information" task on page 19-86.

Step 6 As needed, complete the "DLP-C272 Edit a TL1 Tunnel Using CTC" task on page 19-88.

Step 7 As needed, complete the "DLP-C273 Delete a TL1 Tunnel Using CTC" task on page 19-89.

Stop. You have completed this procedure.

CHAPTER 4

Turn Up a Node

This chapter explains how to provision a single Cisco ONS 15310-CL or Cisco ONS 15310-MA node and turn it up for service.

Before You Begin

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

- Chapter 1, "Install the Cisco ONS 15310-CL"
- Chapter 2, "Install the Cisco ONS 15310-MA"
- 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-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2—Complete this procedure first for the ONS 15310-CL.
2. NTP-C148 Verify Card and SFP Installation for the ONS 15310-MA, page 4-3—Complete this procedure first for the ONS 15310-MA.
3. NTP-C19 Create Users and Assign Security, page 4-4—Complete this procedure to create Cisco Transport Controller (CTC) users and assign their security levels.
4. NTP-C20 Set Up Name, Date, Time, and Contact Information, page 4-4—Continue with this procedure to set the node name, date, time, location, and contact information for a node.
5. NTP-C21 Set Up CTC Network Access, page 4-6— Continue with this procedure to provision the IP address, default router, subnet mask, and network configuration settings including Dynamic Host Configuration Protocol (DHCP), Internet Inter-Orb Protocol (IIOP), proxy server, static routes, Open Shortest Path First (OSPF) protocol, and Routing Information Protocol (RIP).
6. NTP-C177 Set Up the ONS 15310 in EMS Secure Access, page 4-7—Continue with this procedure to connect the CTC in secure mode.
7. NTP-C22 Set Up the ONS 15310-CL or ONS 15310-MA for Firewall Access, page 4-8—Continue with this procedure if the ONS 15310-CL or ONS 15310-MA will be accessed behind firewalls.
8. NTP-C276 Create FTP Host, page 4-10—Continue with this procedure to create FTP host for ENE database backup.
9. NTP-C23 Set Up Timing, page 4-11—Continue with this procedure to set up SONET timing references for the node.
10. NTP-C141 Create Optical Protection Groups for the ONS 15310-CL, page 4-12—As needed, complete this procedure to set up optical protection groups for ONS 15310-CL ports.

11. NTP-C142 Create Protection Groups for the ONS 15310-MA, page 4-13—As needed, complete this procedure to set up protection groups for the ONS 15310-MA.
12. NTP-C25 Set Up SNMP, page 4-15—Complete this procedure if simple network management protocol (SNMP) will be used for network monitoring.
13. NTP-C131 Provision OSI, page 4-16—Complete this procedure if the ONS 15310-CL or ONS 15310-MA will be connected to 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-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL

Purpose	This procedure verifies that the ONS 15310-CL node is ready for turn up.
Tools/Equipment	An engineering work order, site plan, or other document specifying the ONS 15310-CL card installation
Prerequisite Procedures	Chapter 1, "Install the Cisco ONS 15310-CL"
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 If you installed an Ethernet card, verify that it displays a solid green ACT (active) LED on the card faceplate.

Step 2 To install a small-form factor pluggable (SFP) connector for the ONS 15310-CL, complete the "DLP-C16 Install SFP Connectors" task on page 17-22. To remove an SFP, complete the "DLP-C17 Remove SFP Connectors" task on page 17-23.

Step 3 Verify that fiber-optic cables are installed and connected to the locations indicated in the site plan. If the fiber-optic cables are not installed, complete the "NTP-C8 Install Optical Cables" procedure on page 1-12 for the ONS 15310-CL.

Step 4 Verify that fiber is routed correctly in the shelf assembly.

Step 5 Continue with the "NTP-C20 Set Up Name, Date, Time, and Contact Information" procedure on page 4-4.

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

NTP-C148 Verify Card and SFP Installation for the ONS 15310-MA

Purpose	This procedure verifies that the ONS 15310-MA node is ready for turn up.
Tools/Equipment	An engineering work order, site plan, or other document specifying the ONS 15310-MA card installation
Prerequisite Procedures	Chapter 2, "Install the Cisco ONS 15310-MA"
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 According to your site plan, verify that the CTX2500s are installed.

Step 2 Verify that the green ACT (active) LED is illuminated on one CTX2500 and the amber STBY (standby) LED is illuminated on the second CTX2500.

Note If the CTX2500cards are not installed, or if their LEDs are not illuminated as described, do not proceed. Repeat the "NTP-C153 Install the CTX2500 Cards" procedure on page 2-16, or refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* to resolve installation problems before proceeding to the next step.

Step 3 If you installed an electrical card, verify that it displays a solid green ACT (active) LED on the card faceplate. As necessary, complete the "NTP-C155 Install the Electrical Cards" procedure on page 2-20.

Step 4 If you installed an electrical card, verify that the electrical cables are installed. As necessary, complete the "NTP-C158 Install the Electrical Cables" procedure on page 2-24.

Step 5 If you installed an Ethernet card, verify that it displays a solid green ACT (active) LED. To perform Ethernet card installation, complete the "NTP-C154 Install the Ethernet Cards" procedure on page 2-19.

Step 6 To install a small-form factor pluggable (SFP) connector for the ONS 15310-MA, complete the "DLP-C16 Install SFP Connectors" task on page 17-22. To remove an SFP, complete the "DLP-C17 Remove SFP Connectors" task on page 17-23.

Step 7 Verify that fiber-optic cables are installed and connected to the locations indicated in the site plan. If the fiber-optic cables are not installed, complete the "NTP-C160 Install Optical Cables" procedure on page 2-28 for the ONS 15310-MA.

Step 8 Verify that fiber is routed correctly in the shelf assembly.

Step 9 Continue with the "NTP-C20 Set Up Name, Date, Time, and Contact Information" procedure on page 4-4.

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

NTP-C19 Create Users and Assign Security

Purpose	This procedure creates ONS 15310-CL or ONS 15310-MA users and assigns their security levels.
Tools/Equipment	None
Prerequisite Procedures	NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 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 15310-CL or ONS 15310-MA can be used to set up other ONS 15310 users. You can add up to 500 users to one ONS 15310.

Step 2 Complete the "DLP-C37 Create a New User on a Single Node" task on page 17-51 or the "DLP-C38 Create a New User on Multiple Nodes" task on page 17-52 as needed.

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

Step 3 If you want to modify the security policy settings, complete the "NTP-C83 Modify Users and Change Security" procedure on page 11-6.

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

NTP-C20 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-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 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 TL1 compliance, names must begin with an alpha character and have no more than 20 alphanumeric characters.
- Contact—Type the name of the node contact person and the contact phone number up to 255 characters (optional).
- 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 also position nodes manually on the network view map. Press Ctrl while you drag and drop the node icon to the desired location. To create a network map that is visible to all ONS 15310-CL and ONS 15310-MA users, complete the "NTP-C35 Create a Logical Network Map" procedure on page 5-26. This procedure requires a Superuser security level.

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 have 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 15310-CL or ONS 15310-MA 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-C75 Display Alarms and Conditions Using Time Zone" task on page 17-93.

  Note Using an NTP or SNTP server ensures that all ONS 15310-CL or ONS 15310-MA 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, type the IP address of one of the following:

  - An NTP/SNTP server connected to the ONS 15310-CL or ONS 15310-MA
  - Another ONS 15310-CL or ONS 15310-MA with NTP/SNTP enabled that is connected to the ONS 15310-CL or ONS 15310-MA

  If you check the gateway network element (GNE) for the ONS 15310-CL or ONS 15310-MA proxy server, end ONS 15310 network elements (ENEs) must reference the gateway ONS 15310 for NTP/SNTP timing. For more information about the proxy server feature, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Caution If you reference another ONS 15310-CL or ONS 15310-MA for the NTP/SNTP server, make sure the second ONS 15310 references an NTP/SNTP server and not the first ONS 15310 (that is, do not create an NTP/SNTP timing loop by having two ONS 15310s reference each other).

- Date—If the Use NTP/SNTP Server check box is not checked, type the current date in the format mm/dd/yyyy, for example, September 24, 2004 is 09/24/2004.
- Time—If the Use NTP/SNTP Server check box is not checked, type the current time in the format hh:mm:ss, for example, 11:24:58. The ONS 15310-CL and ONS 15310-MA 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 menu 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 is using Daylight Savings Time.

Note The ONS 15310-CL and ONS 15310-MA clock is not running on battery backup, if power is lost the date and time must be reset.

- Insert AIS-V on STS-1 SD-P—Check this check box if you want AIS-Vs inserted on VT circuits carried by STS-1s when the STS-1 crosses its SD-P 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 to 5 to enter the corrections. If the information is correct, continue with the "NTP-C21 Set Up CTC Network Access" procedure on page 4-6.

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

NTP-C21 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, proxy server settings, static routes, Open Shortest Path First (OSPF) protocol, Routing Information Protocol (RIP), and designated SOCKS servers.
Tools/Equipment	None
Prerequisite Procedures	NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-C39 Provision IP Settings" task on page 17-53 to provision the ONS 15310-CL or ONS 15310-MA IP address, subnet mask, default router, DHCP server, IIOP listener port, and proxy server settings.

Step 3 If you want to turn on the ONS 15310-MA secure mode, which allows two IPv4 addresses to be provisioned for the node if CTX2500 cards are installed, complete the "DLP-C289 Enable Node Secure Mode" task on page 19-94.

Step 4 If static routes are needed, complete the "DLP-C40 Create a Static Route" task on page 17-55. Refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for further information about static routes.

Step 5 If the ONS 15310-CL or ONS 15310-MA 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-C41 Set Up or Change Open Shortest Path First Protocol" task on page 17-56.

Step 6 If the ONS 15310-CL or ONS 15310-MA is connected to a LAN or WAN that uses RIP, complete the "DLP-C42 Set Up or Change Routing Information Protocol" task on page 17-58.

Step 7 Complete the "DLP-C274 Provision the Designated SOCKS Servers" task on page 19-89 after the network is provisioned and one or more of the following conditions exist:

- SOCKS proxy is enabled.
- The ratio of ENEs to GNEs is greater than eight to one.
- Most ENEs do not have LAN connectivity.

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

NTP-C177 Set Up the ONS 15310 in EMS Secure Access

Purpose	This procedure provisions ONS 15310s and CTC computers for secure access.
Tools/Equipment	None
Prerequisite Procedures	NTP-C21 Set Up CTC Network Access, page 4-6
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-C22 Set Up the ONS 15310-CL or ONS 15310-MA for Firewall Access

Purpose	This procedure provisions ONS 15310-CL nodes, ONS 15310-MA nodes, and CTC computers for access through firewalls. If an ONS 15310 or CTC computer resides behind a firewall that uses port filtering, you must enable an Internet Inter-ORB Protocol (IIOP) port on the ONS 15310 and/or CTC computer, depending on whether one or both devices reside behind a firewall.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at a node that is behind the firewall. If you are already logged in, continue with Step 2.

Step 2 If the ONS 15310-CL or ONS 15310-MA node resides behind a firewall, complete the "DLP-C43 Provision the IIOP Listener Port on the ONS 15310-CL or ONS 15310-MA" task on page 17-59.

Figure 4-1 shows an ONS 15310-CL in a protected network and the CTC computer in an external network. For the computer to access the ONS 15310-CL/ONS 15310-MA nodes, you must provision the IIOP listener port specified by your firewall administrator on the ONS 15310-CL/ONS 15310-MA.

Figure 4-1 ONS 15310-CL Nodes Residing Behind a Firewall

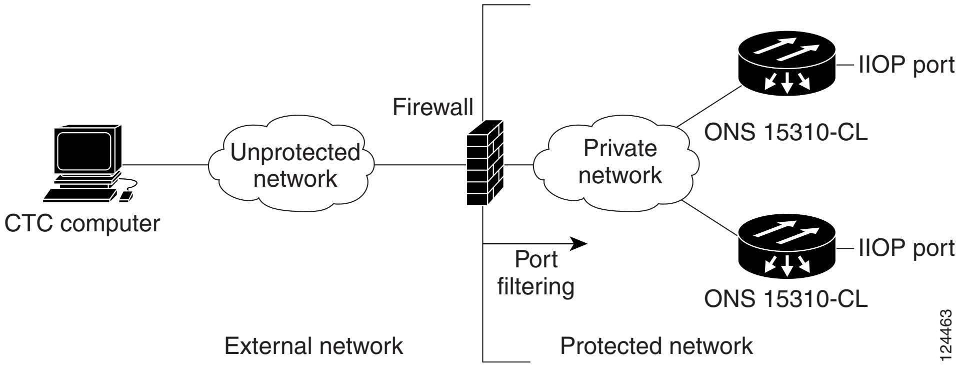
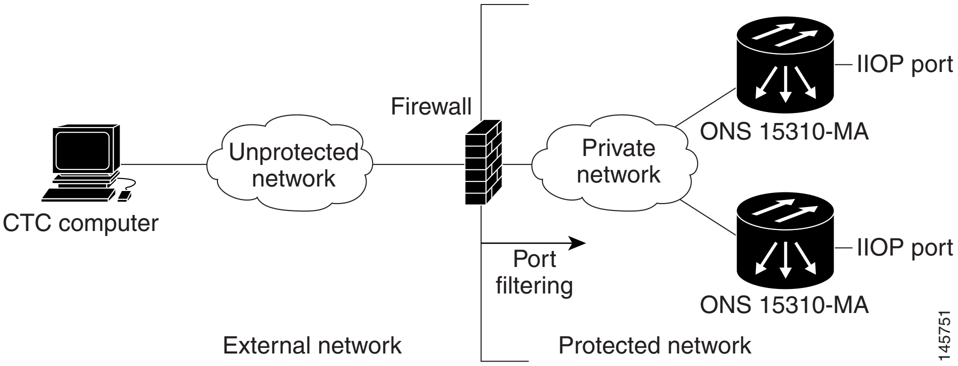


Figure 4-2 shows an ONS 15310-MA in a protected network and the CTC computer in an external network. For the computer to access the ONS 15310-CL/ONS 15310-MA nodes, you must provision the IIOP listener port specified by your firewall administrator on the ONS 15310-CL/ONS 15310-MA.

Figure 4-2 ONS 15310-MA Nodes Residing Behind a Firewall



Step 3 If the CTC computer resides behind a firewall, complete the "DLP-C44 Provision the IIOP Listener Port on the CTC Computer" task on page 17-60.

Figure 4-3 shows a CTC computer and ONS 15310-CL behind firewalls. For the computer to access the ONS 15310-CL, you must provision the IIOP port on the CTC computer and on the ONS 15310-CL.

Figure 4-3 CTC Computer and ONS 15310-CLs Residing Behind Firewalls

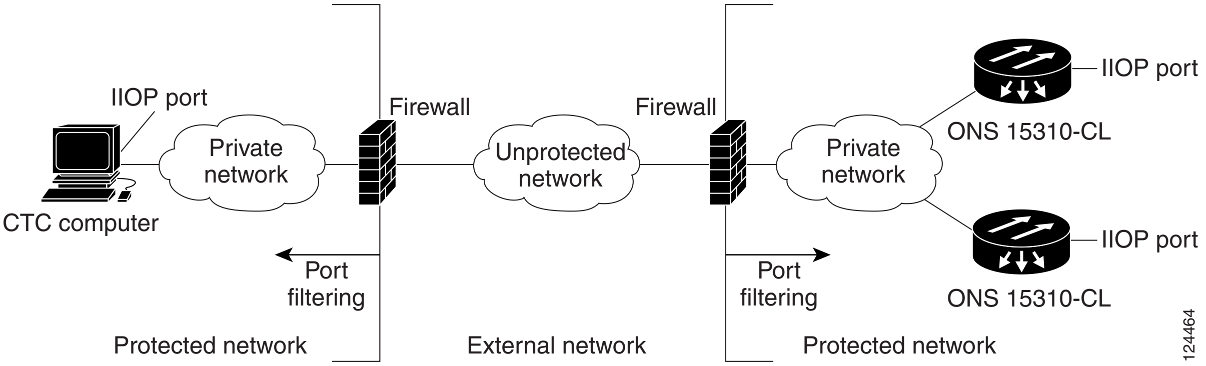
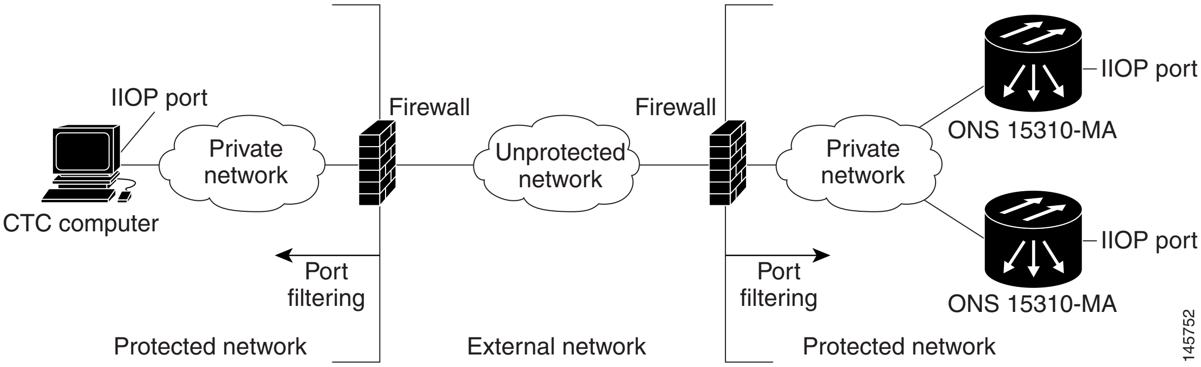


Figure 4-4 shows a CTC computer and ONS 15310-MA behind firewalls. For the computer to access the ONS 15310-MA, you must provision the IIOP port on the CTC computer and on the ONS 15310-MA.

Figure 4-4 CTC Computer and ONS 15310-MAs Residing Behind Firewalls



Stop. You have completed this procedure.

NTP-C276 Create FTP Host

Purpose	This procedure provisions FTP Host for access to ENEs for database backup. Use this procedure for database backup with FTP if proxy/firewall is enabled.
Tools/Equipment	None
Prerequisite Procedures	NTP-C21 Set Up CTC Network Access, page 4-6 NTP-C22 Set Up the ONS 15310-CL or ONS 15310-MA for Firewall Access, page 4-8
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the ONS 15310-CL or ONS 15310-MA node where you want to set up timing. If you are already logged in, continue with Step 3.

Step 2 If you want to turn on the ONS 15310-MA secure mode, which allows two IPv4 addresses to be provisioned for the node if CTX2500 cards are installed, complete the "DLP-C289 Enable Node Secure Mode" task on page 19-94.

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.

Step 6 The Mask is automatically set according to the Net/Subnet Mask length specified in DLP-C39. 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, skip to Step 9

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 Host.

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

NTP-C23 Set Up Timing

Purpose	This procedure provisions the ONS 15310-CL or ONS 15310-MA timing.
Tools/Equipment	None
Prerequisite Procedures	NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the ONS 15310-CL or ONS 15310-MA node where you want to set up timing. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-C45 Set Up External or Line Timing" task on page 17-61 if an external building integrated timing supply (BITS) source is available. This is the most common SONET timing setup procedure.

Step 3 Complete the "DLP-C46 Set Up Internal Timing" task on page 17-63 if you cannot complete Step 2 (an external BITS source is not available). This task can only provide Stratum 3 timing.

Note For information about SONET timing, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* or to Telcordia GR-253-CORE.

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

NTP-C141 Create Optical Protection Groups for the ONS 15310-CL

Purpose	This procedure creates protection groups for ONS 15310-CL optical ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-C130 Manage Pluggable Port Modules, page 10-3 (optional) NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node where you want to create the protection group. If you are already logged in, continue with Step 2.

Step 2 Verify that pluggable port modules (PPM) are provisioned for the same port and port rate on the 15310-CL-CTX where you will create the optical protection group.

Note PPMs are referred to as small-form factor pluggables (SFPs) in the hardware chapters.

You can use either of the following methods:

- In node view, move your mouse over the 15310-CL-CTX client port. If a PPM is provisioned, two dots appear in the port graphic, and the port and PPM port and rate appear when you move the mouse over the port.
- Display the 15310-CL-CTX in card view. Click the **Provisioning > Pluggable Port Module** tabs. Verify that a PPM is provisioned in the Pluggable Port Module area, and the port type and rate is provisioned for it in the Selected PPM area.

The PPM port and port rate must be the same for both 15310-CTX-CL ports. As necessary, complete the "NTP-C130 Manage Pluggable Port Modules" procedure on page 10-3 to make PPM changes.

Step 3 From 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** from the drop-down list.
- Protect Port—Choose the protect port from the drop-down list. The menu displays the available optical ports on the 15310-CL-CTX.
- After you choose the protect port, a list of ports available for protection is displayed under Available Ports.

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 the port to the Working Ports list.

Step 7 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 it 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 port after failure conditions stay corrected for the amount of time entered in the Reversion Time field.
- 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. Reversion time is the amount of time that will elapse before the traffic reverts to the working port. The reversion timer starts after conditions causing the switch are cleared.

Step 8 Click **OK**.

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

NTP-C142 Create Protection Groups for the ONS 15310-MA

Purpose	This procedure creates ONS 15310-MA card protection groups.
Tools/Equipment	None
Prerequisite Procedures	NTP-C130 Manage Pluggable Port Modules, page 10-3 (optional) NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 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 15310-MA.

Table 4-1 Protection Types

Type	Cards	Description and Installation Requirements
1:1	DS1-28/DS3-EC1-3 DS1-84/DS3-EC1-3	Pairs one working card with one protect card. 1:1 protection groups are created automatically and do not require provisioning. There are two sets of paired expansion slots for the electrical cards. Card slots 1 and 2 are a pair and slots 5 and 6 are a pair. The pairing is due to the configuration of the backplane connectors. When two electrical cards are plugged into either of the card slot pairs, a 1:1 protection group is automatically created for the two cards, if possible. If a protection group cannot be created, one of the cards goes into the Mismatched Equipment Alarm (MEA) state, because the 15310-MA cannot support two unprotected electrical cards in the 1–2 or 5–6 card slot pairs. The 1:1 automatic protection group is created when the second electrical card of a pair is either plugged in or is preprovisioned. All ONS 15310-MA electrical cards, by default, are made part of a 1:1 protection group. The 1:1 protection group cannot be deleted. For more information, refer to the "Card Protection" chapter and the card reference material specific to the card in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.
1+1	CTX2500	Pairs a working OC-N port with a protect OC-N port. 1+1 protection can be created between any of the four total optical ports in any combination. For example, 1+1 can created between two ports on the same CTX 2500 card, or it can be created between port 2-1 on one CTX2500 and port 1-1 on the second CTX 2500. You can create a maximum of two 1+1 protection groups, one with the working port on slot 3 and one with the working port on slot 4. The same card can have both working and protect ports on it. 1+1 protection can be revertive or nonrevertive, bidirectional or unidirectional.
Optimized 1+1	CTX2500	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 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.
Unprotected	Any	Unprotected cards can cause signal loss if a card fails or incurs a signal error. Unprotected is the default for Ethernet cards and for the first electrical card plugged into any of the IO slots. For more information about electrical cards, see 1:1 in this table.

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

- 1:1 protection groups are created automatically when two electrical cards are physically installed or preprovisioned and do not require provisioning.
- DLP-C242 Create a 1+1 Protection Group for the ONS 15310-MA, page 19-53
- DLP-C243 Create an Optimized 1+1 Protection Group for the ONS 15310-MA, page 19-55

Note If a protect card is not installed, you can complete the "NTP-C162 Preprovision a Card Slot" procedure on page 2-31 and continue with the card protection provisioning.

Stop. You have completed this procedure.

NTP-C25 Set Up SNMP

Purpose	This procedure provisions the SNMP parameters so that you can use SNMP management software with the ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 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:

- Destination IP Address—Type the IP address of your network management system. If the node you are logged into is an end ONS 15310-CL or ONS 15310-MA network element (ENE), set the destination address to the GNE.
- Community—Type the SNMP community name. For a description of SNMP community names, refer to the "SNMP" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Note The community name is a form of authentication and access control. The community name assigned to the ONS 15310-CL or ONS 15310-MA 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-C225 Set Up SNMP for a GNE" task on page 19-23 and "DLP-C226 Set Up SNMP for an ENE" task on page 19-24.

Note If the node has the SOCKS proxy server enabled and is provisioned as an ENE, the UDP port must be set to the GNE's SNMP relay port, which is 391.

- Trap Version—Choose either SNMPv1 or SNMPv2. Refer to your NMS documentation to determine whether to use SNMP v1 or v2.
- Max Traps Per Second—Choose a number from 0 to 32767. This field limits the number of traps per second to reduce network congestion.

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 gateway node elements (GNEs) and end node elements (ENEs), complete the following tasks as required, depending on the protection groups you want to create:

- DLP-C225 Set Up SNMP for a GNE, page 19-23
- DLP-C226 Set Up SNMP for an ENE, page 19-24
- DLP-C227 Format and Enter NMS Community String for SNMP Command or Operation, page 19-26

Step 8 Click **Apply**.

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

NTP-C131 Provision OSI

Purpose	This procedure provisions the ONS 15310-CL or ONS 15310-MA so it can be networked with other vendor NEs that use the OSI (Open Systems Interface) protocol stack for data communications network (DCN) communications. This procedure provisions the TID Address Resolution Protocol (TARP), OSI routers, manual area addresses, subnetwork points of attachment, and IP over OSI tunnels.
Tools/Equipment	None
Prerequisite Procedures	NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

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 15310-CL and Cisco ONS 15310-MA Reference Manual*.

⚠ **Caution** Do not begin this procedure until you know the role of the ONS 15310-CL or ONS 15310-MA within the OSI and IP network.

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

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 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-C200 Provision OSI Routing Mode, page 19-1—Complete this task first.
- DLP-C201 Provision or Modify TARP Operating Parameters, page 19-2—Complete this task next.
- DLP-C202 Add a Static TID to NSAP Entry to the TARP Data Cache, page 19-4—Complete this task as needed.
- DLP-C204 Add a TARP Manual Adjacency Table Entry, page 19-5—Complete this task as needed.
- DLP-C205 Provision OSI Routers, page 19-6—Complete this task as needed.
- DLP-C206 Provision Additional Manual Area Addresses, page 19-6—Complete this task as needed.
- DLP-C207 Enable the OSI Subnet on the LAN Interface, page 19-7—Complete this task as needed.
- DLP-C208 Create an IP-Over-CLNS Tunnel, page 19-8—Complete this task as needed.

Stop. You have completed this procedure.

CHAPTER 5

Turn Up a Network

This chapter explains how to turn up and test Cisco ONS 15310-CL or Cisco ONS 15310-MA nodes in a network, including terminal point-to-point networks and path protection configurations.

Before You Begin

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

1. NTP-C26 Verify Node Turn-Up, page 5-2—Complete this procedure before beginning network turn up.
2. NTP-C27 Provision a Point-to-Point Network, page 5-3—Complete as needed.
3. NTP-C28 Point-to-Point Network Acceptance Test, page 5-4—Complete this procedure after you create a point-to-point network.
4. NTP-C29 Provision a Linear ADM Network, page 5-6—Complete as needed.
5. NTP-C30 Linear ADM Network Acceptance Test, page 5-8—Complete this procedure after you create a linear ADM.
6. NTP-C31 Provision Path Protection Nodes, page 5-10—Complete as needed.
7. NTP-C32 Path Protection Acceptance Test, page 5-12—Complete this procedure after you create a path protection configuration.
8. NTP-C33 Provision an Open-Ended Path Protection Configuration, page 5-15—As needed, complete this procedure after you provision a path protection configuration.
9. NTP-C34 Open-Ended Path Protection Acceptance Test, page 5-18—As needed, complete this procedure after you provision an open-ended path protection configuration.
10. NTP-C146 Provision a Traditional Path Protection Dual-Ring Interconnect on the ONS 15310-MA, page 5-21—As needed, complete this procedure after you provision a path protection configuration.
11. NTP-C147 Provision an Integrated Path Protection Dual-Ring Interconnect on the ONS 15310-MA, page 5-24—As needed, complete this procedure after you provision a path protection configuration.
12. NTP-C35 Create a Logical Network Map, page 5-26—Complete as needed.

NTP-C26 Verify Node Turn-Up

Purpose	This procedure verifies that each ONS 15310-CL or ONS 15310-MA is ready for network turn up before adding nodes to a network.
Tools/Equipment	None
Prerequisite Procedures	Chapter 4, "Turn Up a Node"
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Superuser

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at any node 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-C88 Disable Alarm Filtering" task on page 17-109 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms are present, investigate and resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

Step 3 Verify that the SW Version and Defaults in the node view status area match the software version and the network element (NE) defaults shown in your site plan.

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-C78 Change Node Management Information" procedure on page 11-2.

Step 5 Click the **Provisioning > Timing** tabs. Verify that the timing settings match the settings on your site plan. If not, see the "NTP-C82 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-C79 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-C143 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-C83 Modify Users and Change Security" procedure on page 11-6.

Step 9 If 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-C84 Change SNMP Settings" procedure on page 11-7.

Stop. You have completed this procedure.

NTP-C27 Provision a Point-to-Point Network

Purpose	This procedure provisions two ONS 15310-CL or ONS 15310-MA nodes in a 1+1 point-to-point (terminal) network.
Tools/Equipment	None
Prerequisite Procedures	NTP-C26 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the ONS 15310-CL or ONS 15310-MA on 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 an optical port on the 15310-CL-CTX or CTX2500. Complete the "NTP-C141 Create Optical Protection Groups for the ONS 15310-CL" procedure on page 4-12 or "NTP-C142 Create Protection Groups for the ONS 15310-MA" procedure on page 4-13 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 ports in the protection groups correspond to the physical fiber connections between the nodes, that is, verify that the working port in one node connects to the working port in the other node and that the protect port in one node connects to the protect port in the other node.

Step 5 Complete the "DLP-C52 Provision Section DCC Terminations" task on page 17-68 for the working optical port signal on both point-to-point nodes. Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-C53 Provision Line DCC Terminations" task on page 17-70.

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 craft (direct) connection to the node. Remote provisioning is possible only after all nodes in the network have DCC terminations provisioned to in-service on the 15310-CL-CTX ports for the ONS 15310 CL or the CTX2500 ports for the ONS 15310 MA.

Step 6 As needed, complete the "DLP-C47 Provision a Proxy Tunnel" task on page 17-64.

Step 7 As needed, complete the "DLP-C48 Provision a Firewall Tunnel" task on page 17-65.

Step 8 As needed, complete the "DLP-C49 Create a Provisionable Patchcord" task on page 17-66 on both point-to-point nodes.

Step 9 Complete the "DLP-C50 Change the Service State for a Port" task on page 17-67 to put the protect port in-service.

Step 10 Verify that timing is set up at both point-to-point nodes. If not, complete the "NTP-C23 Set Up Timing" procedure on page 4-11 for one or both of the nodes.

Step 11 Complete the "NTP-C28 Point-to-Point Network Acceptance Test" procedure on page 5-4.

Stop. You have completed this procedure.

NTP-C28 Point-to-Point Network Acceptance Test

Purpose	This procedure tests two ONS 15310-CLs or two ONS 15310-MAs in a point-to-point network.
Tools/Equipment	Test set/cables appropriate to the test circuit you will create
Prerequisite Procedures	NTP-C27 Provision a Point-to-Point Network, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at one of the point-to-point nodes. 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-C88 Disable Alarm Filtering" task on page 17-109 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms are present, investigate and resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

c. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export the alarm data to a file.

Step 4 Click the **Conditions** tab.

a. Verify that the network does not have any unexplained conditions. If unexplained conditions are present, resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

b. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export the condition data to a file.

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-C37 Create an Automatically Routed DS-1 Circuit" procedure on page 6-6. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-C40 Create an Automatically Routed DS-3 or EC-1 Circuit" procedure on page 6-16. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For optical circuits, complete the "NTP-C47 Create an Automatically Routed Optical Circuit" procedure on page 6-34. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 7 For the ONS 15310-CL, configure the test set for the test circuit type you created:

- Wideband Electrical ports (WBE) DS-1—On the ONS 15310-CL, if you are testing an unmuxed DS-1, you must have a DSX-1 panel or use the high-density DS1 interface through the LFH-96 connector. For information about configuring your test set, consult your test set user guide.
- Broadband Electrical ports (BBE) DS3/EC1—On the ONS 15310-CL, if you are testing a clear channel DS-3 or EC-1, you must have a direct DS-3/EC-1 interface into the ONS 15310-CL through the BBE ports on the 15310-CL-CTX. Set the test set for clear channel DS-3. Set the test set for clear channel 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 For the ONS 15310-MA, configure the test set for the test circuit type you created:

- Wideband Electrical ports (WBE) DS-1—On the ONS 15310-MA, if you are testing an unmuxed DS-1, use the Champ connectors on the BICs on the rear of the chassis. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- Broadband Electrical ports (BBE) DS3/EC1—On the ONS 15310-MA, if you are testing a clear channel DS-3 or EC-1, use the BNC connectors on the BICs on the rear of the chassis. Set the test set for clear channel 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 one end to the test set transmit (Tx) connector and the other end 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 10.

Step 10 Create a physical loopback at the circuit destination. To do so, attach one end of a patch cable to the destination port Tx connector; attach the other end to the port Rx connector.

Step 11 At the circuit source:

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

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

Step 12 Verify that the test set displays a clean signal. If a clean signal is not present, repeat Steps 6 to 11 to make sure the test set and cabling are configured correctly.

Step 13 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 14 Inject BIT errors from the test set. Verify that the errors display at the test set, indicating a complete end-to-end circuit.

Step 15 Complete the "DLP-C54 Optical 1+1 Protection Test" task on page 17-72.

Step 16 Set up and complete a BER test. Use the existing configuration and follow your site requirements for the specified 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. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

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-C88 Disable Alarm Filtering" task on page 17-109 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms are present, investigate and resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

c. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export the alarm data to a file.

Step 20 Repeat Steps 10 to 19 for the other point-to-point node.

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.

Step 22 Delete the test circuit. See the "DLP-C115 Delete Circuits" task on page 18-21 for instructions.

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-C29 Provision a Linear ADM Network

Purpose	This procedure provisions ONS 15310-CL or ONS 15310-MA nodes in a linear add-drop multiplexer (ADM) configuration.
Tools/Equipment	None
Prerequisite Procedures	NTP-C26 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

Note In a linear ADM configuration, two OC-N ports in 1+1 protection are connected to two OC-N ports in 1+1 protection on a second node. On the second node, two more OC-N ports 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. The ONS 15310-CL has only two optical ports. This restricts an ONS 15310-CL to being the end node in a linear ADM network since both ports are necessary to create the 1+1 protection group to the neighbor node. The ONS 15310-MA does not have this restriction since it has four optical ports.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at an ONS 15310-CL or ONS 15310-MA that you want to provision in a linear ADM network. If you are already logged in, continue with Step 2.

Figure 5-1 shows two ONS 15310-CLs in a linear ADM configuration with an ONS 15454. In this example, working traffic flows from the ONS 15310 Node 1/Slot 2/Port 2-1 to the ONS 15454 Node 2/Slot 5, and from Node 2/Slot 12 to the ONS 15310 Node 3/Slot 2/Port 2-1. You create the protect path by placing Slot 2/Port 2-1 in 1+1 protection with Slot 2/Port 1-1 at Nodes 1 through 3.

Figure 5-1 ONS 15310-CL Linear ADM Configuration

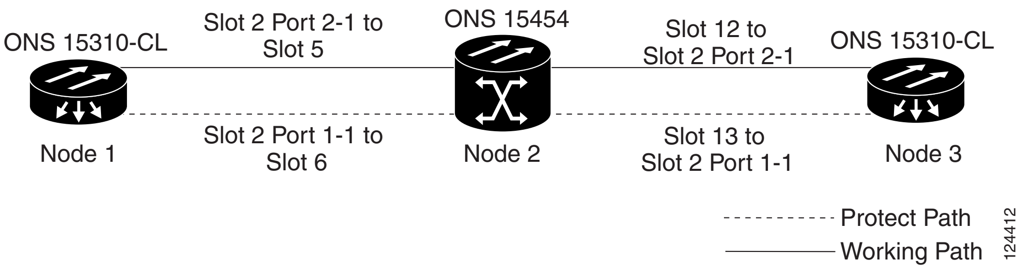
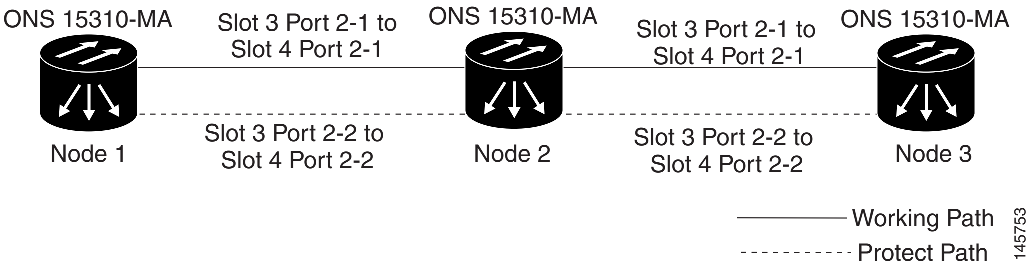

ONS 15310-CL
Slot 2 Port 2-1 to Slot 5
ONS 15454
Slot 12 to Slot 2 Port 2-1
ONS 15310-CL
Node 1
Slot 2 Port 1-1 to Slot 6
Node 2
Slot 13 to Slot 2 Port 1-1
Node 3
Protect Path
Working Path
124412

Figure 5-2 shows three ONS 15310-MAs in a linear ADM configuration. In this example, working traffic flows from Node 1/Slot 3/Port 2-1 to Node 2/Slot 4/Port 2-1, and from Node 2/Slot 3/Port 2-1 to the Node 3/Slot 4/Port 2-1. You create the protect path by placing Slot 3/Port 2-1 in 1+1 protection with Slot 4/Port 2-2 at Nodes 1 through 3.

Figure 5-2 ONS 15310-MA Linear ADM Configuration


ONS 15310-MA
Slot 3 Port 2-1 to Slot 4 Port 2-1
ONS 15310-MA
Slot 3 Port 2-1 to Slot 4 Port 2-1
ONS 15310-MA
Node 1
Slot 3 Port 2-2 to Slot 4 Port 2-2
Node 2
Slot 3 Port 2-2 to Slot 4 Port 2-2
Node 3
Working Path
Protect Path
145753

Step 2 Click the **Provisioning > Protection** tabs. Verify that 1+1 protection is created for the 15310-CL-CTX or CTX2500 at the node. If the protection group has not been created, complete the "NTP-C141 Create Optical Protection Groups for the ONS 15310-CL" procedure on page 4-12.

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

Step 5 Complete the "DLP-C52 Provision Section DCC Terminations" task on page 17-68 for the working optical ports on each linear ADM node. Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-C53 Provision Line DCC Terminations" task on page 17-70.

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

Note Terminating nodes will have one DCC termination (Nodes 1 and 3 in Figure 5-1 on page 5-7), and intermediate nodes will have two DCC terminations (Node 2/Slot 5 and Node 2/Slot 12 in Figure 5-1). An ONS 15310-CL cannot be used as an intermediate node because two optical ports are required. An ONS 15310-MA can be used as an intermediate node.

Step 6 As needed, complete the "DLP-C47 Provision a Proxy Tunnel" task on page 17-64.

Step 7 As needed, complete the "DLP-C48 Provision a Firewall Tunnel" task on page 17-65.

Step 8 As needed, complete the "DLP-C49 Create a Provisionable Patchcord" task on page 17-66 on all linear ADM nodes.

Step 9 Verify that timing has been set up at each linear node. If not, complete the "NTP-C23 Set Up Timing" procedure on page 4-11.

Step 10 Complete the "NTP-C30 Linear ADM Network Acceptance Test" procedure on page 5-8.

Stop. You have completed this procedure.

NTP-C30 Linear ADM Network Acceptance Test

Purpose	This procedure tests a linear ADM network.
Tools/Equipment	Test set/cables appropriate to the test circuit you will create
Prerequisite Procedures	NTP-C29 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-C29 Log into CTC" task on page 17-44 at an ONS 15310-CL or ONS 15310-MA on 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-C88 Disable Alarm Filtering" task on page 17-109 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms are present, investigate and resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

c. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export alarm data to a file on your hard drive.

Step 4 Click the **Conditions** tab.

a. Verify that the network does not have any unexplained conditions. If unexplained conditions are present, resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

b. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export condition data to a file on your hard drive.

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-C37 Create an Automatically Routed DS-1 Circuit" procedure on page 6-6. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-C40 Create an Automatically Routed DS-3 or EC-1 Circuit" procedure on page 6-16. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For OC-N circuits, complete the "NTP-C47 Create an Automatically Routed Optical Circuit" procedure on page 6-34. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 7 For the ONS 15310-CL, configure the test set for the test circuit type you created:

- Wideband Electrical ports (WBE) DS-1—On the ONS 15310-CL, if you are testing an unmuxed DS-1, you must have a DSX-1 panel or use the high-density DS1 interface through the LFH-96 connector. For information about configuring your test set, consult your test set user guide.
- Broadband Electrical ports (BBE) DS3/EC1—On the ONS 15310-CL, if you are testing a clear channel DS-3 or EC-1, you must have a direct DS-3/EC-1 interface into the ONS 15310-CL through the BBE ports on the 15310-CL-CTX. Set the test set for clear channel DS-3. Set the test set for clear channel 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 For the ONS 15310-MA, configure the test set for the test circuit type you created:

- Wideband Electrical ports (WBE) DS-1—On the ONS 15310-MA, if you are testing an unmuxed DS-1, use the Champ connectors on the BICs on the rear of the chassis. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- Broadband Electrical ports (BBE) DS3/EC1—On the ONS 15310-MA, if you are testing a clear channel DS-3 or EC-1, use the BNC connectors on the BICs on the rear of the chassis. Set the test set for clear channel 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 one end to the test set transmit (Tx) connector and the other end 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 the next step.

Step 10 Create a physical loopback at the circuit destination. 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 11 At the circuit source:

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 displays a clean signal. If a clean signal is not displayed, repeat Steps 6 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 on the test set, indicating a complete end-to-end circuit.

Step 14 Complete the "DLP-C54 Optical 1+1 Protection Test" task on page 17-72 to test the OC-N port protection group switching.

Step 15 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 16 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

Step 17 In network view, click the **Alarms** tab. Verify that the network does not have any unexplained alarms. If unexplained alarms are present, resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

Step 18 Delete the test circuit. See the "DLP-C115 Delete Circuits" task on page 18-21 for instructions.

Step 19 Repeat Steps 5 through 18 for the next linear ADM node you are testing.

Step 20 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.

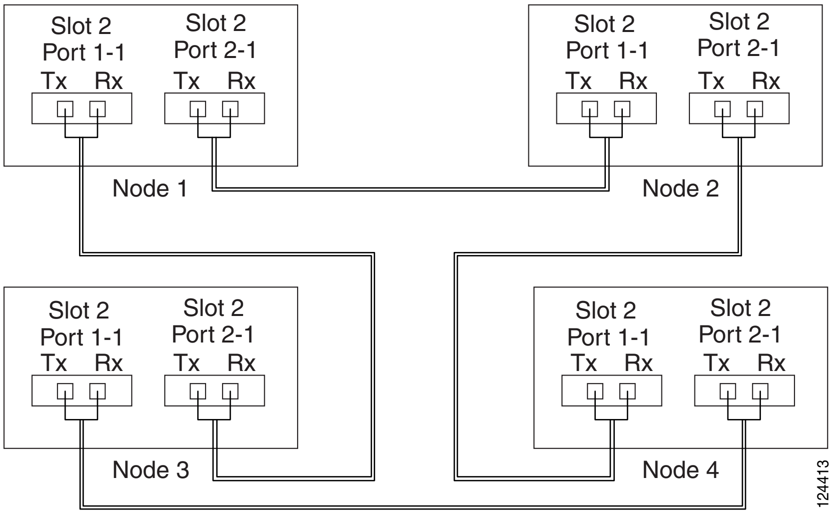
NTP-C31 Provision Path Protection Nodes

Purpose	This procedure provisions nodes for inclusion in a path protection configuration. A path protection configuration is created after the fiber connections are made.
Tools/Equipment	None
Prerequisite Procedures	NTP-C26 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

Note Path protection is the default ONS 15310-CL and ONS 15310-MA topology. It is available as soon as you install the SFPs (which provide the optical ports), connect the OC-N fibers, and create the DCC terminations.

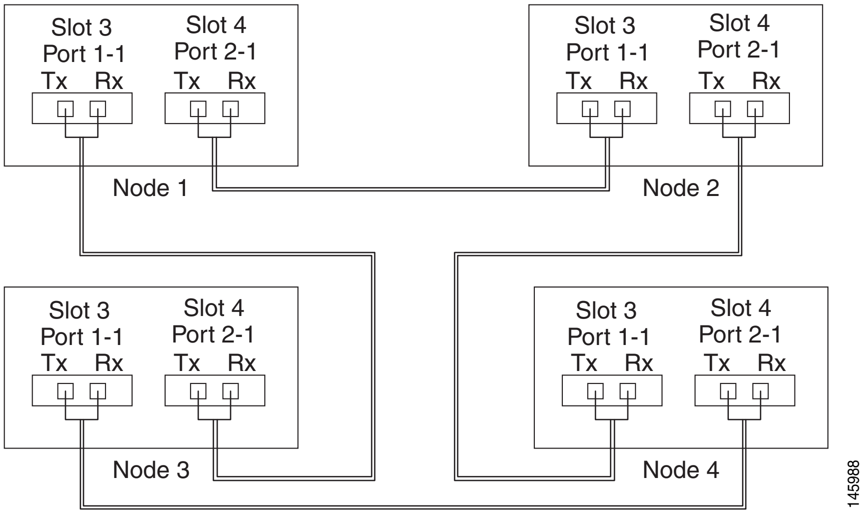
Step 1 For the ONS 15310-CL, verify that the fiber is correctly connected to the path protection trunk (span) optical ports similar to Figure 5-3. See the "NTP-C8 Install Optical Cables" procedure on page 1-12.

Figure 5-3 ONS 15310-CL Path Protection Fiber Connection Example



Step 2 For the ONS 15310-MA, verify that the fiber is correctly connected to the path protection trunk (span) optical ports similar to Figure 5-4. See the "NTP-C160 Install Optical Cables" procedure on page 2-28.

Figure 5-4 ONS 15310-MA Path Protection Fiber Connection Example



Step 3 Complete the "DLP-C29 Log into CTC" task on page 17-44 at an ONS 15310-CL or ONS 15310-MA in the path protection configuration you are turning up. If you are already logged in, continue with Step 4.

Step 4 Complete the "DLP-C52 Provision Section DCC Terminations" task on page 17-68 for the two ports that will serve as the path protection ports on the node. For example, on an ONS15310-CL you can use Node 1/Slot 2/Port 2-1 (OC-3) and Node 1/Slot 2/Port 1-1 (OC-3). On an ONS15310-MA, you can use Node 1/Slot 3/Port 2-1 (OC-3) and Node 1/Slot 4/Port 1-1 (OC-3). (Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-C53 Provision Line DCC Terminations" task on page 17-70.)

Note If an ONS 15310-CL or ONS 15310-MA is not connected to a corporate LAN, DCC provisioning must be performed through a craft (direct) connection. Remote provisioning is possible only after all nodes in the network have DCC terminations provisioned to in-service for ports on the 15310-CL-CTX for the ONS 15310-CL or the CTX2500 for the ONS 15310-MA.

Step 5 Repeat Steps 3 and 4 for each node in the path protection configuration.

Step 6 As needed, complete the "DLP-C47 Provision a Proxy Tunnel" task on page 17-64.

Step 7 As needed, complete the "DLP-C48 Provision a Firewall Tunnel" task on page 17-65.

Step 8 As needed, complete the "DLP-C49 Create a Provisionable Patchcord" task on page 17-66 on both point-to-point nodes.

Step 9 Complete the "NTP-C32 Path Protection Acceptance Test" procedure on page 5-12.

Stop. You have completed this procedure.

NTP-C32 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-C31 Provision Path Protection Nodes, page 5-10
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44. 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-C88 Disable Alarm Filtering" task on page 17-109 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms are present, investigate and resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

c. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export alarm data to a file on your hard drive.

Step 4 Click the **Conditions** tab.

a. Verify that the network does not have any unexplained conditions. If unexplained conditions are present, resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

b. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export condition data to a file on your hard drive.

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-C37 Create an Automatically Routed DS-1 Circuit" procedure on page 6-6. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-C40 Create an Automatically Routed DS-3 or EC-1 Circuit" procedure on page 6-16. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For OC-N circuits, complete the "NTP-C47 Create an Automatically Routed Optical Circuit" procedure on page 6-34. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 7 For the ONS 15310-CL, configure the test set for the test circuit type you created:

- Wideband Electrical ports (WBE) DS-1—On the ONS 15310-CL, if you are testing an unmuxed DS-1, you must have a DSX-1 panel or use the high-density DS1 interface through the LFH-96 connector. For information about configuring your test set, consult your test set user guide.
- Broadband Electrical ports (BBE) DS3/EC1—On the ONS 15310-CL, if you are testing a clear channel DS-3 or EC-1, you must have a direct DS-3/EC-1 interface into the ONS 15310-CL through the BBE ports on the 15310-CL-CTX. Set the test set for clear channel DS-3. Set the test set for clear channel 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 For the ONS 15310-MA, configure the test set for the test circuit type you created:

- Wideband Electrical ports (WBE) DS-1—On the ONS 15310-MA, if you are testing an unmuxed DS-1, use the Champ connectors on the BICs on the rear of the chassis. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- Broadband Electrical ports (BBE) DS3/EC1—On the ONS 15310-MA, if you are testing a clear channel DS-3 or EC-1, use the BNC connectors on the BICs on the rear of the chassis. Set the test set for clear channel 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 one end to the test set transmit (Tx) connector and the other end 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 continuing.

Step 10 Create a physical loopback at the circuit destination:

a. Attach one end of a patch cable to the destination port Tx connector.

b. Attach the other end to the port Rx connector.

Step 11 At the circuit source:

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 displays a clean signal. If a clean signal is not displayed, repeat Steps 1 through 9 to make sure the test set and cabling are configured correctly.

Step 13 Inject BIT errors from the test set. To verify that you have a complete end-to-end circuit, verify that the errors display at the test set.

Step 14 From the View menu choose **Go to Network View**.

Step 15 Click one of the two spans leaving the circuit source node and complete the "DLP-C55 Path Protection Switching Test" task on page 17-73.

Step 16 In network view, click the other circuit source span and complete the "DLP-C55 Path Protection Switching Test" task on page 17-73.

Step 17 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 18 Complete the "DLP-C115 Delete Circuits" task on page 18-21 to delete the test circuit.

Step 19 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

Step 20 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-C88 Disable Alarm Filtering" task on page 17-109 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms are present, investigate and resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

c. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export alarm data to a file on your hard drive.

Step 21 Click the **Conditions** tab.

a. Verify that the network does not have any unexplained conditions. If unexplained conditions are present, resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

b. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export condition data to a file on your hard drive.

Step 22 Repeat Steps 6 through 21 for each node on the network.

Step 23 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."

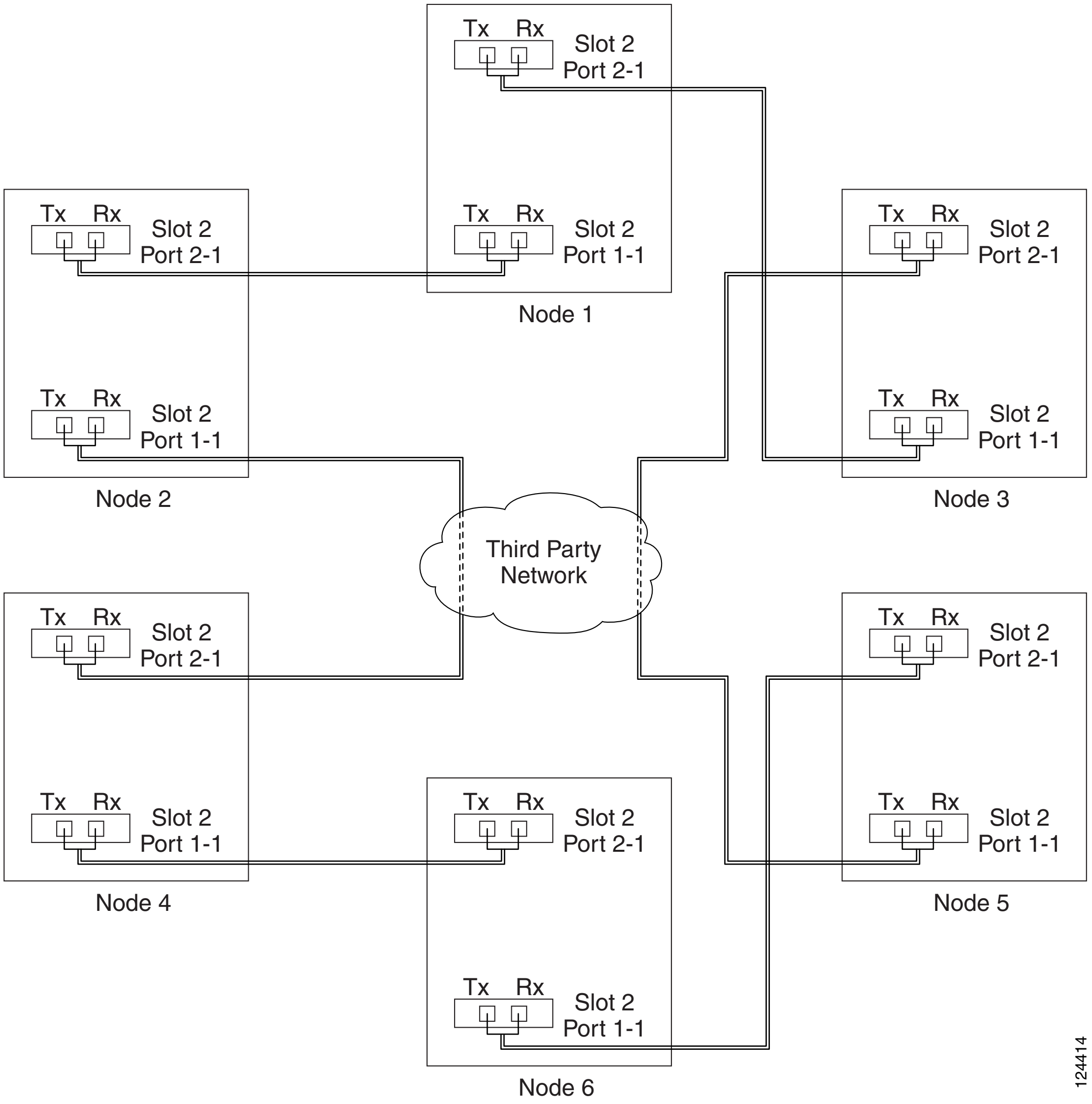
Stop. You have completed this procedure.

NTP-C33 Provision an Open-Ended Path Protection Configuration

Purpose	This procedure provisions ONS 15310-CL or ONS 15310-MA 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 15310 network to another ONS 15310 network through the third-party network.
Tools/Equipment	None
Prerequisite Procedures	NTP-C26 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

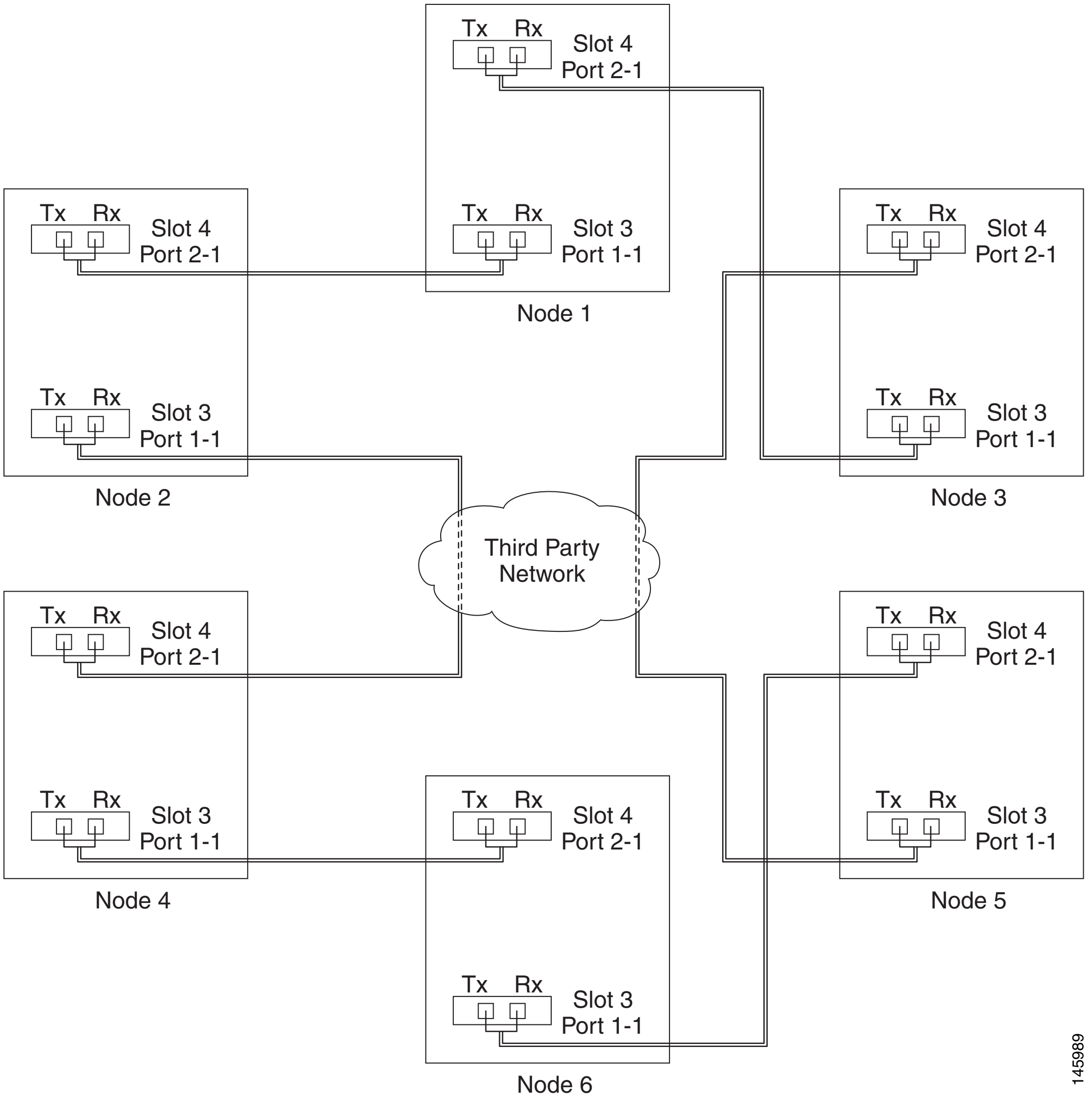
Step 1 Verify that the fiber is correctly connected to the path protection optical ports at each open-ended path protection node. For the ONS 15310-CL, Figure 5-5 shows an example. Node 1 is connected to ONS 15310-CL Nodes 2 and 3 through Slot 2/Port 2-1 and Slot 2/Port 1-1. Optical ports on 15310-CL-CTX at Nodes 2 and 3 are connected to the third-party vendor equipment.

Figure 5-5 ONS 15310-CL Open-Ended Path Protection Configurations Fiber Connection Example



Step 2 For the ONS 15310-MA, Figure 5-6 shows an example. Node 1 is connected to ONS 15310-MA Nodes 2 and 3 through Slot 3/Port 1-1 and Slot 4/Port 2-1. Optical ports on CTX2500 at Nodes 2 and 3 are connected to the third-party vendor equipment.

Figure 5-6 ONS 15310-MA Open-Ended Path Protection Configurations Fiber Connection Example



Step 3 Verify that the third-party cards or units to which the ONS 15310-CL or ONS 15310-MA trunk ports are connected are the same OC-N rate as the ONS 15310 trunk ports. The third-party time slots must match the ONS 15310 time slots to which they are connected. For example, if you are using an OC-3 port, the third-party vendor card or unit must have STSs 1-3 available.

Step 4 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node you are turning up. If you are already logged in, continue with Step 5.

Step 5 Complete the "DLP-C52 Provision Section DCC Terminations" task on page 17-68 for the ONS 15310-CL or ONS 15310-MA cards/ports that are connected to another ONS 15310-CL or ONS 15310-MA. (Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-C53 Provision Line DCC Terminations" task on page 17-70.) Do not create a DCC termination for the card/port that connects to the third-party equipment. The ONS 15310-CL for example in Figure 5-5, has DCC terminations created at the following cards/ports:

- Nodes 1 and 6: Slot 2, Port 2-1 and Slot 2, Port 1-1

- Node 2 and 5: Slot 2, Port 2-1
- Node 3 and 4: Slot 2, Port 1-1

The ONS 15310-MA in Figure 5-6, has DCC terminations created at the following cards/ports:

- Nodes 1 and 6: Slot 4, Port 2-1 and Slot 3, Port 1-1
- Node 2 and 5: Slot 4, Port 2-1
- Node 3 and 4: Slot 3, Port 1-1

Note If an ONS 15310-CL or ONS 15310-MA is not connected to a corporate LAN, DCC provisioning must be performed through a direct (craft) connection. Remote provisioning is possible only after all nodes in the network have DCC terminations provisioned to in-service OC-N ports.

Step 6 Repeat Steps 4 through 5 for each node in the path protection configuration.

Step 7 As needed, complete the "DLP-C47 Provision a Proxy Tunnel" task on page 17-64.

Step 8 As needed, complete the "DLP-C48 Provision a Firewall Tunnel" task on page 17-65.

Step 9 As needed, complete the "DLP-C49 Create a Provisionable Patchcord" task on page 17-66 on both point-to-point nodes.

Step 10 Following the documentation provided by the third-party vendor, provision the optical loop leading from the ONS 15310-CL or ONS 15310-MA connection at one end to the ONS 15310-CL or ONS 15310-MA connection at the other end. In other words, you will create an open-ended path protection configuration using procedures for the third-party equipment.

Step 11 Continue with the "NTP-C34 Open-Ended Path Protection Acceptance Test" procedure on page 5-18.

Stop. You have completed this procedure.

NTP-C34 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-C34 Open-Ended Path Protection Acceptance Test, page 5-18
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 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-C88 Disable Alarm Filtering" task on page 17-109 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms are present, investigate and resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

c. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export alarm data to a file on your hard drive.

Step 4 Click the **Conditions** tab.

a. Verify that the network does not have any unexplained conditions. If unexplained conditions are present, resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

b. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export condition data to a file on your hard drive.

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 15310-CL-CTX or CTX2500 OC-N port on the nodes that connect to the third-party network. For example, on the ONS 15310-CL in Figure 5-5 on page 5-16, a circuit is created from Node 1 to the OC-3 port at Node 2/Slot 2/Port 2-1, and a secondary circuit destination is created on the OC-3 port at Node 3/Slot 2/Port 1-1.

On the ONS 15310-MA in Figure 5-6 on page 5-17, a circuit is created from Node 1 to the OC-3 port at Node 2/Slot 4/Port 2-1, and a secondary circuit destination is created on the OC-3 port at Node 3/Slot 3/Port 1-1. For circuit creation procedures, complete one of the following:

- For EC-1 circuits, complete the "NTP-C40 Create an Automatically Routed DS-3 or EC-1 Circuit" procedure on page 6-16. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-1 circuits, complete the "NTP-C37 Create an Automatically Routed DS-1 Circuit" procedure on page 6-6. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-C40 Create an Automatically Routed DS-3 or EC-1 Circuit" procedure on page 6-16. 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 15310-CL or ONS 15310-MA connection ports to the second set of ONS 15310-CL or ONS 15310-MA 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. On the ONS 15310-CL in Figure 5-5, this is Node 6. However, this circuit will have two sources, one at Node 4/Slot 2/Port 2-1, and one at Node 5/Slot 2/Port 1-1. The destination will be the 15310-CL-CTX on Node 6.

On the ONS 15310-MA in Figure 5-6, this is Node 6. However, this circuit will have two sources, one at Node 4/Slot 4/Port 2-1, and one at Node 5/Slot 3/Port 1-1. The destination will be the CTX2500 on Node 6.

Step 9 For the ONS 15310-CL, configure the test set for the test circuit type you created:

- Wideband Electrical ports (WBE) DS-1—On the ONS 15310-CL, if you are testing an unmuxed DS-1, you must have a DSX-1 panel or use the high-density DS1 interface through the LFH-96 connector. For information about configuring your test set, consult your test set user guide.
- Broadband Electrical ports (BBE) DS3/EC1—On the ONS 15310-CL, if you are testing a clear channel DS-3 or EC-1, you must have a direct DS-3/EC-1 interface into the ONS 15310-CL through the BBE ports on the 15310-CL-CTX. Set the test set for clear channel DS-3. Set the test set for clear channel 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 For the ONS 15310-MA, configure the test set for the test circuit type you created:

- Wideband Electrical ports (WBE) DS-1—On the ONS 15310-MA, if you are testing an unmuxed DS-1, use the Champ connectors on the BICs on the rear of the chassis. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- Broadband Electrical ports (BBE) DS3/EC1—On the ONS 15310-MA, if you are testing a clear channel DS-3 or EC-1, use the BNC connectors on the BICs on the rear of the chassis. Set the test set for clear channel 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 11 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 and the other end 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 continuing.

Step 12 Create a physical loopback at the circuit destination:

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 13 At the circuit source:

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 14 Verify that the test set shows a clean signal. If a clean signal does not appear, repeat Steps 1 through 9 to make sure the test set and cabling are configured correctly.

Step 15 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 16 From the View menu, choose **Go to Network View**.

Step 17 Click one of the two spans leaving the circuit source node.

Step 18 Test the path protection switching function on this span. Complete the "DLP-C55 Path Protection Switching Test" task on page 17-73.

Step 19 In network view, click the other circuit source span and repeat Step 18.

Step 20 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 21 Complete the "DLP-C115 Delete Circuits" task on page 18-21 for the test circuit.

Step 22 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete.

Step 23 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-C88 Disable Alarm Filtering" task on page 17-109 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms are present, investigate and resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

c. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export alarm data to a file on your hard drive.

Step 24 Click the **Conditions** tab.

a. Verify that the network does not have any unexplained conditions. If unexplained conditions are present, resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

b. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export condition data to a file on your hard drive.

Step 25 Repeat Steps 6 through 24 for each node that will be a source or destination for circuits traversing the third-party network.

Step 26 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-C146 Provision a Traditional Path Protection Dual-Ring Interconnect on the ONS 15310-MA

Purpose	This procedure provisions path protection configurations in a DRI topology. DRIs interconnect two or more path protection configurations to provide an additional level of protection.
Tools/Equipment	None
Prerequisite Procedures	NTP-C26 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

Note To route circuits on the DRI, you must check the Dual Ring Interconnect check box during circuit creation.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at any node in the path protection configuration. If you are already logged in, continue with Step 2.

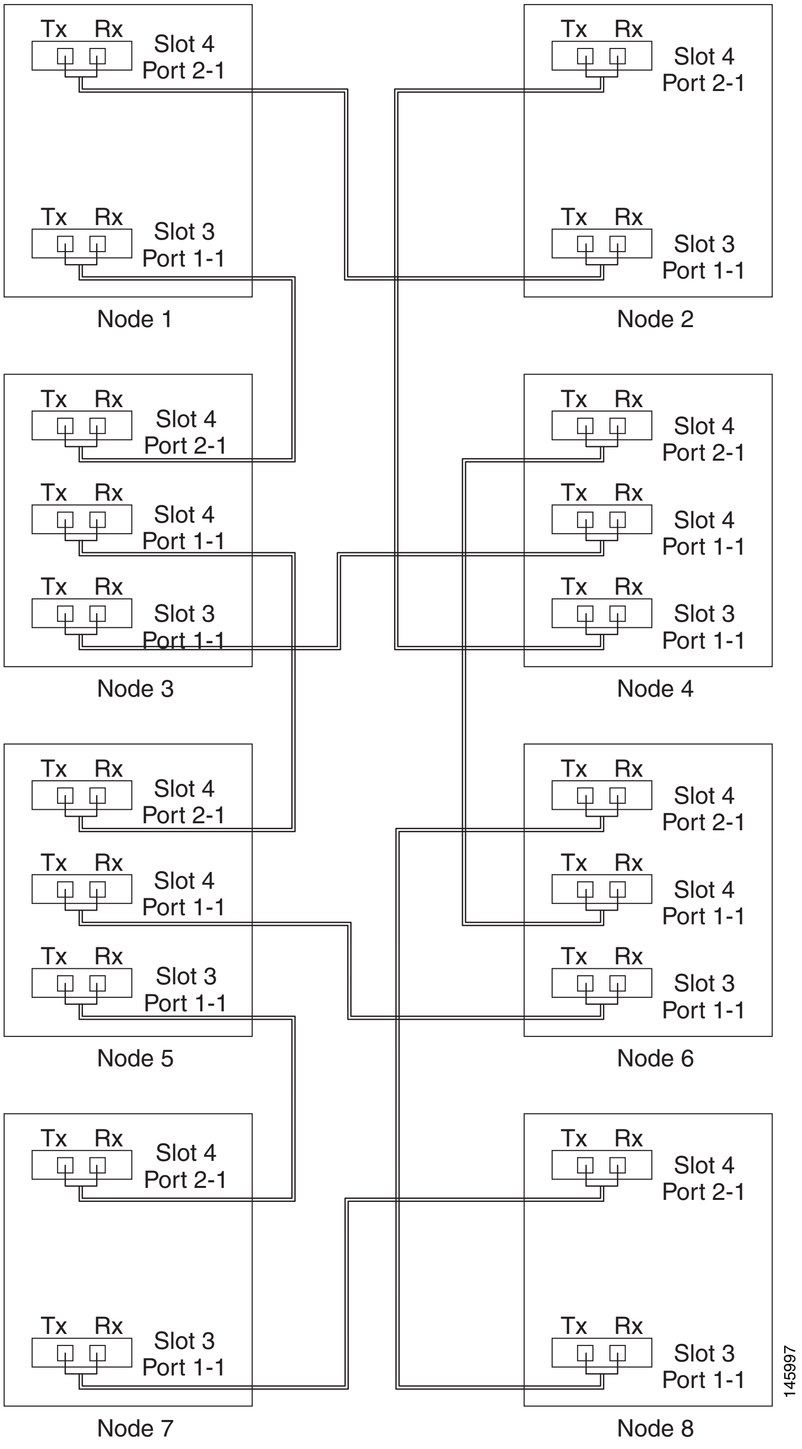
Step 2 Complete the following steps if you have not provisioned the path protection configurations that you will interconnect in a path protection DRI. If the path protection configurations are created, go to Step 3.

a. Complete the "NTP-C31 Provision Path Protection Nodes" procedure on page 5-10 to provision the path protection configurations.

b. Complete the "NTP-C32 Path Protection Acceptance Test" procedure on page 5-12 to test the path protection configurations.

Step 3 Verify that the path protection DRI interconnect nodes have fiber connections to the other interconnect node. 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, Slot 4, Port 2-1 at Node 4 is connected to Slot 4, Port 1-1 at Node 6. Nodes 3 and 5 are interconnected by Slot 4, Port 1-1 at Node 3 and Slot 4, Port 2-1 at Node 5.

Figure 5-7 Traditional Path Protection DRI Fiber Connection Example



Stop. You have completed this procedure.

NTP-C147 Provision an Integrated Path Protection Dual-Ring Interconnect on the ONS 15310-MA

Purpose	This procedure provisions path protection configurations in an integrated DRI topology.
Tools/Equipment	None
Prerequisite Procedures	NTP-C26 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

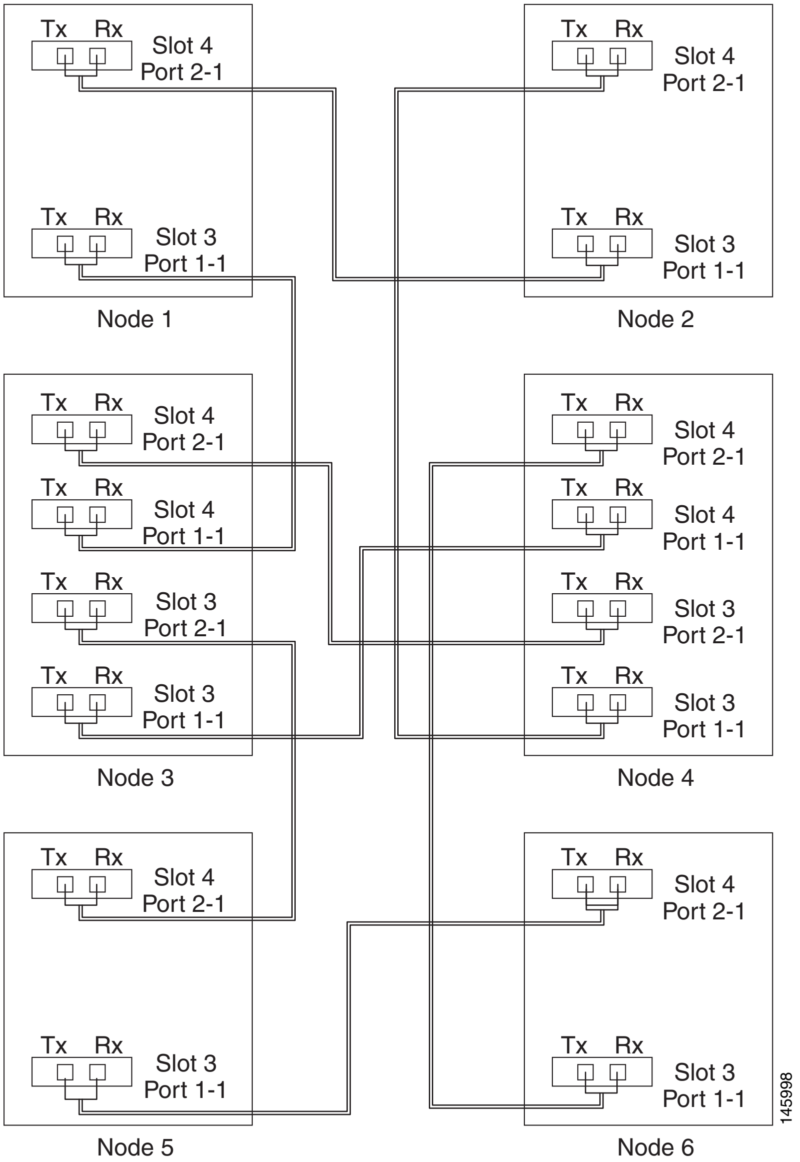
Step 2 Complete the following steps if you have not provisioned the path protection configurations that you will interconnect in a path protection DRI. If the path protection configurations are created, go to Step 3.

a. Complete the "NTP-C31 Provision Path Protection Nodes" procedure on page 5-10 to provision the path protection configurations.

b. Complete the "NTP-C32 Path Protection Acceptance Test" procedure on page 5-12 to test the path protection configurations.

Step 3 Verify that the path protection DRI interconnect nodes have fiber connections to the other interconnect nodes. An example is shown in Figure 5-8 on page 5-25. 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-C35 Create a Logical Network Map

Purpose	This procedure positions nodes in the network view. This procedure allows a superuser to create a consistent network view for all nodes on the network.
Tools	None
Prerequisite Procedures	NTP-C26 Verify Node Turn-Up, page 5-2
	This procedure also assumes that network turn up is completed.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at any node on the network. 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 plan.

a. Press the **Ctrl** key while you drag and drop a node icon to a new location.

b. Deselect the previously selected node.

c. Repeat Steps a and b 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 the network view map and choose Reset Node Position.

Stop. You have completed this procedure.

CHAPTER 6

Create Circuits and VT Tunnels

This chapter explains how to create Cisco ONS 15310-CL and ONS 15310-MA electrical circuits, Virtual Tributary (VT) tunnels, optical circuits, and Ethernet circuits. For additional information about ONS 15310-CL and ONS 15310-MA circuits, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA 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 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* as necessary.

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

1. NTP-C36 Verify Network Turn-Up, page 6-4—Complete this procedure before you create any circuits.
2. NTP-C37 Create an Automatically Routed DS-1 Circuit, page 6-6—Complete as needed.
3. NTP-C38 Create a Manually Routed DS-1 Circuit, page 6-10—Complete as needed.
4. NTP-C39 Create a Unidirectional DS-1 Circuit with Multiple Drops, page 6-12—Complete as needed.
5. NTP-C40 Create an Automatically Routed DS-3 or EC-1 Circuit, page 6-16—Complete as needed.
6. NTP-C41 Create a Manually Routed DS-3 or EC-1 Circuit, page 6-20—Complete as needed.
7. NTP-C42 Create a Unidirectional DS-3 or EC-1 Circuit with Multiple Drops, page 6-22—Complete as needed.
8. NTP-C46 Test Electrical Circuits, page 6-26—Complete this procedure after you create an electrical circuit.
9. NTP-C43 Create an Automatically Routed VT Tunnel, page 6-27—Complete as needed.
10. NTP-C44 Create a Manually Routed VT Tunnel, page 6-30—Complete as needed.
11. NTP-C45 Create a VT Aggregation Point, page 6-32—Complete as needed.
12. NTP-C47 Create an Automatically Routed Optical Circuit, page 6-34—Complete as needed.
13. NTP-C48 Create a Manually Routed Optical Circuit, page 6-39—Complete as needed.
14. NTP-C49 Create a Unidirectional Optical Circuit with Multiple Drops, page 6-41—Complete as needed.

15. NTP-C50 Test Optical Circuits, page 6-44—Complete this procedure after you create an optical circuit.
16. NTP-C51 Create an Automatically Routed VCAT Circuit, page 6-46—Complete as needed.
17. NTP-C52 Create a Manually Routed VCAT Circuit, page 6-52—Complete as needed.
18. NTP-C55 Create Overhead Circuits, page 6-55—Complete as needed to create data communications channel (DCC) tunnels, IP-encapsulated tunnels, and user data channel (UDC) circuits.
19. NTP-C140 Create a Server Trail, page 6-56—Complete as needed.

Table 6-1 defines ONS 15310-CL and ONS 15310-MA circuit creation terms and options.

Table 6-1 ONS 15310-CL and ONS 15310-MA Circuit Options

Circuit Option	Description
Source	The circuit source is where the circuit enters the ONS network.
Destination	The circuit destination is where the circuit exits an ONS 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 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).
VCAT	Virtual concatenated (VCAT) circuits transport traffic using noncontiguous time division multiplexing (TDM) time slots, avoiding the bandwidth fragmentation problem that exists with contiguous concatenated (CCAT) circuits. The cards that support VCAT circuits are the CE-100T-8 and ML-100T-8 cards. For more information, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.
VT tunnel	VT tunnels allow VT1.5 circuits to pass through a node without utilizing cross-connect 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.
VT aggregation point	VT aggregation points (VAPs) allow VT circuits to be aggregated into an STS for handoff to non-ONS networks or equipment, such as interoffice facilities (IOFs), switches, or digital access cross-connect systems (DACS). VAPs reduce VT matrix resource utilization at the node where the VT1.5s are aggregated onto the STS. This node is called the STS grooming end. The STS grooming end requires an OC-N port. VT aggregation points can be created on 1+1 or unprotected nodes, but cannot be created on path protectionnodes.

Table 6-2 shows the circuit source and destination options for ONS 15310-CL VT circuits.

Table 6-2 CTC Circuit Source/Destination Options for ONS 15310-CL VT Circuits

Card	Port Type	Ports	Port Rate	VTs	VCAT Members
15310-CL-CTX	Optical	2	OC-12 or OC-3	28 per STS	—
	Broadband	3	DS-3 or EC-1	28 per STS	—
	Wide band	21	DS-1	1 per DS-1	—

Table 6-2 CTC Circuit Source/Destination Options for ONS 15310-CL VT Circuits (continued)

Card	Port Type	Ports	Port Rate	VTs	VCAT Members
CE-100T-8	Ethernet/POS	8	—	—	1–64 per port
ML-100T-8		8	—	—	1–3 per port

Table 6-3 shows the circuit source and destination options for ONS 15310-CL STS circuits.

Table 6-3 CTC Circuit Source/Destination Options for ONS 15310-CL STS Circuits

Card	Port Type	Ports	Port Rate	STSs	VCAT Members
15310-CL-CTX	Optical	2	OC-12	12	—
			OC-3	3	—
	Broadband	3	DS-3 or EC-1	3	—
	Wide band	21	DS1	1	—
CE-100T-8	Ethernet/POS	8	—	1–3 per port	1–3 per port
ML-100T-8		2	—	1 per port	1–2 per port

Table 6-4 shows the circuit source and destination options for ONS 15310-MA VT circuits.

Table 6-4 CTC Circuit Source/Destination Options for ONS 15310-MA VT Circuits

Card	Port Type	Ports	Port Rate	VTs	VCAT Members
CTX2500	Optical	2	OC-48	28 per STS	—
			OC-12	28 per STS	—
			OC-3	28 per STS	—
DS1-28/DS3-EC1-3	Broadband	3	DS-3 or EC-1	28 per STS	—
	Wide band	28	DS-1	1 per DS-1	—
DS1-84/DS3-EC1-3	Broadband	3	DS-3 or EC-1	28 per STS	—
	Wide band	84	DS-1	1 per DS-1	—
CE-100T-8	Ethernet/POS	8	—	—	1–64 per port
ML-100T-8		8	—	—	1–3 per port

Table 6-5 shows the circuit source and destination options for ONS 15310-MA STS circuits.

Table 6-5 CTC Circuit Source/Destination Options for ONS 15310-MA STS Circuits

Card	Port Type	Ports	Port Rate	STSs	VCAT Members
CTX2500	Optical	2	OC-48	48	—
			OC-12	12	—
			OC-3	3	—
DS1-28/DS3-EC1-3	Broadband	3	DS-3 or EC-1	1	—
	Wide band	28	DS-1	28	—
DS1-84/DS3-EC1-3	Broadband	3	DS-3 or EC-1	3	—
	Wide band	84	DS-1	84	—
CE-100T-8	Ethernet/POS	8	—	1–3 per port	1–3 per port
ML-100T-8		2	—	1 per port	1–2 per port

NTP-C36 Verify Network Turn-Up

Purpose	This procedure verifies that the ONS 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-C29 Log into CTC" task on page 17-44. 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 network, the node icons will be stacked on the left side of the graphic area, possibly out of view. Use the scroll bar below the network map to display the icons. To separate the icons, drag and drop an icon to a new location. Repeat until all the nodes are visible on the graphic area.

Step 3 Verify node accessibility. In the 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 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

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.

a. Verify that the alarm filter is not on. See the "DLP-C88 Disable Alarm Filtering" task on page 17-109 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms are present, investigate and resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

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 on the shelf map. Verify that the 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-C78 Change Node Management Information" procedure on page 11-2.

c. Click the **Network** tab. Verify that the IP address, subnet mask, default router, SOCKS proxy server, and gateway settings are correctly provisioned. If not, make corrections using the "NTP-C79 Change CTC Network Access" procedure on page 11-2.

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-C141 Create Optical Protection Groups for the ONS 15310-CL" procedure on page 4-12.

e. Click the **Security** tab. Verify that the users and access levels are provisioned as specified. If not, see the "NTP-C19 Create Users and Assign Security" procedure on page 4-4 to correct the information.

f. 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-C84 Change SNMP Settings" procedure on page 11-7 to correct the information.

g. Click the **Comm Channels** tab. Verify that Section DCCs (SDCCs) or Line DCCs (LDCCs) were created on the applicable OC-N ports. If DCCs were not created, see Chapter 5, "Turn Up a Network" and complete the turn-up procedure appropriate for your network topology.

h. Click the **Timing** tab. Verify that timing is provisioned as specified. If not, use the "NTP-C82 Change Node Timing" procedure on page 11-6 to make the changes.

i. Click the **Alarm Profiles** tab. If you provisioned optional alarm profiles, verify that the alarms are provisioned as specified. If not, see the "NTP-C60 Create, Download, and Assign Alarm Severity Profiles" procedure on page 9-6 to change the information.

j. Verify that the network element (NE) defaults file listed in the status area of the node view window is correct. Refer to the "Network Element Defaults" appendix in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* document for more information about NE defaults.

Step 7 Repeat Step 6 for each node in the network.

Step 8 As appropriate, complete the circuit creation procedure listed in the "Before You Begin" section on page 6-1.

Stop. You have completed this procedure.

NTP-C37 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-C36 Verify Network Turn-Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at a node on the network 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-C56 Assign a Name to a Port" task on page 17-75. 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** or **VT**. STS or VT cross-connects will carry the DS-1 circuit across the ONS 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 autoranging 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. Autoranging creates identical (same source and destination), sequential circuits automatically. Uncheck this check 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 on page 6-7):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters, (including spaces). Circuit names should be 44 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 you are creating an STS circuit, choose **STS-1**. If you are creating a VT circuit, Size displays VT1.5 and cannot be changed.
- Bidirectional—Leave the default unchanged (checked) for this 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. Also, 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-C111 Change a Circuit Service State" task on page 18-17.

Note If VT circuit source and destination ports are in an OOS-AU,AINS; OOS-MA,MT; or IS-NR service state, VT circuits in OOS-AU,AINS change to IS-NR even if a physical signal is not present.

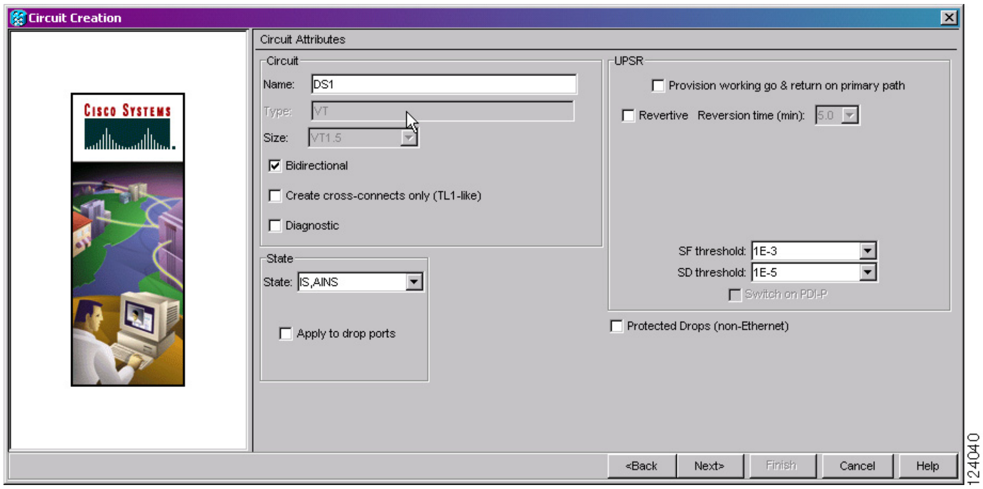
For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

- Apply to drop ports—Check this check box 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 is 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.

- Protected Drops—Check this check box if you want the circuit routed on protected drops only, that is, to ports that are in 1+1 protection. If you check this check box, CTC displays only protected cards and ports as source and destination choices.

Figure 6-1 Setting Circuit Attributes for a DS-1 Circuit



Circuit Creation

Circuit Attributes

Circuit

Name: DS1

Type: VT

Size: VT1.5

☑ Bidirectional

☐ Create cross-connects only (TL1-like)

☐ Diagnostic

State

State: IS,AINS

☐ Apply to drop ports

UPSR

☐ Provision working go & return on primary path

☐ Revertive Reversion time (min): 5.0

SF threshold: 1E-3

SD threshold: 1E-5

☐ Switch on PDI-P

☐ Protected Drops (non-Ethernet)

Step 8 If the circuit will be routed on a path protection configuration, complete the "DLP-C57 Provision Path Protection Selectors During Circuit Creation" task on page 17-75. Otherwise, continue with the next step.

Step 9 Click **Next**.

Step 10 Complete the "DLP-C58 Provision a DS-1 Circuit Source and Destination" task on page 17-76.

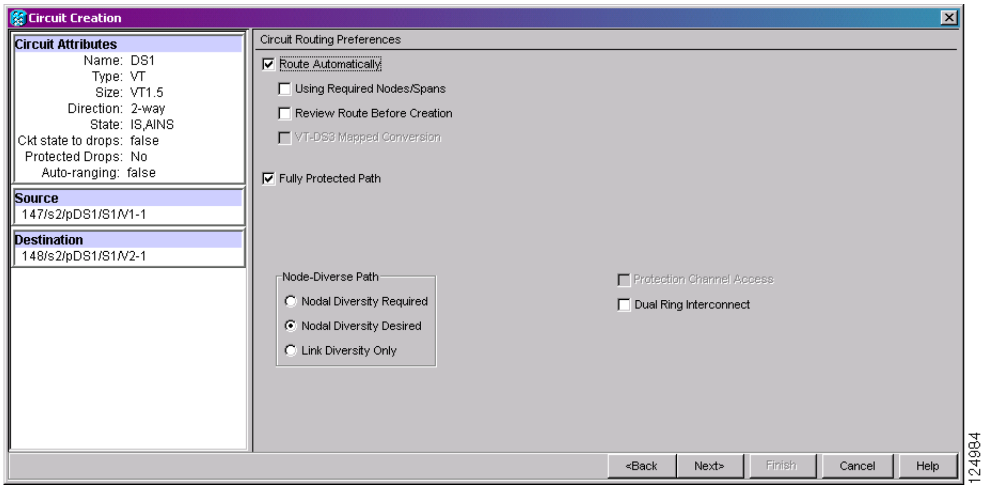
Step 11 In the Circuit Routing Preferences area (Figure 6-2), click **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- 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



Circuit Creation

Circuit Attributes
Name: DS1
Type: VT
Size: VT1.5
Direction: 2-way
State: IS,AINS
Ckt state to drops: false
Protected Drops: No
Auto-ranging: false

Source
147/s2/pDS1/S1/V1-1

Destination
148/s2/pDS1/S1/V2-1

Circuit Routing Preferences
☑ Route Automatically
□ Using Required Nodes/Spans
□ Review Route Before Creation
□ VT-DS3 Mapped Conversion
☑ Fully Protected Path

Node-Diverse Path
○ Nodal Diversity Required
● Nodal Diversity Desired
○ Link Diversity Only

□ Protection Channel Access
□ Dual Ring Interconnect

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.

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 path protection dual-ring interconnect (DRI), check the **Dual Ring Interconnect** check box.

Step 15 If you selected Using Required Nodes/Spans in Step 11, complete the following substeps. If not, continue with Step 17.

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 will be routed. Click spans twice to change the circuit direction.

d. Repeat Step c for each node or span you want to include or exclude.

e. Review the circuit route. To change the circuit routing order, choose a node from 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 If you are creating an STS circuit, skip this step and continue with Step 17. If you are creating a VT circuit, click **Next** and complete the "DLP-C59 Provision STS and VT Grooming Nodes" task on page 17-77.

Step 17 If you selected Review Route Before Creation in Step 11, complete the following substeps. If not, continue with Step 18.

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 the circuit information. If the circuit needs to be routed to a different path, see the "NTP-C38 Create a Manually Routed DS-1 Circuit" procedure on page 6-10.

Step 18 Click **Finish**. One of the following results occurs, depending on the circuit properties you chose in the Circuit Creation dialog box:

- If you entered 1 in the Number of Circuits field, CTC creates the circuit.
- If you entered more than 1 in the Number of Circuits field and selected Auto-ranged, CTC automatically creates the number of circuits entered in the Number of Circuits field. If autoranging 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 autoranging. After completing the circuits, the Circuits window appears.
- If you entered more than 1 in the Number of Circuits field and did not choose Auto-ranged, the Circuit Creation dialog box appears for you to create the remaining circuits. Repeat Steps 5 through 17 for each additional circuit. After completing the circuits, the Circuits window appears.

Step 19 In the Circuits window, verify that the new circuits appear in the circuits list.

Step 20 Complete the "NTP-C46 Test Electrical Circuits" procedure on page 6-26. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-C38 Create a Manually Routed DS-1 Circuit

Purpose	This procedure creates a DS-1 circuit and provisions its circuit route.
Tools/Equipment	None
Prerequisite Procedures	NTP-C36 Verify Network Turn-Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at a node on the network 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-C56 Assign a Name to a Port" task on page 17-75. If not, continue with Step 3. CTC assigns a circuit name automatically based on circuit type, node name, and sequence number.

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** or **VT**. STS or VT cross-connects will carry the DS-1 circuit across the ONS network.
- Number of Circuits—Enter the number of DS-1 circuits that you want to create. The default is 1.
- Auto-ranged—Applies to automatically routed circuits only. If you entered more than 1 in Number of Circuits, uncheck this check box. (The check box is unavailable if only one circuit is entered in Number of Circuits.)

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-1 on page 6-7):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 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 you are creating an STS circuit, choose **STS-1**. If you are creating a VT circuit, Size displays VT1.5 and cannot be changed.
- Bidirectional—Leave the default unchanged (checked) for this 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. Also, 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-C111 Change a Circuit Service State" task on page 18-17.

Note If VT circuit source and destination ports are in an OOS-AU,AINS; OOS-MA,MT; or IS-NR service state, VT circuits in OOS-AU,AINS change to IS-NR even if a physical signal is not present.

For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

- Apply to drop ports—Check this check box 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 is 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.

- Protected Drops—Check this check box if you want the circuit routed on protected drops only, that is, to ports that are in 1+1 protection. If you check this check 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-C57 Provision Path Protection Selectors During Circuit Creation" task on page 17-75. Otherwise, continue with the next step.

Step 9 Click **Next**.

Step 10 Complete the "DLP-C58 Provision a DS-1 Circuit Source and Destination" task on page 17-76.

Step 11 In the Circuit Routing Preferences area (Figure 6-2 on page 6-8), 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.

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, check the **Dual Ring Interconnect** check box.

Step 15 If you are creating an STS circuit, skip this step and continue with Step 16. If you are creating a VT circuit, click **Next** and complete the "DLP-C59 Provision STS and VT Grooming Nodes" task on page 17-77.

Step 16 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 17 Complete the "DLP-C60 Provision a DS-1, DS-3, or EC-1 Circuit Route" task on page 17-78 for the DS-1 circuit that you are creating.

Step 18 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 19 If you entered more than 1 in the Number of Circuits field, the Circuit Creation dialog box appears for you to create the remaining circuits. Repeat Steps 5 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 are correct.

Step 21 Complete the "NTP-C46 Test Electrical Circuits" procedure on page 6-26. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-C39 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-C36 Verify Network Turn-Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at a node on the network 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-C56 Assign a Name to a Port" task on page 17-75. 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** or **VT**.
- Number of Circuits—Leave the default (1) unchanged.
- Auto-ranged—Unavailable when the Number of Circuits field is 1.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-3 on page 6-14):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 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 you are creating an STS circuit, choose **STS-1**. If you are creating a VT circuit, Size displays VT1.5 and cannot be changed.
- Bidirectional—Uncheck for this 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 this check box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Diagnostic—Leave the default (unchecked) unchanged.
- 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-C111 Change a Circuit Service State" task on page 18-17.

  Note If VT circuit source and destination ports are in an OOS-AU,AINS; OOS-MA,MT; or IS-NR service state, VT circuits in OOS-AU,AINS change to IS-NR even if a physical signal is not present.

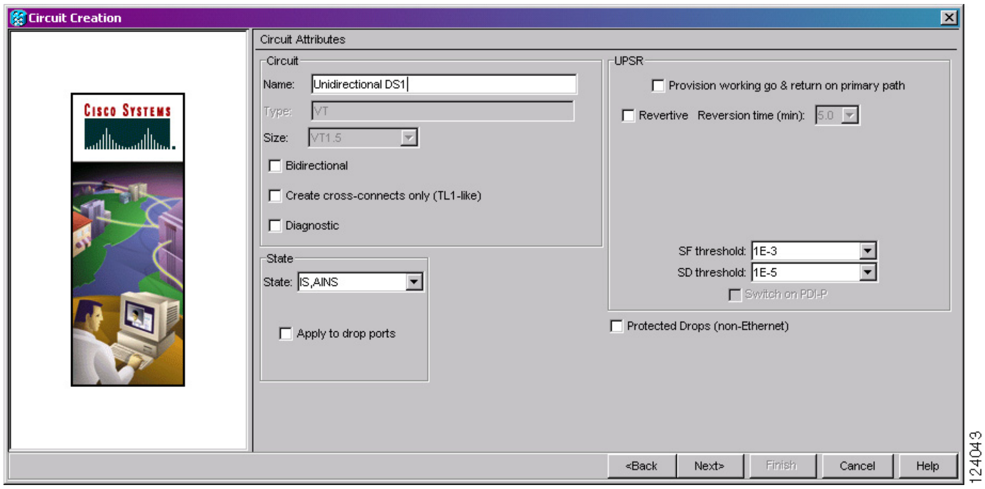
  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

- Apply to drop ports—Check this check box 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 is 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.

- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ports that are in 1+1 protection. If you check this check box, CTC displays only protected ports as source and destination choices.

Figure 6-3 Setting Circuit Attributes for a Unidirectional DS-1 Circuit



Circuit Creation

Circuit Attributes

Circuit
Name: Unidirectional DS1
Type: VT
Size: VT1.5
□ Bidirectional
□ Create cross-connects only (TL1-like)
□ Diagnostic

State
State: IS,AINS
□ Apply to drop ports

UPSR
□ Provision working go & return on primary path
□ Revertive Reversion time (min): 5.0
SF threshold: 1E-3
SD threshold: 1E-5
□ Switch on PDI-P

□ Protected Drops (non-Ethernet)

Step 8 Click **Next**.

Step 9 Complete the "DLP-C58 Provision a DS-1 Circuit Source and Destination" task on page 17-76.

Step 10 In the Circuit Routing Preferences area, uncheck **Route Automatically**. When Route Automatically is not checked, 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 14.

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 path protection DRI, check the **Dual Ring Interconnect** check box.

Step 14 If you are creating an STS circuit, skip this step and continue with Step 15. If you are creating a VT circuit, click **Next** and complete the "DLP-C59 Provision STS and VT Grooming Nodes" task on page 17-77.

Step 15 Click **Next**. In the Route Review and Edit area, node icons appear for you to route the circuit manually. 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 16 Complete the "DLP-C60 Provision a DS-1, DS-3, or EC-1 Circuit Route" task on page 17-78 for the DS-1 circuit that you are creating.

Step 17 Click **Finish**. CTC completes the circuit. The Circuits window appears.

Step 18 In the Circuits window, click the circuit that you want to route to multiple drops. The Delete, Edit, and Search buttons become active.

Step 19 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 display 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 20 In the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops appears.

Step 21 Click **Create**.

Step 22 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 DS-1 drop-down lists. The card selected in Step b determines the fields that appear. See Table 6-2 on page 6-2 for a list of options.

d. The routing preferences for the new drop will match those of the original circuit. If the original circuit was routed on a 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.

e. If you want to change the circuit state, choose the circuit state from the Target Circuit 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 State to the circuit source and destination drops.

g. Click **Finish**. The new drop appears in the Drops list.

Step 23 If you need to create additional drops for the circuit, repeat Steps 21 and 22 to create the additional drops.

Step 24 Click **Close**. The Circuits window appears.

Step 25 Verify that the new drops appear in the Destination column for the circuit you edited. If they do not appear repeat Steps 5 through 24, making sure all options are provisioned correctly.

Step 26 Complete the "NTP-C46 Test Electrical Circuits" procedure on page 6-26. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-C40 Create an Automatically Routed DS-3 or EC-1 Circuit

Purpose	This procedure creates an automatically routed DS-3 or EC-1 circuit. CTC routes the circuit automatically based on circuit creation parameters and the software version.
Tools/Equipment	None
Prerequisite Procedures	NTP-C36 Verify Network Turn-Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at a node on the network 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-C56 Assign a Name to a Port" task on page 17-75. 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 (both DS-3 and EC-1)** or **VT (EC-1 only)**.
- 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 autoranging 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. 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 this check box if you do not want CTC to create sequential circuits automatically.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-4 on page 6-17):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 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 you are creating an STS circuit, choose **STS-1**. If you are creating a VT circuit, Size displays VT1.5 and cannot be changed.
- Bidirectional—Leave the default (checked) for this 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. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Diagnostic—Leave the default (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-C111 Change a Circuit Service State" task on page 18-17.

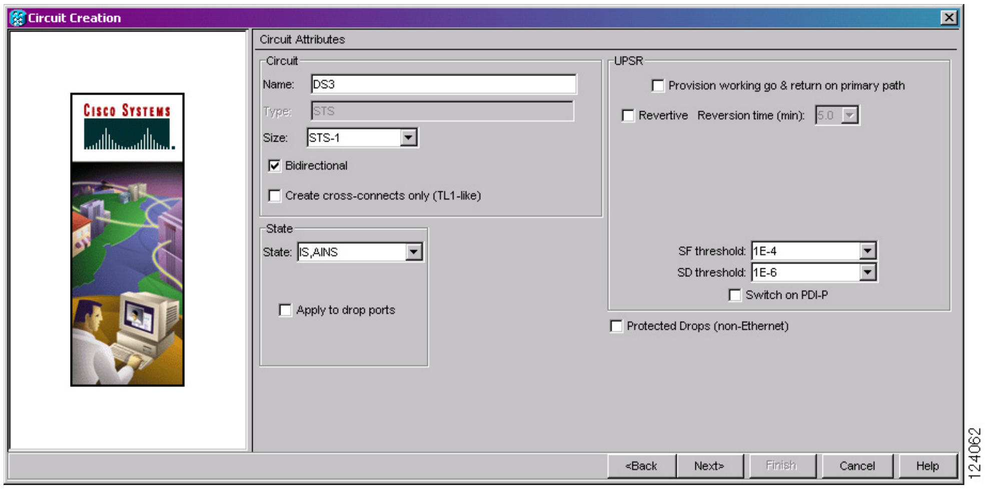
  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

- Apply to drop ports—Check this check box 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 is 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.

- Protected Drops—Check this check box if you want the circuit routed on protected drops only, that is, to ports that are in 1+1 protection. If you check this check box, CTC displays only protected cards and ports as source and destination choices.

Figure 6-4 Setting Circuit Attributes for a DS-3 or EC-1



Circuit Creation

Circuit Attributes

Circuit

Name: DS3

Type: STS

Size: STS-1

☑ Bidirectional

□ Create cross-connects only (TL1-like)

State

State: IS,AINS

□ Apply to drop ports

UPSR

□ Provision working go & return on primary path

□ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-6

□ Switch on PDI-P

□ Protected Drops (non-Ethernet)

Step 8 If the circuit will be routed on a path protection configuration, complete the "DLP-C57 Provision Path Protection Selectors During Circuit Creation" task on page 17-75.

Step 9 Click **Next**.

Step 10 Complete the "DLP-C61 Provision a DS-3 or EC-1 Circuit Source and Destination" task on page 17-79.

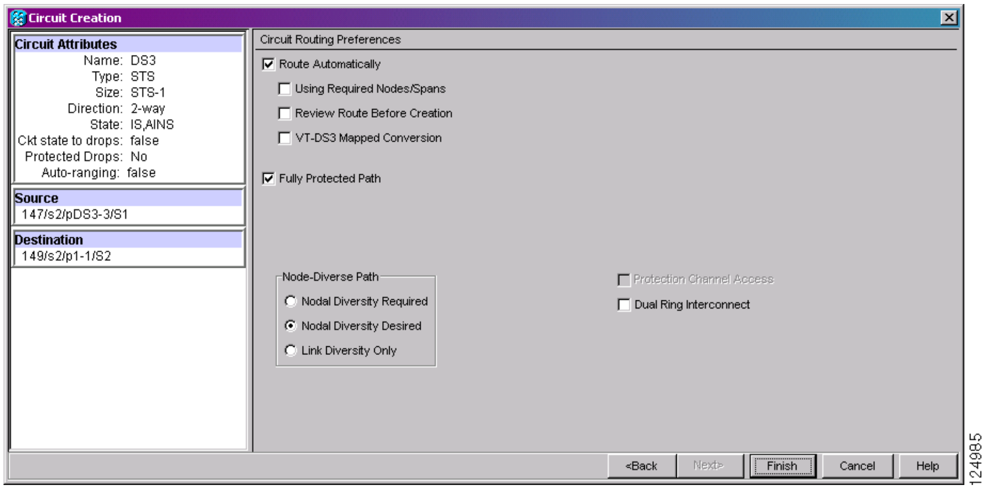
Step 11 In the Circuit Routing Preferences area (Figure 6-5), choose **Route Automatically**. Two options are available; choose either, both, or none based on your preferences:

- Using Required Nodes/Spans—Check this check box to specify nodes and spans to include or exclude in the CTC-generated 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 6-5 Setting Circuit Routing Preferences for a DS-3 or EC-1 Circuit



Circuit Creation

Circuit Attributes
Name: DS3
Type: STS
Size: STS-1
Direction: 2-way
State: IS,AINS
Ckt state to drops: false
Protected Drops: No
Auto-ranging: false

Source
147/s2/pDS3-3/S1

Destination
149/s2/p1-1/S2

Circuit Routing Preferences

☑ Route Automatically
☐ Using Required Nodes/Spans
☐ Review Route Before Creation
☐ VT-DS3 Mapped Conversion

☑ Fully Protected Path

Node-Diverse Path
○ Nodal Diversity Required
● Nodal Diversity Desired
○ Link Diversity Only

☐ Protection Channel Access
☐ Dual Ring Interconnect

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.

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 path protection DRI, check the **Dual Ring Interconnect** check box.

Step 15 If you selected Using Required Nodes/Spans in Step 11, complete the following substeps; otherwise, continue with Step 17:

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 determines the circuit sequence. Click spans twice to change the circuit direction.

d. Repeat Step c for each node or span you want to include or exclude.

e. Review the circuit route. To change the circuit routing order, choose a node from 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.

Note If a node or span stays gray, that node or span is required.

Step 16 If you are creating an STS circuit, skip this step and continue with Step 17. If you are creating a VT circuit, click **Next** and complete the "DLP-C59 Provision STS and VT Grooming Nodes" task on page 17-77.

Step 17 If you selected Review Route Before Creation in Step 11, complete the following substeps; otherwise, continue with Step 18.

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 the circuit information. If the circuit needs to be routed to a different path, see the "NTP-C41 Create a Manually Routed DS-3 or EC-1 Circuit" procedure on page 6-20.

Step 18 Click **Finish**. One of the following actions occurs based on the circuit properties you selected:

- If you entered 1 in the Number of Circuits field, CTC creates the circuit.
- If you entered more than 1 in the Number of Circuits field and chose Auto-ranged, CTC automatically creates the number of circuits entered in the Number of Circuits field. If autoranging 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 autoranging. After completing the circuits, the Circuits window appears.
- If you entered more than 1 in the Number of Circuits field and did not choose Auto-ranged, the Circuit Creation dialog box appears for you to create the remaining circuits. Repeat Steps 5 through 17 for each additional circuit. After completing the circuits, the Circuits window appears.

Step 19 In the Circuits window, verify that the circuits you just created appear in the circuits list.

Step 20 Complete the "NTP-C46 Test Electrical Circuits" procedure on page 6-26. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-C41 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 choose the circuit route.
Tools/Equipment	None
Prerequisite Procedures	NTP-C36 Verify Network Turn-Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at a node on the network 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-C56 Assign a Name to a Port" task on page 17-75. 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 (both DS-3 and EC-1)** or **VT (EC-1 only)**.
- Number of Circuits—Enter the number of DS-3 or EC-1 circuits that you want to create. The default is 1.
- Auto-ranged—Applies to automatically routed circuits only. If you entered more than 1 in Number of Circuits, uncheck this check box. (The check box is unavailable if only one circuit is entered in Number of Circuits.)

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-4 on page 6-17):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 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—If you are creating an STS circuit, choose **STS-1**. If you are creating a VT circuit, Size displays VT1.5 and cannot be changed.
- Bidirectional—Leave the default (checked).
- 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. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Diagnostic—Leave the default (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-C111 Change a Circuit Service State" task on page 18-17.

For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

- Apply to drop ports—Check this check box 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 is 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.

- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ports that are in 1+1 protection. If you check this check box, CTC displays only protected cards as source and destination choices.

Step 8 If the circuit will be routed on a path protection configuration, complete the "DLP-C57 Provision Path Protection Selectors During Circuit Creation" task on page 17-75.

Step 9 Click **Next**.

Step 10 Complete the "DLP-C61 Provision a DS-3 or EC-1 Circuit Source and Destination" task on page 17-79.

Step 11 In the Circuit Routing Preferences area (Figure 6-5 on page 6-18), 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 15.

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, check the **Dual Ring Interconnect** check box.

Step 15 If you are creating an STS circuit, skip this step and continue with Step 16. If you are creating a VT circuit, click **Next** and complete the "DLP-C59 Provision STS and VT Grooming Nodes" task on page 17-77.

Step 16 Click **Next**. In the Route Review and Edit area, node icons appear for you to 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 17 Complete the "DLP-C60 Provision a DS-1, DS-3, or EC-1 Circuit Route" task on page 17-78 for the DS-3 or EC-1 circuit that you are creating.

Step 18 Click **Finish**.

Step 19 If you entered more than 1 in the Number of Circuits field, the Circuit Creation dialog box appears for you to create the remaining circuits. Repeat Steps 5 through 17 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 "NTP-C46 Test Electrical Circuits" procedure on page 6-26. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-C42 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	None
Prerequisite Procedures	NTP-C36 Verify Network Turn-Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at a node on the network 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-C56 Assign a Name to a Port" task on page 17-75. 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 (both DS-3 and EC-1)** or **VT (EC-1 only)**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable when the Number of Circuits is 1.

Step 6 Click **Next**.

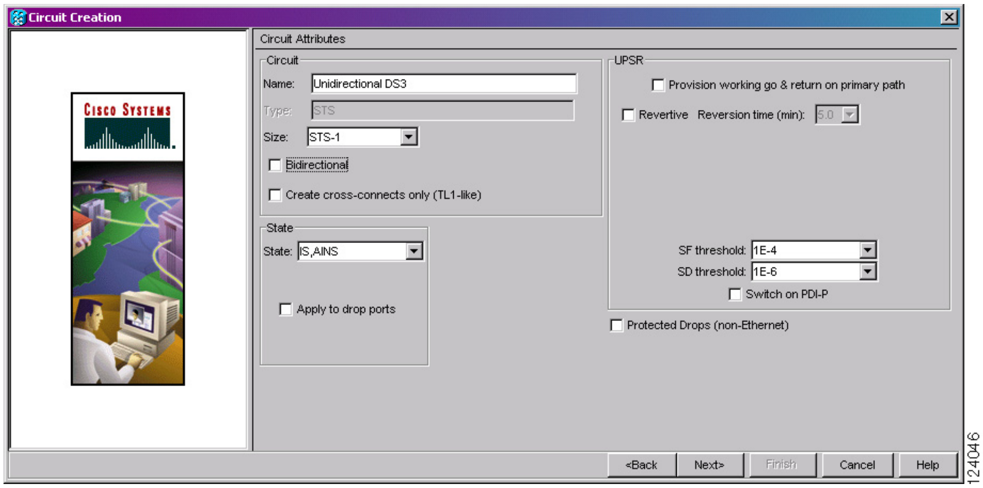
Step 7 Define the circuit attributes (Figure 6-6 on page 6-24):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 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 you are creating an STS circuit, choose **STS-1**. If you are creating a VT circuit, Size displays VT1.5 and cannot be changed.
- Bidirectional—Uncheck for this 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. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Diagnostic—Leave the default (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-C111 Change a Circuit Service State" task on page 18-17.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual.*
- Apply to drop ports—Check this check box 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 is 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.
- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ports that are in 1+1 protection. If you check this check box, CTC displays only protected cards as source and destination choices.

Figure 6-6 Setting Circuit Attributes for a Unidirectional DS-3 or EC-1 Circuit



Circuit Creation

Circuit Attributes

Circuit
Name: Unidirectional DS3
Type: STS
Size: STS-1
□ Bidirectional
□ Create cross-connects only (TL1-like)

State
State: IS,AINS
□ Apply to drop ports

UPSR
□ Provision working go & return on primary path
□ Revertive Reversion time (min): 5.0
SF threshold: 1E-4
SD threshold: 1E-6
□ Switch on PDI-P

□ Protected Drops (non-Ethernet)

Step 8 If the circuit will be routed on a path protection configuration, complete the "DLP-C57 Provision Path Protection Selectors During Circuit Creation" task on page 17-75.

Step 9 Click **Next**.

Step 10 Complete the "DLP-C61 Provision a DS-3 or EC-1 Circuit Source and Destination" task on page 17-79.

Step 11 Uncheck **Route Automatically**. When Route Automatically is not checked, Using Required Nodes/Spans and Review Route Before Circuit Creation 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.

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, check the **Dual Ring Interconnect** check box.

Step 15 If you are creating an STS circuit, skip this step and continue with Step 16. If you are creating a VT circuit, click **Next** and complete the "DLP-C59 Provision STS and VT Grooming Nodes" task on page 17-77.

Step 16 Click **Next**. In the Route Review and Edit area, node icons appear for you to route the circuit manually. 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 17 Complete the "DLP-C60 Provision a DS-1, DS-3, or EC-1 Circuit Route" task on page 17-78 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 display 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 lists display. See Table 6-2 on page 6-2 for a list of options.

d. VT—If applicable, choose the VT from the VT drop-down list.

e. The routing preferences for the new drop will match those of the original circuit. If the original circuit was routed on a protected path, you can change the nodal diversity options: Nodal Diversity Required, Nodal Diversity Desired, or Link Diversity Only. See Step 13 for option descriptions.

f. If you want to change the circuit state, choose the circuit state from the Target Circuit State drop-down list. The state chosen applies to the entire circuit.

g. Check **Apply to drop ports** if you want to apply the state chosen in the Target Circuit State to the circuit source and destination drops.

h. 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 this procedure, making sure all options are provisioned correctly.

Step 27 Complete the "NTP-C46 Test Electrical Circuits" procedure on page 6-26. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-C46 Test Electrical Circuits

Purpose	This procedure tests DS-1, DS-3, and EC-1 circuits.
Tools/Equipment	A test set and all appropriate cables
Prerequisite Procedures	This procedure assumes you completed a facility loopback tests on the fibers and cables from the source and destination nodes to the DSX and that you created a circuit using one of the following procedures: NTP-C37 Create an Automatically Routed DS-1 Circuit, page 6-6 NTP-C38 Create a Manually Routed DS-1 Circuit, page 6-10 NTP-C39 Create a Unidirectional DS-1 Circuit with Multiple Drops, page 6-12 NTP-C40 Create an Automatically Routed DS-3 or EC-1 Circuit, page 6-16 NTP-C41 Create a Manually Routed DS-3 or EC-1 Circuit, page 6-20 NTP-C42 Create a Unidirectional DS-3 or EC-1 Circuit with Multiple Drops, page 6-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at a node on the network where you created the 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-C111 Change a Circuit Service State" task on page 18-17 to set the circuit and circuit ports to the OOS-MA,MT service state. Note the original state because you will change it back at the end of the procedure.

Step 5 Set the source and destination DS-1 port 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 node.
- **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 being tested.

Step 7 Attach loopback cables to the circuit source node:

a. Test the loopback cable by connecting one end to the test set Tx port and the other end to the test set 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. 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 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 panel or use the high-density DS-1 interface through the LFH-96 connector. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3/EC-1—If you are testing a clear channel DS-3 or EC-1, you must have a direct DS-3/EC-1 interface into the node through the broadband electrical (BBE) ports on the CTX card. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.

Step 9 Verify that the test set displays 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 display at the source and destination nodes.

Step 11 Clear the performance monitoring (PM) counts for the ports that you tested. See the "DLP-C95 Clear Selected PM Counts" task on page 17-114 for instructions.

Step 12 Complete the "DLP-C111 Change a Circuit Service State" task on page 18-17 to set the circuit and circuit ports to their original service state.

Step 13 As needed, complete the "DLP-C55 Path Protection Switching Test" task on page 17-73.

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 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-C43 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-C36 Verify Network Turn-Up, page 6-4
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 nodes without consuming VT matrix resources on the 15310-CL-CTX or CTX2500 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 15310-CL and Cisco ONS 15310-MA Reference Manual* for more information.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at a node on the network 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-C56 Assign a Name to a Port" task on page 17-75. 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**.

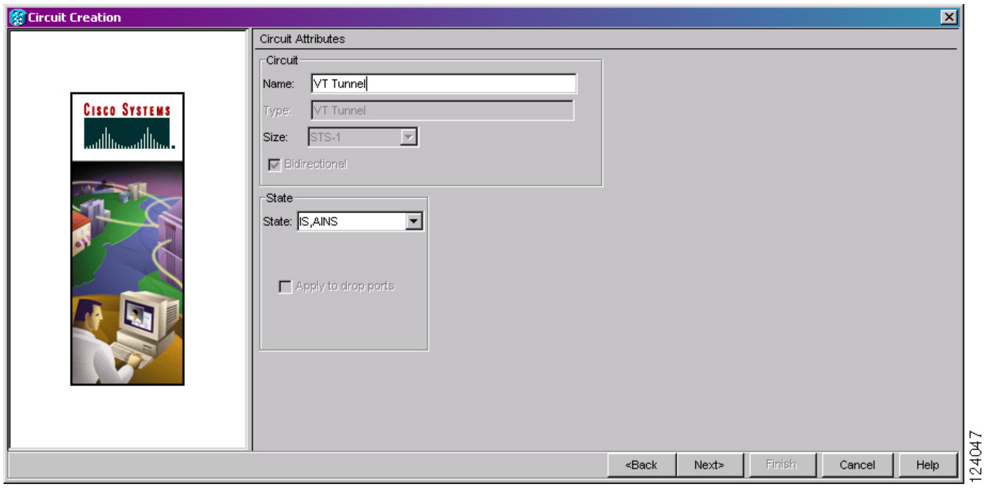
Step 7 Define the circuit attributes (Figure 6-7 on page 6-29):

- Name—Assign a name to the VT tunnel. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 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 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-C111 Change a Circuit Service State" task on page 18-17.

  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 15310-CL and Cisco ONS 15310-MA Reference Manual.*
- Apply to drop ports—Unavailable for VT tunnels.

Figure 6-7 Setting Attributes for a VT Tunnel



Circuit Creation

Circuit Attributes

Circuit

Name: VT Tunnel

Type: VT Tunnel

Size: STS-1

☑ Bidirectional

State

State: IS,AINS

☐ Apply to drop ports

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.

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 Step c for each node or span you want 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.

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-C44 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-C36 Verify Network Turn-Up, page 6-4
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 nodes without consuming VT matrix resources on the 15310-CL-CTX or CTX2500 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 15310-CL and Cisco ONS 15310-MA Reference Manual* for more information.

Step 1 Complete the “DLP-C29 Log into CTC” task on page 17-44 at a node on the network 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-C56 Assign a Name to a Port” task on page 17-75. 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 6-7 on page 6-29):

- Name—Assign a name to the VT tunnel. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 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 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-C111 Change a Circuit Service State" task on page 18-17.

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 15310-CL and Cisco ONS 15310-MA Reference Manual*.

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 for you to 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-C62 Provision a VT Tunnel Route" task on page 17-80 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-C45 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 port. VAPs allow multiple VT1.5 circuits to pass through the 15310-CL-CTX or CTX2500 card without utilizing resources on the 15310-CL-CTX or CTX2500 card VT matrix.
Tools/Equipment	None
Prerequisite Procedures	NTP-C36 Verify Network Turn-Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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 no other VT1.5 circuits terminate at the node, the maximum number of VAPs that can terminate at one node is five for the ONS 15310-CL and ten for the ONS 15310-MA.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at a node on the network 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-C56 Assign a Name to a Port" task on page 17-75. 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 6-8 on page 6-33):

- 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 44 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—(Display only) Displays STS-1.
- Bidirectional—(Display only) The check box is checked.
- 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.

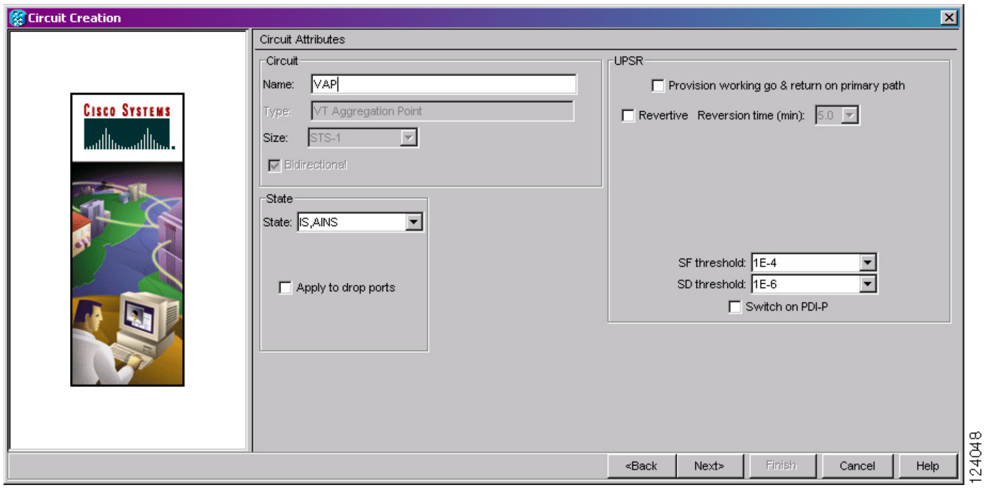
- **OOS,MT**—Puts the circuit cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the "DLP-C111 Change a Circuit Service State" task on page 18-17.

> **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 15310-CL and Cisco ONS 15310-MA Reference Manual*.

- Apply to drop ports—Uncheck this check box.

Figure 6-8 Setting Attributes for a VT Aggregation Point



Circuit Creation

Circuit Attributes

Circuit

Name: VAP

Type: VT Aggregation Point

Size: STS-1

☑ Bidirectional

State

State: IS,AINS

□ Apply to drop ports

UPSR

□ Provision working go & return on primary path

□ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-6

□ Switch on PDI-P

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 port where the VAP will originate.

c. From the Port drop-down list, choose the desired port.

d. 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**. 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 VAP 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 VAP route before the circuit is created.

Step 14 If you selected Using Required Nodes/Spans in Step 13, complete the following steps:

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 Step c for each node or span you want 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 15 If you selected Review Route Before Creation in Step 13, complete the following steps:

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 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-C47 Create an Automatically Routed Optical Circuit

Purpose	This procedure creates an automatically routed optical circuit.
Tools/Equipment	None
Prerequisite Procedures	NTP-C36 Verify Network Turn-Up, page 6-4 NTP-C130 Manage Pluggable Port Modules, page 10-3 (as needed)
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at a node on the network 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-C56 Assign a Name to a Port" task on page 17-75. 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-100T-8 circuits, complete the "DLP-C190 Provision CE-100T-8 Card Ethernet Ports" task on page 18-89.
- To provision POS ports for CE-100T-8 circuits, complete the "DLP-C191 Provision CE-100T-8 Card POS Ports" task on page 18-91.
- To provision link integrity soak timer for Ethernet card, complete the "DLP-C278 Configure Link Integrity Timer" task on page 19-93.

Step 4 From the View menu, choose **Go to Network View**.

Step 5 Click the **Circuits** tab, then click **Create**.

- Circuit Type—Choose **STS** or **VT**.
- 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 autoranging to create the circuits automatically.
- Auto-ranged—This check box is automatically checked when you enter more than 1 in the Number of Circuits field. Leave checked if you are creating multiple optical circuits with the same source and destination and you want CTC to create the circuits automatically. Uncheck this check box if you do not want CTC to create the circuits automatically.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-9 on page 6-36):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 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 optical circuit size. If you are creating an STS circuit, the choices are STS-1, STS-3c, STS-6c, STS-9c, or STS-12c. If you are creating a VT circuit, the Size displays VT1.5. You cannot change it.
- Bidirectional—Leave the default (checked) for this 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. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Diagnostic—Leave the default (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-C111 Change a Circuit Service State" task on page 18-17.

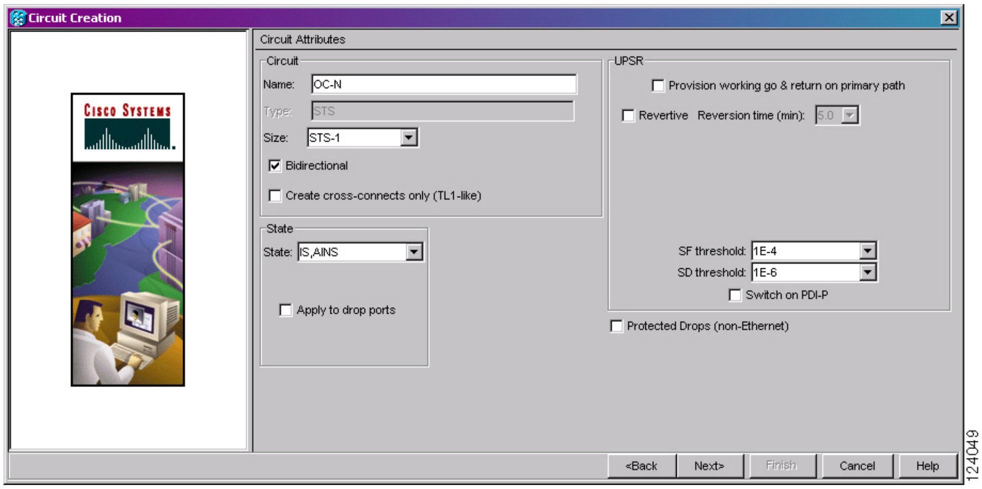
For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

- Apply to drop ports—Check this check box 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 is 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.

- Protected Drops—Check this check box if you want the circuit routed to protected drops only, that is, to ports that are in 1+1 protection. If you check this check box, CTC displays only protected cards as source and destination choices.

Figure 6-9 Setting Circuit Attributes for an Optical Circuit



Circuit Attributes

Circuit
Name: OC-N
Type: STS
Size: STS-1
☑ Bidirectional
□ Create cross-connects only (TL1-like)

State
State: IS,AINS
□ Apply to drop ports

UPSR
□ Provision working go & return on primary path
□ Revertive Reversion time (min): 5.0
SF threshold: 1E-4
SD threshold: 1E-6
□ Switch on PDI-P

□ Protected Drops (non-Ethernet)

Step 8 If the circuit will be routed on a path protection configuration, complete the "DLP-C57 Provision Path Protection Selectors During Circuit Creation" task on page 17-75.

Step 9 Click **Next**.

Step 10 Complete the "DLP-C63 Provision an OC-N Circuit Source and Destination" task on page 17-80 for the optical circuit that you are creating.

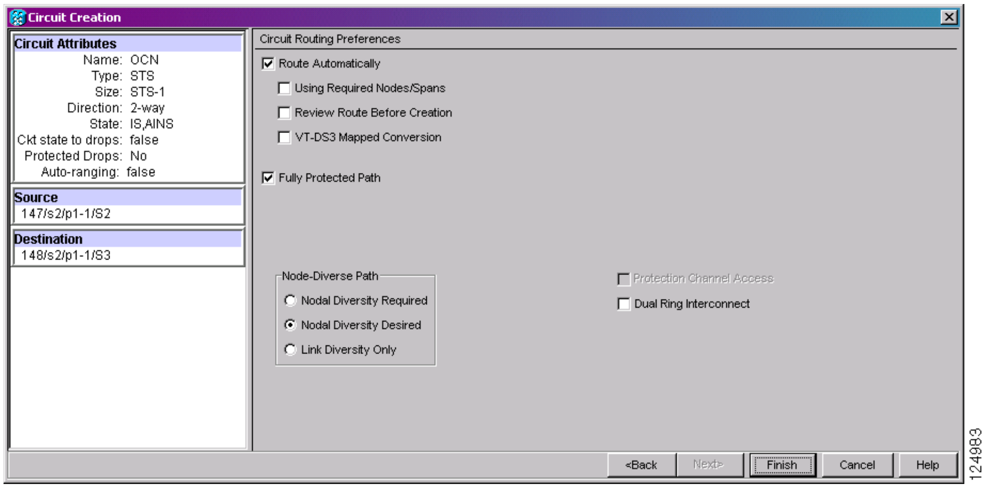
Step 11 In the Circuit Routing Preferences area (Figure 6-10), choose **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- Using Required Nodes/Spans—Check this check box to specify nodes and spans to include or exclude in the CTC-generated 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 6-10 *Setting Circuit Routing Preferences for an Optical Circuit*



Circuit Attributes
Name: OCN
Type: STS
Size: STS-1
Direction: 2-way
State: IS,AINS
Ckt state to drops: false
Protected Drops: No
Auto-ranging: false

Source
147/s2/p1-1/S2

Destination
148/s2/p1-1/S3

Circuit Routing Preferences

☑ Route Automatically
☐ Using Required Nodes/Spans
☐ Review Route Before Creation
☐ VT-DS3 Mapped Conversion

☑ Fully Protected Path

Node-Diverse Path
○ Nodal Diversity Required
● Nodal Diversity Desired
○ Link Diversity Only

☐ Protection Channel Access
☐ Dual Ring Interconnect

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.

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 path protection DRI, check the **Dual Ring Interconnect** check box.

Step 15 If you selected Using Required Nodes/Spans in Step 11, complete the following substeps. If not, continue with Step 17:

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, 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.

d. Repeat Step c for each node or span you want 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.

Step 16 If you are creating an STS circuit, skip this step and continue with Step 17. If you are creating a VT circuit, click **Next** and complete the "DLP-C59 Provision STS and VT Grooming Nodes" task on page 17-77.

Step 17 If you selected Review Route Before Creation in Step 11, complete the following substeps; otherwise, continue with Step 18:

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 the circuit information. If the circuit needs to be routed to a different path, see the "NTP-C48 Create a Manually Routed Optical Circuit" procedure on page 6-39 to assign the circuit route yourself.

Step 18 Click **Finish**. One of the following results occurs, based on the circuit properties you provisioned in the Circuit Creation dialog box:

- If you entered 1 in the Number of Circuits field, CTC creates the circuit.
- If you entered more than 1 in Number of Circuits and chose Auto-ranged, CTC automatically creates the number of circuits entered in Number of Circuits. If autoranging 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 autoranging. After completing the circuits, the Circuits window appears.
- If you entered more than 1 in Number of Circuits and did not choose Auto-ranged, the Circuit Creation dialog box appears for you to create the remaining circuits. Repeat Steps 7 through 17 for each additional circuit. After completing the circuits, the Circuits window appears.

Step 19 In the Circuits window, verify that the circuits you created appear in the circuits list.

Step 20 Complete the "NTP-C50 Test Optical Circuits" procedure on page 6-44. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-C48 Create a Manually Routed Optical Circuit

Purpose	This procedure creates a manually routed optical circuit.
Tools/Equipment	None
Prerequisite Procedures	NTP-C36 Verify Network Turn-Up, page 6-4
	NTP-C130 Manage Pluggable Port Modules, page 10-3 (as needed)
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at a node on the network 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-C56 Assign a Name to a Port" task on page 17-75. 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-100T-8 circuits, complete the "DLP-C190 Provision CE-100T-8 Card Ethernet Ports" task on page 18-89.
- To provision POS ports for CE-100T-8 circuits, complete the "DLP-C191 Provision CE-100T-8 Card POS Ports" task on page 18-91.
- To provision link integrity soak timer for Ethernet card, complete the "DLP-C278 Configure Link Integrity Timer" task on page 19-93.

Step 4 From the View menu, choose **Go to Network View**.

Step 5 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **STS** or **VT**.
- Number of Circuits—Enter the number of optical circuits that you want to create. The default is 1.
- Auto-ranged—Applies to 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 Number of Circuits.)

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 44 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 optical circuit size. If you are creating an STS circuit, the choices are STS-1, STS-3c, STS-6c, STS-9c, or STS-12c. If you are creating a VT circuit, Size displays VT1.5. You cannot change it.
- Bidirectional—Leave the default (checked) for this 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. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Diagnostic—Leave the default (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-C111 Change a Circuit Service State" task on page 18-17.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.
- Apply to drop ports—Check this check box 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 is 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.
- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ports that are in 1+1 protection. If you check this check box, CTC displays only protected cards as source and destination choices.

Step 8 If the circuit will be routed on a path protection configuration, complete the "DLP-C57 Provision Path Protection Selectors During Circuit Creation" task on page 17-75.

Step 9 Click **Next**.

Step 10 Complete the "DLP-C63 Provision an OC-N Circuit Source and Destination" task on page 17-80 for the optical circuit that you are creating.

Step 11 In the Circuit Routing Preferences area (Figure 6-10 on page 6-37), 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.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.

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, check the **Dual Ring Interconnect** check box.

Step 15 If you are creating an STS circuit, skip this step and continue with Step 16. If you are creating a VT circuit, click **Next** and complete the "DLP-C59 Provision STS and VT Grooming Nodes" task on page 17-77.

Step 16 Click **Next**. In the Route Review and Edit area, node icons appear for you to route the circuit manually.

Step 17 Complete the "DLP-C64 Provision an OC-N Circuit Route" task on page 17-81.

Step 18 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 Number of Circuits, the Circuit Creation dialog box appears after the circuit is created for you to create the remaining circuits. Repeat Steps 5 through 17 for each additional circuit.

Step 19 When all the circuits are created, the main Circuits window appears. Verify that the circuits you created appear in the window.

Step 20 Complete the "NTP-C50 Test Optical Circuits" procedure on page 6-44. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-C49 Create a Unidirectional Optical Circuit with Multiple Drops

Purpose	This procedure creates a unidirectional optical circuit with multiple traffic drops (circuit destinations).
Tools/Equipment	None
Prerequisite Procedures	NTP-C36 Verify Network Turn-Up, page 6-4 NTP-C130 Manage Pluggable Port Modules, page 10-3 (as needed)
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at a node on the network 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-C56 Assign a Name to a Port" task on page 17-75. 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** or **VT**.

- 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:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 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. If you are creating an STS circuit, the choices are STS-1, STS-3c, STS-6c, STS-9c, or STS-12c. If you are creating a VT circuit, Size displays VT1.5. You cannot change it.
- Bidirectional—Uncheck this check box for this 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. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Diagnostic—Leave the default (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-C111 Change a Circuit Service State" task on page 18-17.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.
- Apply to drop ports—Check this check box 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 is 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.
- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ports that are in 1+1 protection. If you check this check box, CTC displays only protected cards as source and destination choices.

Step 8 If the circuit will be routed on a path protection configuration, complete the "DLP-C57 Provision Path Protection Selectors During Circuit Creation" task on page 17-75.

Step 9 Click **Next**.

Step 10 Complete the "DLP-C63 Provision an OC-N Circuit Source and Destination" task on page 17-80 for the circuit that you are creating.

Step 11 Uncheck **Route Automatically**. When Route Automatically is not checked, Using Required Nodes/Spans and Review Route Before Circuit Creation 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.

Step 13 If you selected Fully Protected Path in Step 12, 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 path protection DRI, check the **Dual Ring Interconnect** check box.

Step 15 If you are creating an STS circuit, skip this step and continue with Step 16. If you are creating a VT circuit, click **Next** and complete the "DLP-C59 Provision STS and VT Grooming Nodes" task on page 17-77.

Step 16 Click **Next**. In the Route Review and Edit area, node icons appear for you to 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 17 Complete the "DLP-C64 Provision an OC-N Circuit Route" task on page 17-81.

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. Circuit source and destination information appears under the source and destination nodes. To display 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, pressing **Ctrl** and 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 choice in these menus depends on the card selected in Step b. See Table 6-2 on page 6-2 for a list of options.

d. The routing preferences for the new drop will match those of the original circuit. If the original circuit was routed on a protected path, you can change the nodal diversity options: Nodal Diversity Required, Nodal Diversity Desired, or Link Diversity Only. See Step 13 for options descriptions.

e. Click **OK**. 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 5 through 25 making sure all options are provisioned correctly.

Step 27 Complete the "NTP-C50 Test Optical Circuits" procedure on page 6-44. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-C50 Test Optical Circuits

Purpose	This procedure tests an optical circuit.
Tools/Equipment	Test set capable of optical speeds, appropriate fibers, and attenuators
Prerequisite Procedures	This procedure assumes you completed facility loopback tests to test the fibers and cables from the source and destination ONS 15310-CLs or ONS 15310-MAs to the fiber distribution panel or the DSX and one of following circuit procedures: NTP-C47 Create an Automatically Routed Optical Circuit, page 6-34 NTP-C48 Create a Manually Routed Optical Circuit, page 6-39 NTP-C49 Create a Unidirectional Optical Circuit with Multiple Drops, page 6-41
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at a node on the network where you created the 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-C111 Change a Circuit Service State" task on page 18-17 to set the circuit and circuit ports to the OOS-MA,MT service state. Note the original state because you will change it back at the end of the procedure.

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 set 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 loopback 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 set 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 port:

- OC-3 ports—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 ports—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.

Step 8 Verify that the test set displays 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 display at the source and destination nodes.

Step 10 Clear the PM counts for the ports that you tested. See the "DLP-C95 Clear Selected PM Counts" task on page 17-114 for instructions.

Step 11 Complete the "DLP-C55 Path Protection Switching Test" task on page 17-73.

Step 12 Perform a BERT for 12 hours or a duration dictated by local testing custom. For information about configuring your test set for 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-C111 Change a Circuit Service State" task on page 18-17 to return the circuit and circuit ports to their original service state.

Stop. You have completed this procedure.

NTP-C51 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 15310-CL and Cisco ONS 15310-MA Reference Manual*.
Tools/Equipment	ML-100T-8 or CE-100T-8 cards must be installed at the nodes used in the VCAT circuit. For information about the ML-100T-8 or CE-100T-8 cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.
Prerequisite Procedures	NTP-C36 Verify Network Turn-Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 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-100T-8 circuits, complete the "DLP-C190 Provision CE-100T-8 Card Ethernet Ports" task on page 18-89.
- To provision POS ports for CE-100T-8 circuits, complete the "DLP-C191 Provision CE-100T-8 Card POS Ports" task on page 18-91.
- To provision a VCAT circuit that traverses through a third-party network, complete the "NTP-C140 Create a Server Trail" procedure on page 6-56.
- To provision link integrity soak timer for Ethernet card, complete the "DLP-C278 Configure Link Integrity Timer" task on page 19-93.

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.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-11 on page 6-48):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 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 the administrative state to apply to all of the member cross-connects in a VCAT circuit:
  - **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 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 member 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**—(LCAS 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. OOS-MA,OOG applies only 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.
- 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 is 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.
- 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 15310-CL and Cisco ONS 15310-MA 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 15310-CL and Cisco ONS 15310-MA 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:
  - None—Provides no protection. A failure on one member causes the entire VCAT circuit to fail. For CE-100T-8 card, 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 ML-100T-8 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 provides interoperability with the ONS 15454 ML-Series cards. SW-LCAS uses legacy SONET failure indicators like AIS-P and RDI-P to detect member failure. You cannot add or delete members from a VCAT circuit with SW-LCAS protection.

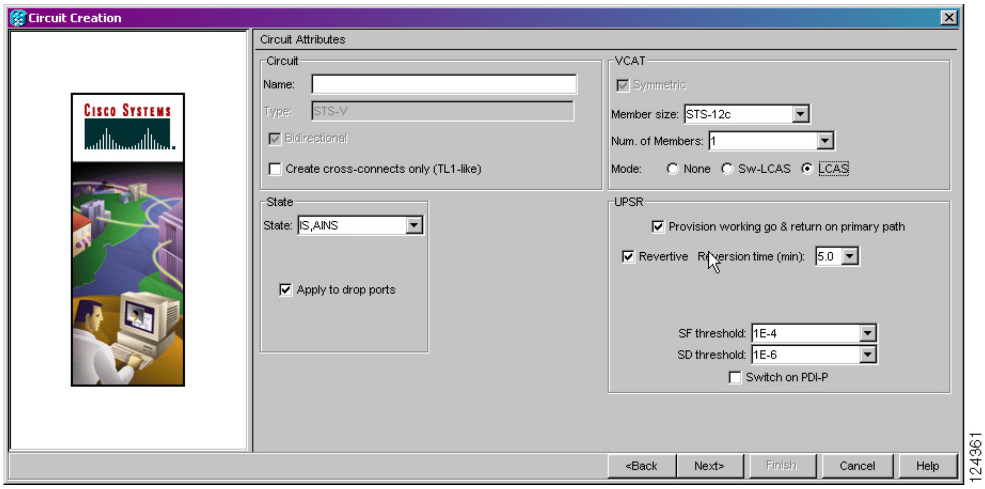
Note While deleting SW-LCAS circuit members change the administrative state of the members to OOS,DSBLD. This is applicable to circuits created on CE-Series and ML-Series cards.

- LCAS—Sets the VCAT circuit to use LCAS. With LCAS, you can add or delete members without interrupting the operation of noninvolved 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 mode for CE-100T-8 and ML-100T-8 cards that do not need to interoperate with the ONS 15454 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 6-11 Setting VCAT Circuit Attributes



Circuit
Name:
Type: STS-V
☑ Bidirectional
☐ Create cross-connects only (TL1-like)

VCAT
☑ Symmetric
Member size: STS-12c
Num. of Members: 1
Mode: ○ None ○ Sw-LCAS ● LCAS

State
State: IS,AINS
☑ Apply to drop ports

UPSR
☑ Provision working go & return on primary path
☑ Revertive Reversion time (min): 5.0
SF threshold: 1E-4
SD threshold: 1E-6
☐ Switch on PDI-P

Step 8 Click **Next**.

Step 9 Complete the "DLP-C65 Provision a VCAT Circuit Source and Destination" task on page 17-82 for the VCAT circuit that you are creating.

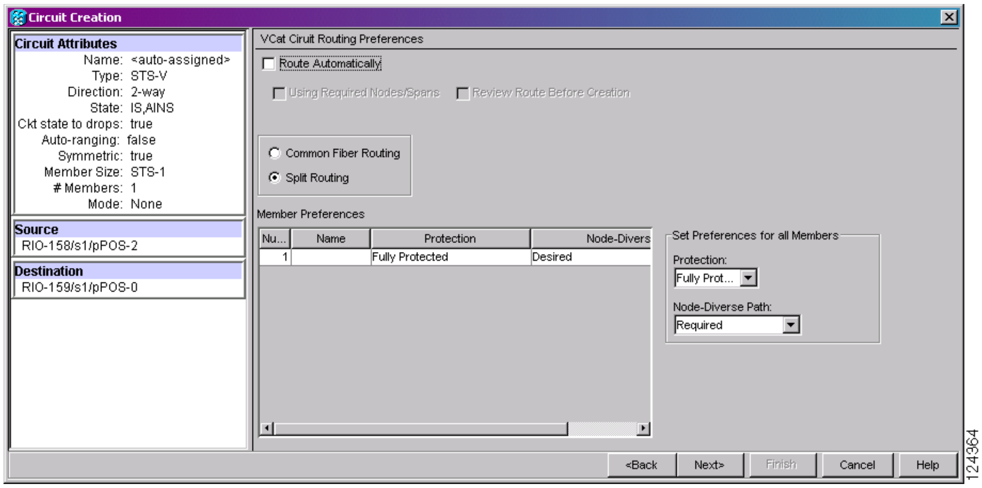
Step 10 In the VCAT Circuit Routing Preferences area (Figure 6-12), check **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- 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 6-12 Automatically Routing a VCAT Circuit



Circuit Creation

Circuit Attributes

Name: <auto-assigned>
Type: STS-V
Direction: 2-way
State: IS,AINS
Ckt state to drops: true
Auto-ranging: false
Symmetric: true
Member Size: STS-1
Members: 1
Mode: None

Source
RIO-158/s1/pPOS-2

Destination
RIO-159/s1/pPOS-0

VCat Ciruit Routing Preferences

☐ Route Automatically

☐ Using Required Nodes/Spans ☐ Review Route Before Creation

○ Common Fiber Routing
● Split Routing

Member Preferences

Nu...	Name	Protection	Node-Divers
1		Fully Protected	Desired

Set Preferences for all Members

Protection: Fully Prot...

Node-Diverse Path: Required

Step 11 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.

Step 12 If you want to set preferences for individual members, complete the following in the Member Preferences area. To set identical preferences for all members, skip this step and continue with Step 13.

- Number—Choose a number 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—(Future use) Routes the member on a bidirectional line switched ring (BLSR) protection channel.

    Note Although ONS 15310-CLs and ONS 15310-MAs do not support BLSR, you can route an LCAS VCAT circuit over a BLSR network of ONS 15600s or ONS 15454s.

  - DRI—(Split routing only) Routes the member on a DRI 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—(Future use) Routes the member on a BLSR protection channel.
  - DRI—(Split routing only) Routes the member on a DRI circuit.
- Node-Diverse Path—(Split routing only) Available when Fully Protected is chosen.

Step 14 Click **Next**. If you chose Fully Protected, click **OK** in the confirmation dialog box to continue. If not, continue with Step 15.

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 Route Constraints area, choose the member that you want to route from the Route Member number drop-down list (Figure 6-13).

b. Click a node or span on the circuit map.

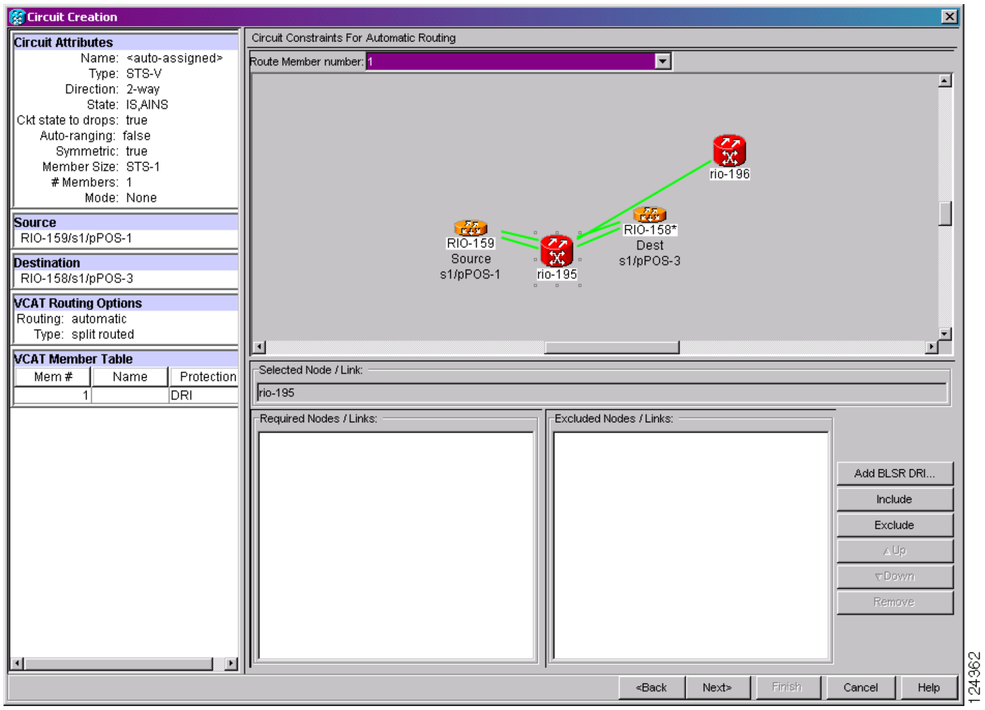
c. Click **Include** to include the node or span in the circuit, or click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans is the order in which the circuit is routed. Click spans twice to change the circuit direction.

d. Repeat Steps b and c for each node or span you want 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 6-13 VCAT Circuit Route Constraints



Circuit Creation

Circuit Attributes

Name: <auto-assigned>
Type: STS-V
Direction: 2-way
State: IS,AINS
Ckt state to drops: true
Auto-ranging: false
Symmetric: true
Member Size: STS-1
Members: 1
Mode: None

Source
RIO-159/s1/pPOS-1

Destination
RIO-158/s1/pPOS-3

VCAT Routing Options
Routing: automatic
Type: split routed

VCAT Member Table

Mem #	Name	Protection
1		DRI

Circuit Constraints For Automatic Routing

Route Member number: 1

Selected Node / Link: rio-195

Required Nodes / Links:

Excluded Nodes / Links:

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 the circuit information. If the circuit needs to be routed to a different path, see the "NTP-C52 Create a Manually Routed VCAT Circuit" procedure on page 6-52 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 might take several minutes.

Step 18 In the Circuits window, verify that the circuits you created appear in the circuits list.

Step 19 As needed, complete the "DLP-C190 Provision CE-100T-8 Card Ethernet Ports" task on page 18-89 and/or the "DLP-C191 Provision CE-100T-8 Card POS Ports" task on page 18-91.

Stop. You have completed this procedure.

NTP-C52 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 15310-CL and Cisco ONS 15310-MA Reference Manual*.
Tools/Equipment	ML-100T-8 or CE-100T-8 cards must be installed at the nodes used in the VCAT circuit. For information about the ML-100T-8 and CE-100T-8 cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.
Prerequisite Procedures	NTP-C36 Verify Network Turn-Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 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-C56 Assign a Name to a Port" task on page 17-75. 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-100T-8 circuits, complete the "DLP-C190 Provision CE-100T-8 Card Ethernet Ports" task on page 18-89.
- To provision POS ports for CE-100T-8 circuits, complete the "DLP-C191 Provision CE-100T-8 Card POS Ports" task on page 18-91.
- To provision link integrity soak timer for Ethernet card, complete the "DLP-C278 Configure Link Integrity Timer" task on page 19-93.
- To provision a VCAT circuit that traverses through a third-party network, complete the "NTP-C140 Create a Server Trail" procedure on page 6-56.

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.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 6-11 on page 6-48):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 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 the administrative state to apply to all of the member cross-connects in a VCAT circuit:
  - **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 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 member 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**—(LCAS 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. OOS-MA,OOG applies only 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.
- 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 is 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.
- 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 15310-CL and Cisco ONS 15310-MA Reference Manual*.
- Num. of members—Choose the number of members from the drop-down list. For information about the number of members supported for each card, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA 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:
  - None—Provides no protection. A failure on one member causes the entire VCAT circuit to fail. For CE-100T-8 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 ML-100T-8 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 provides interoperability with the ONS 15454 ML-Series cards. SW-LCAS uses legacy SONET failure indicators like AIS-P and RDI-P to detect member failure. You cannot add or delete members from a VCAT circuit with SW-LCAS protection.

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 noninvolved 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 and ML-100T-8 cards that do not need to interoperate with the ONS 15454 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-C65 Provision a VCAT Circuit Source and Destination" task on page 17-82 for the VCAT circuit that you are creating.

Step 10 In the Circuit Routing Preferences area (Figure 6-12 on page 6-49), uncheck **Route Automatically**.

Step 11 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.

Step 12 If you want to set preferences for individual members, complete the following in the Member Preferences area. To set identical preferences for all members, skip this step and continue with Step 13.

- Number—Choose a number 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—(Future use) Routes the member on a BLSR protection channel.

    Note Although ONS 15310-CLs and ONS 15310-MAs do not support BLSR, you can route an LCAS VCAT circuit over a BLSR network of ONS 15600s or ONS 15454s.

  - DRI—(Split routing only) Routes the member on a DRI 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—(Future use) Routes the member on a BLSR protection channel.
  - DRI—(Split routing only) Routes the member on a DRI circuit.
- Node-Diverse Path—(Split routing only) Available when Fully Protected is chosen.

Step 14 Click **Next**. If you chose Fully Protected, 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-C66 Provision a VCAT Circuit Route" task on page 17-83.

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 might take several minutes.

Step 18 When all the circuits are created, the main Circuits window appears. Verify that the circuits you created appear in the window.

Step 19 As needed, complete the "DLP-C190 Provision CE-100T-8 Card Ethernet Ports" task on page 18-89 and/or the "DLP-C191 Provision CE-100T-8 Card POS Ports" task on page 18-91.

Stop. You have completed this procedure.

NTP-C55 Create Overhead Circuits

Purpose	This procedure creates overhead circuits on an ONS network. Overhead circuits include DCC tunnels, orderwire, UDC circuits, and IP tunnels.
Tools/Equipment	None
Prerequisite Procedures	NTP-C36 Verify Network Turn-Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The ONS 15310-CL and ONS 15310-MA support pass-through orderwire circuits if the source and destination are on ONS 15454 node optical ports. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at a node on the network 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-C67 Create a DCC Tunnel" task on page 17-84.

Step 4 As needed, complete the "DLP-C68 Create a User Data Channel Circuit" task on page 17-85.

Step 5 As needed, complete the "DLP-C228 Provision Orderwire" task on page 19-27.

Step 6 As needed, complete the "DLP-C69 Create an IP-Encapsulated Tunnel" task on page 17-86.

Stop. You have completed this procedure.

NTP-C140 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-C36 Verify Network Turn-Up, page 6-4
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-C29 Log into CTC" task on page 17-44 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**.

Stop. You have completed this procedure.

NTP-C186 Configure CCAT/VCAT Circuit in Manual Mode

Purpose	This procedure configures a CCAT/VCAT circuit in MANUAL mode.
Tools/Equipment	None
Prerequisite Procedures	NTP-C36 Verify Network Turn-Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 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 Click the **Circuits** > **Circuits** tabs .

Step 4 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 44 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 the administrative state to apply to all of the member cross-connects in a VCAT circuit:
  - **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 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 member 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**—(LCAS 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. OOS-MA,OOG applies only 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.
- 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 is 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.
- 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 15310-CL and Cisco ONS 15310-MA Reference Manual*.
- Num. of members—Choose the number of members from the drop-down list. For information about the number of members supported for each card, refer to the “Circuits and Tunnels” chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA 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:
  - None—Provides no protection. A failure on one member causes the entire VCAT circuit to fail. For CE-100T-8, 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 ML-100T-8 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 provides interoperability with the ONS 15454 ML-Series cards. SW-LCAS uses legacy SONET failure indicators like AIS-P and RDI-P to detect member failure. You cannot add or delete members from a VCAT circuit with SW-LCAS protection.

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 noninvolved 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 and ML-100T-8 cards that do not need to interoperate with the ONS 15454 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-C65 Provision a VCAT Circuit Source and Destination" task on page 17-82 for the VCAT circuit that you are creating.

Step 10 In the Circuit Routing Preferences area, uncheck **Route Automatically**.

Step 11 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.

Step 12 If you want to set preferences for individual members, complete the following in the Member Preferences area. To set identical preferences for all members, skip this step and continue with Step 13.

- Number—Choose a number 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—(Future use) Routes the member on a BLSR protection channel.

    Note Although ONS 15310-CLs and ONS 15310-MAs do not support BLSR, you can route an LCAS VCAT circuit over a BLSR network of ONS 15600s or ONS 15454s.

  - DRI—(Split routing only) Routes the member on a DRI 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—(Future use) Routes the member on a BLSR protection channel.
  - DRI—(Split routing only) Routes the member on a DRI circuit.
- Node-Diverse Path—(Split routing only) Available when Fully Protected is chosen.

Step 14 Click **Next**. If you chose Fully Protected, 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-C66 Provision a VCAT Circuit Route" task on page 17-83.

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 might take several minutes.

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.

CHAPTER 7

Manage Circuits

This chapter explains how to manage Cisco ONS 15310-CL and ONS 15310-MA electrical, optical, and Ethernet circuits. To create circuits, see Chapter 6, "Create Circuits and VT Tunnels."

Before You Begin

To clear any alarm or trouble conditions, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

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

1. NTP-C69 Locate and View Circuits, page 7-2—Complete as needed.
2. NTP-C70 View Cross-Connect Resource Usage, page 7-2—Complete as needed.
3. NTP-C71 Modify and Delete Circuits, page 7-3—Complete as needed to edit a circuit name; change the active and standby colors of spans; change signal fail thresholds, signal degrade thresholds, reversion time, and payload defect indication path (PDI-P) settings for path protection circuits; or add or delete a virtual concatenated (VCAT) member.
4. NTP-C72 Modify and Delete Overhead Circuits and Server Trails, page 7-4—Complete as needed to change a tunnel type, repair an IP circuit, or delete overhead circuits and server trails.
5. NTP-C73 Create a Monitor Circuit, page 7-4—Complete as needed to monitor traffic on primary bidirectional circuits.
6. NTP-C144 Create a J0 Section Trace, page 7-5—Complete as needed to monitor interruptions or changes to circuit traffic.
7. NTP-C74 Create a J1 Path Trace, page 7-7—Complete as needed to monitor interruptions or changes to circuit traffic.
8. NTP-C75 Create a J2 Path Trace, page 7-7—Complete as needed to monitor interruptions or changes to circuit traffic on the CE-100T-8 card.
9. NTP-C129 Bridge and Roll Traffic, page 7-10—Complete as needed to reroute live traffic without interrupting service.
10. NTP-C76 Reconfigure Circuits, page 7-11—Complete as needed to reconfigure (rebuild) circuits.
11. NTP-C77 Merge Circuits, page 7-11—Complete as needed to merge two circuits into a master circuit.

NTP-C69 Locate and View Circuits

Purpose	This procedure allows you to locate and view ONS 15310-CL and ONS 15310-MA circuits. You can also export circuit data from the Circuits and Edit Circuits windows.
Tools/Equipment	None
Prerequisite Procedures	Circuit creation procedures 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-C29 Log into CTC" task on page 17-44 on a node in the network where you want to view the circuits. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-C107 View Circuit Information" task on page 18-12.

Step 3 As needed, complete the "DLP-C78 Search for Circuits" task on page 17-95.

Step 4 As needed, complete the "DLP-C109 Filter the Display of Circuits" task on page 18-14.

Step 5 As needed, complete the "DLP-C110 View Circuits on a Span" task on page 18-16.

Step 6 As needed, complete the "DLP-C223 Export CTC Data" task on page 19-20.

Stop. You have completed this procedure.

NTP-C70 View Cross-Connect Resource Usage

Purpose	This procedure displays the percentage of cross-connect resources used by circuits that traverse or terminate at an ONS 15310-CL or ONS 15310-MA.
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-C29 Log into CTC" task on page 17-44 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 section of the Resources Usage tab, view the following information:

- STS-1 Matrix—Provides the percent of the cross-connect synchronous transport signal (STS) resources that are used. For the 15310-CL-CTX, 48 STS-1 paths are available. For the CTX2500, 216 STS-1 paths are available.

- VT1.5 Matrix Ports—Provides the percent of the cross-connect virtual tributary (VT) matrix ports that are used. Each port is one STS in size, and each can transport 28 VT1.5s. For the 15310-CL-CTX, 24 VT matrix ports are available. For the CTX2500, 96 VT matrix ports are available.
- VT1.5 Matrix—Provides the percent of the VT matrix resources that are used. For the 15310-CL-CTX, there are 672 available, which is the number of VT matrix ports (24) multiplied by the number of VT1.5s in an STS (28). For the CTX2500, there are 2128 available.

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 VT tunnel name if the VT port is on a VT tunnel origination or termination port.
- % Used—Shows the percent of the matrix port that is used. Each matrix port can carry 28 VT1.5s, so for example, if one STS carries seven VT1.5 circuits, the matrix port will be 25% used.
- Usage—Shows the port usage. For example, if one STS carries seven VT1.5 circuits, the matrix port will show 7 of 28 are used.

Stop. You have completed this procedure.

NTP-C71 Modify and Delete Circuits

Purpose	This procedure modifies and deletes ONS 15310-CL and ONS 15310-MA circuits.
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-C29 Log into CTC" task on page 17-44 at a node on the network containing the circuit you want to modify. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-C111 Change a Circuit Service State" task on page 18-17.

Step 3 As needed, complete the "DLP-C112 Edit a Circuit Name" task on page 18-18.

Step 4 As needed, complete the "DLP-C113 Change Active and Standby Span Color" task on page 18-19.

Step 5 As needed, complete the "DLP-C114 Edit Path Protection Circuit Path Selectors" task on page 18-20.

Step 6 As needed, complete the "DLP-C241 Edit Path Protection Dual-Ring Interconnect Circuit Hold-Off Timer" task on page 19-53.

Step 7 As needed, complete the "DLP-C115 Delete Circuits" task on page 18-21.

Step 8 As needed, complete the "DLP-C180 Change a VCAT Member Service State" task on page 18-73.

Step 9 As needed, complete the "DLP-C116 Add a Member to a VCAT Circuit" task on page 18-22.

Step 10 As needed, complete the "DLP-C117 Delete a Member from a VCAT Circuit" task on page 18-26.

Stop. You have completed this procedure.

NTP-C72 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-C29 Log into CTC" task on page 17-44 at a node on the network containing the circuit you want to modify. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-C118 Change Tunnel Type" task on page 18-27.

Step 3 As needed, complete the "DLP-C119 Repair an IP Tunnel" task on page 18-28.

Step 4 As needed, complete the "DLP-C120 Delete Overhead Circuits" task on page 18-28.

Step 5 As needed, complete the "DLP-C232 Delete a Server Trail" task on page 19-31.

Stop. You have completed this procedure.

NTP-C73 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-C29 Log into CTC" task on page 17-44 on an ONS 15310-CL or ONS 15310-MA node on the network where you want to 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**.

Note If the circuit name is longer than 44 characters, it appends "_MON" after truncating the circuit name to 40 characters.

Step 6 In the Edit Circuit window, click the **Monitors** tab.

The Monitors tab provides ports that you can use to monitor the circuit. The Monitor tab is only available when the circuit has a DISCOVERED status.

Step 7 In the Monitors tab, choose the monitor source port. The monitor circuit displays traffic coming into the node at the port you choose.

Step 8 Click **Create Monitor Circuit**.

Step 9 In the Circuit Destination section of the Circuit Creation wizard, choose the destination node, slot, port, STS, VT, or DS1 for the monitored circuit.

Step 10 Click **Next**.

Step 11 In the Circuit Routing Preferences area, review the monitor circuit information.

Step 12 Click **Finish**.

Step 13 In the Edit Circuit window, click **Close**. The new monitor circuit appears on the Circuits tab.

Stop. You have completed this procedure.

NTP-C144 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	An ONS 15310-MA CTX2500, DS1-84/DS3-3, or DS1-28/DS3-EC1-3 card must be installed. J0 section trace applies to optical and EC-1 ports.
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-C29 Log into CTC" task on page 17-44 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 CTX2500, DS1-84/DS3-3, or DS1-28/DS3-EC1-3 card.

Step 3 Click the **Provisioning > EC1** or **Optical > 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 15310-CL and Cisco ONS 15310-MA 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-C74 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 15310-CL and ONS 15310-MA cards capable of transmitting and/or receiving path trace must be installed. See Table 18-6 on page 18-29 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

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 on an ONS 15310-CL or ONS 15310-MA node on the network where you will create the path trace. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-C121 Provision Path Trace on Circuit Source and Destination Ports" task on page 18-29.

Step 3 As needed, complete the "DLP-C122 Provision Path Trace on OC-N Ports" task on page 18-32.

Stop. You have completed this procedure.

NTP-C75 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	ONS 15310-CL and ONS 15310-MA cards capable of transmitting and/or receiving path trace must be installed. See Table 18-6 on page 18-29 for a list of cards.
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 You cannot create a J2 path trace on a TL1-like circuit.

Note This procedure assumes 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-C29 Log into CTC" task on page 17-44 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. On 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 Alarm Indication Signal 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 Alarm Indication Signal 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 window 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-C129 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 "NTP-C141 Create Optical Protection Groups for the ONS 15310-CL" procedure on page 4-12. • When a roll involves two circuits, a data communications channel (DCC) connection must exist. See the "DLP-C52 Provision Section DCC Terminations" task on page 17-68. • Use the "NTP-C69 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 15310-CL and Cisco ONS 15310-MA 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.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the ONS 15310-CL or ONS 15310-MA circuit source node. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-C183 Roll the Source or Destination of One Optical Circuit" task on page 18-75.

Step 3 As needed, complete the "DLP-C184 Roll One Cross-Connect from an Optical Circuit to a Second Optical Circuit" task on page 18-78.

Step 4 As needed, complete the "DLP-C185 Roll Two Cross-Connects on One Optical Circuit Using Automatic Routing" task on page 18-80 or the "DLP-C186 Roll Two Cross-Connects on One Optical Circuit Using Manual Routing" task on page 18-84.

Step 5 As needed, complete the "DLP-C187 Roll Two Cross-Connects from One Optical Circuit to a Second Optical Circuit" task on page 18-86.

Step 6 As needed, complete the "DLP-C189 Cancel a Roll" task on page 18-88.

Step 7 As needed, complete the "DLP-C188 Delete a Roll" task on page 18-88. Use caution when selecting this option. Delete a roll only if it cannot be completed or cancelled. Circuits may have a PARTIAL status when this option is selected.

Stop. You have completed this procedure.

NTP-C76 Reconfigure Circuits

Purpose	This procedure rebuilds circuits, which may be necessary when a large number of circuits are in the PARTIAL status.
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-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 Click the **Circuits** tab.

Step 3 Choose 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-C77 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	Circuits must exist on the network. See Chapter 6, "Create Circuits and VT Tunnels" for circuit creation procedures.
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44. 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.

CHAPTER 8

Monitor Performance

Performance monitoring (PM) parameters are used by service providers to gather, store, and report performance data for early detection of problems. For more PM information, details, and definitions, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*. This chapter explains how to enable and view PM statistics for the Cisco ONS 15310-CL and Cisco ONS 15310-MA.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* as necessary.

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

1. NTP-C64 Change the PM Display, page 8-2—Complete as needed.
2. NTP-C65 Monitor Electrical Performance, page 8-3—Complete as needed.
3. NTP-C66 Monitor Optical Performance, page 8-4—Complete as needed
4. NTP-C67 Monitor Ethernet Performance, page 8-5—Complete as needed.
5. NTP-C68 Create or Delete Ethernet RMON Thresholds, page 8-5—Complete as needed.
6. NTP-C175 Enable or Disable AutoPM, page 8-6—Complete as needed.

Note For additional information regarding PM parameters, refer to Telcordia’s GR-1230-CORE, GR-499-CORE, and GR-253-CORE documents and GR-820-CORE document titled Generic Digital Transmission Surveillance, and in the ANSI T1.231 document entitled *Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*.

NTP-C64 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 10, "Change Port Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node that you want to monitor. If you are already logged in, continue with Step 2.

Step 2 As needed, use the following tasks to change the display of PM counts:

- DLP-C89 Refresh PM Counts for a Different Port, page 17-109
- DLP-C90 Refresh Electrical or Optical PM Counts at Fifteen-Minute Intervals, page 17-110
- DLP-C91 Refresh Electrical or Optical PM Counts at One-Day Intervals, page 17-111
- DLP-C92 Monitor Near-End PM Counts, page 17-112
- DLP-C93 Monitor Far-End PM Counts, page 17-112
- DLP-C94 Reset Current PM Counts, page 17-113
- DLP-C95 Clear Selected PM Counts, page 17-114
- DLP-C264 Clear All PM Thresholds, page 19-79
- DLP-C96 Set Auto Refresh Interval for Displayed PM Counts, page 17-115
- DLP-C97 Monitor PM Counts for Selected Signal Types, page 17-116

Stop. You have completed this procedure.

NTP-C65 Monitor Electrical Performance

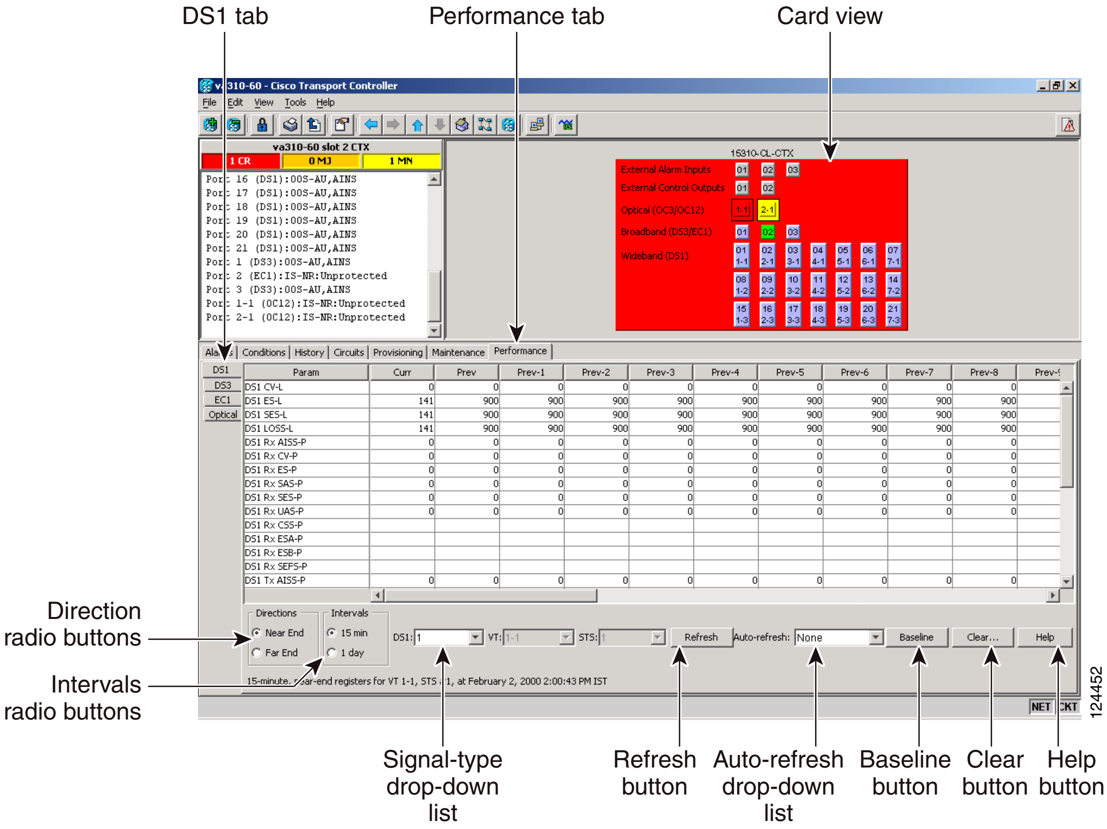
Purpose	This procedure allows you to view near-end or far-end performance on electrical ports at specified time intervals to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, “Create Circuits and VT Tunnels” and Chapter 10, “Change Port Settings.”
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the “DLP-C29 Log into CTC” task on page 17-44 at the node you want to monitor. If you are already logged in, continue to Step 2.

Step 2 In node view, double-click the 15310-CL-CTX card or an ONS 15310-MA electrical card. The 15310-MA electrical cards are the DS1-28/DS3-EC1-3 and the DS1-84/DS3-EC1-3. The card view appears.

Step 3 Click the **Performance** tab (Figure 8-1).

Figure 8-1 Viewing Electrical Performance Monitoring Information



```
Por  16 (DS1):OOS-AU,AINS
Por  17 (DS1):OOS-AU,AINS
Por  18 (DS1):OOS-AU,AINS
Por  19 (DS1):OOS-AU,AINS
Por  20 (DS1):OOS-AU,AINS
Por  21 (DS1):OOS-AU,AINS
Por  1 (DS3):OOS-AU,AINS
Por  2 (EC1):IS-NR:Unprotected
Por  3 (DS3):OOS-AU,AINS
Por  1-1 (OC12):IS-NR:Unprotected
Por  2-1 (OC12):IS-NR:Unprotected
```

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-
DS1 CV-L	0	0	0	0	0	0	0	0	0	0	
DS1 ES-L	141	900	900	900	900	900	900	900	900	900	
DS1 SES-L	141	900	900	900	900	900	900	900	900	900	
DS1 LOSS-L	141	900	900	900	900	900	900	900	900	900	
DS1 Rx AISS-P	0	0	0	0	0	0	0	0	0	0	
DS1 Rx CV-P	0	0	0	0	0	0	0	0	0	0	
DS1 Rx ES-P	0	0	0	0	0	0	0	0	0	0	
DS1 Rx SAS-P	0	0	0	0	0	0	0	0	0	0	
DS1 Rx SES-P	0	0	0	0	0	0	0	0	0	0	
DS1 Rx UAS-P	0	0	0	0	0	0	0	0	0	0	
DS1 Rx CSS-P											
DS1 Rx ESA-P											
DS1 Rx ESB-P											
DS1 Rx SEFS-P											
DS1 Tx AISS-P	0	0	0	0	0	0	0	0	0	0	

Directions: ● Near End ○ Far End

Intervals: ● 15 min ○ 1 day

DS1: 1 VT: 1-1 STS: 1 Auto-refresh: None

15-minute. ear-end registers for VT 1-1, STS 1, at February 2, 2000 2:00:43 PM IST

Step 4 Click the **DS1**, **DS3**,or **EC1** tabs to view the PM parameters.

The PM parameter names appear on the left side of the window in the Param column. The PM values appear on the right side of the window in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-C64 Change the PM Display" procedure on page 8-2.

Stop. You have completed this procedure.

NTP-C66 Monitor Optical Performance

Purpose	This procedure allows you to view near-end or far-end performance on an optical card and port at specified time intervals 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 Port Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node you want to monitor. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-C98 Enable Pointer Justification Count Performance Monitoring" task on page 17-117 if you need to monitor clock synchronization.

Step 3 Complete the "DLP-C99 Enable Intermediate-Path Performance Monitoring" task on page 17-119 if you need to monitor large amounts of synchronous transport signal (STS) traffic through intermediate nodes.

Step 4 Complete the "DLP-C100 View Optical OC-N PM Parameters" task on page 18-1 as needed.

Note To refresh, reset, or clear PM counts, see the "NTP-C64 Change the PM Display" procedure on page 8-2.

Stop. You have completed this procedure.

NTP-C67 Monitor Ethernet Performance

Purpose	This procedure allows you to view node transmit and receive performance on an Ethernet card and port at specified time intervals 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 Port Settings.”
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Complete the “DLP-C29 Log into CTC” task on page 17-44 at the node you want to monitor. If you are already logged in, continue with Step 2.

Step 2 Complete the “DLP-C101 View Ether Ports and POS Ports Statistics PM Parameters” task on page 18-2 as needed.

Step 3 Complete the “DLP-C102 View Ether Ports and POS Ports Utilization PM Parameters” task on page 18-4 as needed.

Step 4 As needed, use the “DLP-C103 Refresh Ethernet PM Counts at a Different Time Interval” task on page 18-5 to change the display of Ethernet utilization PM counts.

Step 5 Complete the “DLP-C104 View Ether Ports and POS Ports History PM Parameters” task on page 18-5 as needed.

Stop. You have completed this procedure.

NTP-C68 Create or Delete Ethernet RMON Thresholds

Purpose	This procedure creates or deletes remote monitoring (RMON) Ethernet thresholds for the ONS 15310-CL and ONS 15310-MA.
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-C29 Log into CTC” task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 Perform any of the following tasks as needed:

- DLP-C105 Create Ethernet RMON Alarm Thresholds, page 18-6

- DLP-C106 Delete Ethernet RMON Alarm Thresholds, page 18-11

Stop. You have completed this procedure.

NTP-C175 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-C29 Log into CTC" task on page 17-44. 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 9

Manage Alarms

This chapter explains how to view and manage the alarms and conditions on a Cisco ONS 15310-CL and Cisco ONS 15310-MA.

Cisco Transport Controller (CTC) detects and reports SONET alarms generated by the ONS 15310-CL, ONS 15310-MA, and the larger SONET network. You can use CTC to monitor and manage alarms at a card, node, or network level.

Before You Begin

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

1. NTP-C56 Document Existing Provisioning, page 9-2—Complete this procedure as needed to print and export node information.
2. NTP-C57 View Alarms, History, Events, and Conditions, page 9-2—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-C58 Delete Cleared Alarms from Display, page 9-3—Complete this procedure as needed to delete cleared alarm information that is no longer needed.
4. NTP-C59 View Alarm-Affected Circuits, page 9-5—Complete this procedure as needed to find circuits that are affected by a particular alarm or condition.
5. NTP-C60 Create, Download, and Assign Alarm Severity Profiles, page 9-6—Complete this procedure as needed to change the default severity for certain alarms; assign the new severities to a port, card, or node; and delete alarm profiles.
6. NTP-C61 Enable, Modify, or Disable Alarm Severity Filtering, page 9-7—Complete this procedure as needed to enable, disable, or modify alarm severity filtering in the Conditions, Alarms, or History screens; or you can enable, modify, and disable alarm severity filtering at the node or network level.
7. NTP-C62 Suppress Alarms or Discontinue Alarm Suppression, page 9-7—Complete this procedure as needed to suppress reported alarms at the port, card, or node level and disable the suppress command to resume normal alarm reporting.
8. NTP-C63 Provision External Alarms and Controls, page 9-8—Complete this procedure as needed to provision external alarms and controls on the 15310-CL-CTX card (ONS 15310-CL) or CTX2500 card (ONS 15310-MA).

NTP-C56 Document Existing Provisioning

Purpose	This procedure prints card, node, or network CTC information in graphical or tabular form on a Windows-provisioned printer. It also exports card, node, or network information as delineated text files to other applications. This procedure is useful for network record keeping and troubleshooting.
Tools/Equipment	Printer connected to the CTC computer by a direct or network connection
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node that has the information you want to record or save. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-C222 Print CTC Data" task on page 19-18.

Step 3 As needed, complete the "DLP-C223 Export CTC Data" task on page 19-20.

Stop. You have completed this procedure.

NTP-C57 View Alarms, History, Events, and Conditions

Purpose	This procedure views current or historical alarms and conditions for a card, a node, or network. The 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 or higher

Step 1 Log into the node that contains the alarms you want to view. See the "DLP-C29 Log into CTC" task on page 17-44 for instructions. If you are already logged in, proceed to Step 2.

Step 2 Complete the "DLP-C72 View Alarms" task on page 17-87 as needed.

Step 3 Complete the "DLP-C73 View Alarm or Event History" task on page 17-90 as needed.

Step 4 Complete the "DLP-C74 Change the Maximum Number of Session Entries for Alarm History" task on page 17-92 as needed.

Step 5 Complete the "DLP-C75 Display Alarms and Conditions Using Time Zone" task on page 17-93 as needed.

Step 6 Complete the "DLP-C76 Synchronize Alarms" task on page 17-93 as needed.

Step 7 Complete the "DLP-C77 View Conditions" task on page 17-94 as needed.

Stop. You have completed this procedure.

NTP-C58 Delete Cleared Alarms from Display

Purpose	This procedure deletes Cleared (C) status alarms from the alarms window. The procedure can be used to delete 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 Log into a node where you want to delete alarms. See the "DLP-C29 Log into CTC" task on page 17-44 for instructions. If you are already logged in, continue with Step 2.

Step 2 To delete cleared node-level alarms:

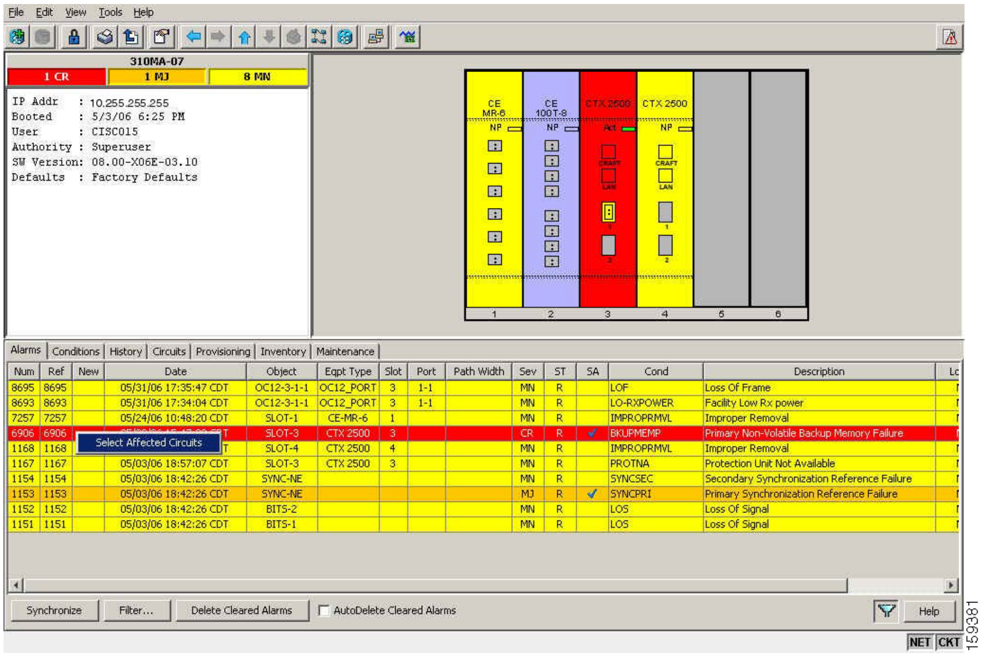
a. In node view, click the **Alarms** tab.

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 15310-CL alarms from the Alarms display. The rows of cleared alarms turn white and have a C in their status (ST) column (Figure 9-1). The ONS 15310-MA Conditions window is shown. The ONS 15310-CL Conditions window is very similar to it.

Figure 9-1 ONS 15310-MA Node View Conditions Window



```
IP Addr   : 10.255.255.255
Booted    : 5/3/06 6:25 PM
User      : CISCO15
Authority : Superuser
SW Version: 08.00-X06E-03.10
Defaults  : Factory Defaults
```

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Path Width	Sev	ST	SA	Cond	Description
8695	8695		05/31/06 17:35:47 CDT	OC12-3-1-1	OC12_PORT	3	1-1		MN	R		LOF	Loss Of Frame
8693	8693		05/31/06 17:34:04 CDT	OC12-3-1-1	OC12_PORT	3	1-1		MN	R		LO-RXPOWER	Facility Low Rx power
7257	7257		05/24/06 10:48:20 CDT	SLOT-1	CE-MR-6	1			MN	R		IMPROPRMVL	Improper Removal
6906	6906		[illegible]	SLOT-3	CTX 2500	3			CR	R	✓	BKUPMEMP	Primary Non-Volatile Backup Memory Failure
1168	1168		[illegible]	SLOT-4	CTX 2500	4			MN	R		IMPROPRMVL	Improper Removal
1167	1167		05/03/06 18:57:07 CDT	SLOT-3	CTX 2500	3			MN	R		PROTNA	Protection Unit Not Available
1154	1154		05/03/06 18:42:26 CDT	SYNC-NE					MN	R		SYNCSEC	Secondary Synchronization Reference Failure
1153	1153		05/03/06 18:42:26 CDT	SYNC-NE					MJ	R	✓	SYNCPRI	Primary Synchronization Reference Failure
1152	1152		05/03/06 18:42:26 CDT	BITS-2					MN	R		LOS	Loss Of Signal
1151	1151		05/03/06 18:42:26 CDT	BITS-1					MN	R		LOS	Loss Of Signal

Step 3 To delete cleared card-level alarms:

a. In 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 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.

Step 4 To delete cleared network-level alarms:

a. From the **View menu choose Go to Network View**.

b. Click the **Alarms** tab and then 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 (CL) severity. The alarm can be removed by clicking the Delete Cleared Alarms button.

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-C59 View Alarm-Affected Circuits

Purpose	Use this procedure to view all circuits, if any, affected by an alarm or condition.
Tools/Equipment	None
Prerequisite Procedures	NTP-C57 View Alarms, History, Events, and Conditions, page 9-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

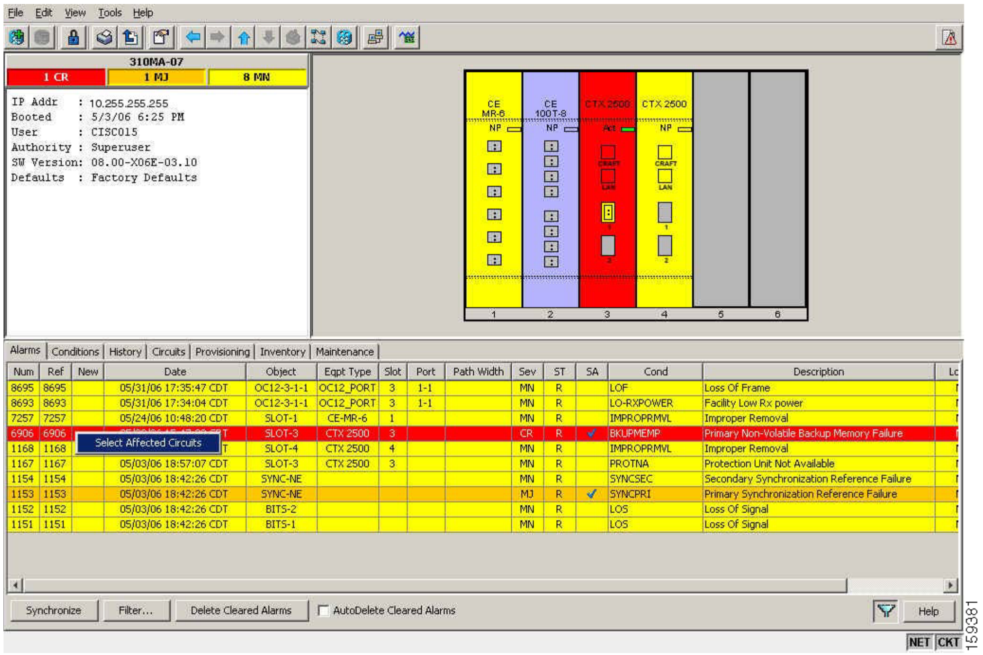
Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

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 9-2). The ONS 15310-MA Conditions window is shown. The ONS 15310-CL Conditions window is very similar.

Figure 9-2 ONS 15310-MA Select Affected Circuits Option



```
IP Addr   : 10.255.255.255
Booted    : 5/3/06 6:25 PM
User      : CISCO15
Authority : Superuser
SW Version: 08.00-X06E-03.10
Defaults  : Factory Defaults
```

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Path Width	Sev	ST	SA	Cond	Description
8695	8695		05/31/06 17:35:47 CDT	OC12-3-1-1	OC12_PORT	3	1-1		MN	R		LOF	Loss Of Frame
8693	8693		05/31/06 17:34:04 CDT	OC12-3-1-1	OC12_PORT	3	1-1		MN	R		LO-RXPOWER	Facility Low Rx power
7257	7257		05/24/06 10:48:20 CDT	SLOT-1	CE-MR-6	1			MN	R		IMPROPRMVL	Improper Removal
6906	6906		[illegible]	SLOT-3	CTX 2500	3			CR	R	✓	BKUPMEMP	Primary Non-Volatile Backup Memory Failure
1168	1168		[illegible]	SLOT-4	CTX 2500	4			MN	R		IMPROPRMVL	Improper Removal
1167	1167		05/03/06 18:57:07 CDT	SLOT-3	CTX 2500	3			MN	R		PROTNA	Protection Unit Not Available
1154	1154		05/03/06 18:42:26 CDT	SYNC-NE					MN	R		SYNCSEC	Secondary Synchronization Reference Failure
1153	1153		05/03/06 18:42:26 CDT	SYNC-NE					MJ	R	✓	SYNCPRI	Primary Synchronization Reference Failure
1152	1152		05/03/06 18:42:26 CDT	BITS-2					MN	R		LOS	Loss Of Signal
1151	1151		05/03/06 18:42:26 CDT	BITS-1					MN	R		LOS	Loss Of Signal

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-C78 Search for Circuits" task on page 17-95.

Stop. You have completed this procedure.

NTP-C60 Create, Download, and Assign Alarm Severity Profiles

Purpose	This procedure creates a customized alarm profile at the network, node, or card level; assigns custom severities individually to a port, card, or node; and deletes 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-C29 Log into CTC" task on page 17-44 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-C79 Create a Cloned Alarm Severity Profile" task on page 17-96. This task clones a current alarm profile and then renames and customizes it.

Step 3 Complete the "DLP-C80 Download an Alarm Severity Profile" task on page 17-99. 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-C81 Apply Alarm Profiles to Ports" task on page 17-100 or the "DLP-C82 Apply Alarm Profiles to Cards and Nodes" task on page 17-101.

Step 5 As needed, complete the "DLP-C83 Delete Alarm Severity Profiles" task on page 17-103.

Stop. You have completed this procedure.

NTP-C61 Enable, Modify, or Disable Alarm Severity Filtering

Purpose	This procedure starts, changes, or stops 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-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 As necessary, complete the "DLP-C84 Enable Alarm Filtering" task on page 17-104 to enable alarm filtering at the card, node, and network views for all nodes in the network. Alarm filtering can be enabled for alarms or conditions.

Step 3 As necessary, complete the "DLP-C85 Modify Alarm and Condition Filtering Parameters" task on page 17-105 to modify the alarm filtering for network nodes to show or hide particular alarms or conditions.

Step 4 As necessary, complete the "DLP-C88 Disable Alarm Filtering" task on page 17-109 to disable alarm profile filtering for all network nodes.

Stop. You have completed this procedure.

NTP-C62 Suppress Alarms or Discontinue Alarm Suppression

Purpose	This procedure prevents 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 Alarms or History display. This procedure also resumes 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-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-C86 Suppress Alarm Reporting" task on page 17-107 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-C87 Discontinue Alarm Suppression" task on page 17-108 to discontinue alarm suppression and resume normal alarm reporting.

Stop. You have completed this procedure.

NTP-C63 Provision External Alarms and Controls

Purpose	Use this procedure to create external (environmental) alarms and controls on the 15310-CL and ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C9 Install External Alarm Cables on the ONS 15310-CL, page 17-12
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

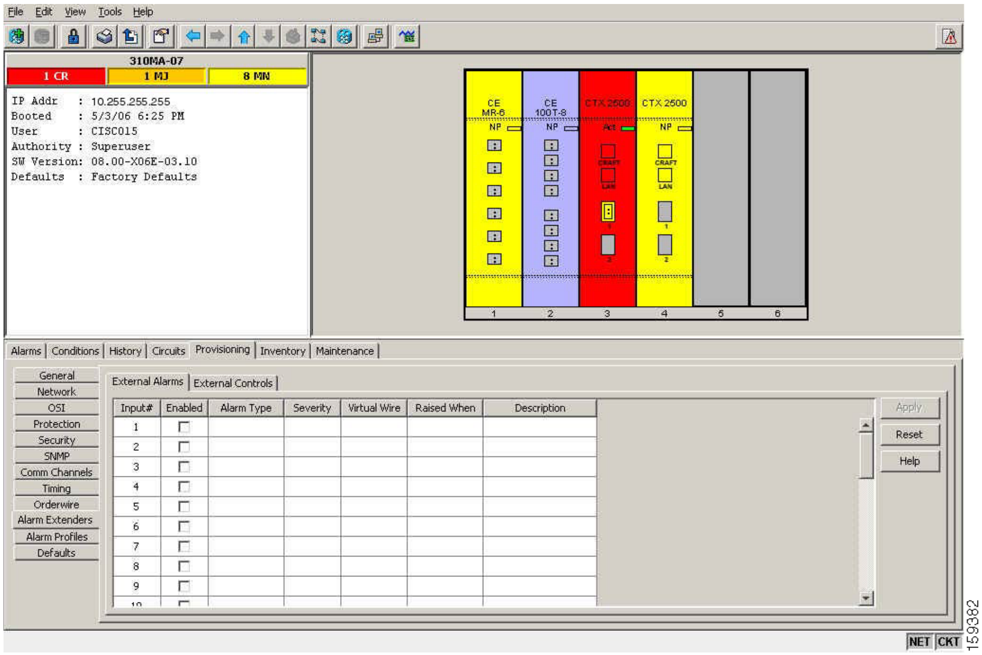
Note External alarm physical connections are made using the ALARM port on the front of the ONS 15310-CL and ONS 15310-MA. The alarms and controls are provisioned using the 15310-CL-CTX and CTX2500 card view. For information about the 15310-CL-CTX and CTX2500 external alarms and controls, virtual wire, and orderwire, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 1 In the node view, double-click the active 15310-CL-CTX or CTX2500 card. The card view appears.

Step 2 If you are provisioning external alarms, click the **Provisioning > External Alarms** tabs (Figure 9-3). (The view is similar for either platform.) If you are not provisioning external alarms, continue with Step 7.

Step 3 To add User Defined Alarm Types, complete the"DLP-C277 Create User Defined Alarm Types" task on page 19-92. If you are not adding User Defined Alarm Types continue with Step 4

Figure 9-3 External Alarms for the ONS 15310-MA



```
IP Addr    : 10.255.255.255
Booted     : 5/3/06 6:25 PM
User       : CISC015
Authority  : Superuser
SW Version: 08.00-X06E-03.10
Defaults   : Factory Defaults
```

Input#	Enabled	Alarm Type	Severity	Virtual Wire	Raised When	Description
1	☐					
2	☐					
3	☐					
4	☐					
5	☐					
6	☐					
7	☐					
8	☐					
9	☐					
10	☐					

Step 4 Complete the following fields for each external device wired to the controller card:

- Enabled—Check this check box to activate the fields for the alarm input number.
- Alarm Type—Choose an option from the **Alarm Type** drop-down list.
- Severity—Choose an option from the **Severity** drop-down list.

  The severity determines the severity the alarm has in the Alarms and History tabs and determines whether the LEDs are activated. Critical (CR), Major (MJ), and Minor (MN) alarms activate the 15310-CL-CTX and CTX2500 LEDs. Not-Alarmed (NA) and Not-Reported (NR) do not activate LEDs, but do report the information in CTC.
- Virtual Wire—Choose an option to assign the external device to a virtual wire. Otherwise, do not change the None default. For information about the virtual wire, see the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.
- Raised When—Choose the condition (open or closed) that triggers the alarm.
- Description—A default description is provided; enter a different description if needed.

Step 5 To provision up to six virtual wire inputs for external devices, complete Step 4 for each additional device.

Step 6 Click **Apply**.

Step 7 If you are provisioning external control outputs for external devices connected to the controller card, click the **External Controls** tab (Figure 9-3).

Step 8 Complete the following fields for each external control wired to the controller card:

- Enabled—Check this check box to activate the Control Type, Trigger Type, and Description columns for the alarm input number.
- Control Type—Choose an option: 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 9 To provision a second external control, complete Step 8 for the additional device.

Step 10 Click **Apply**.

Stop. You have completed this procedure.

CHAPTER 10

Change Port Settings

This chapter explains how to change transmission settings on ports in a Cisco ONS 15310-CL or Cisco ONS 15310-MA.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* as necessary.

⚠ **Caution** Changing card or port settings can be service affecting. You should make all changes during a scheduled maintenance window.

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

1. NTP-C86 Modify Line Settings and PM Parameter Thresholds for Electrical Ports, page 10-2—Complete as needed.
2. NTP-C87 Modify Line Settings and PM Parameter Thresholds for Optical Ports, page 10-2—Complete as needed.
3. NTP-C130 Manage Pluggable Port Modules, page 10-3—Complete this procedure to provision, change, or delete pluggable port modules (PPMs), which provide OC-3 or OC-12 line rates for ONS 15310-CL and ONS 15310-MA optical ports.
4. NTP-C92 Change Card or PPM Service State, page 10-4—Complete as needed.
5. NTP-C172 Provision the Soak Timer for an ML-100T-8 Card, page 10-4—Complete as needed.

NTP-C86 Modify Line Settings and PM Parameter Thresholds for Electrical Ports

Purpose	This procedure changes the line and threshold settings for electrical ports.
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-C29 Log into CTC" task on page 17-44 at the node where you want to change the port settings.

Step 2 According to site practice, complete the "NTP-C102 Back Up the Database" procedure on page 15-2 to preserve the existing database.

Step 3 Perform any of the following tasks as needed:

- DLP-C233 Change Line and Threshold Settings for DS-1 Ports, page 19-32
- DLP-C236 Change Line and Threshold Settings for DS-3 Ports, page 19-39
- DLP-C237 Change Line and Threshold Settings for the EC-1 Ports, page 19-42

Step 4 When you have finished changing the port settings, complete the "NTP-C102 Back Up the Database" procedure on page 15-2 according to site practice.

Stop. You have completed this procedure.

NTP-C87 Modify Line Settings and PM Parameter Thresholds for Optical Ports

Purpose	This procedure changes the line and threshold settings for the optical ports.
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-C29 Log into CTC" task on page 17-44 at the node where you want to change the port settings. If you are already logged in, continue with Step 2.

Step 2 According to site practice, complete the "NTP-C102 Back Up the Database" procedure on page 15-2 to preserve the existing database.

Step 3 Perform any of the following tasks as needed:

- DLP-C238 Change Optical Port Line Settings, page 19-46

- DLP-C239 Change Optical Port SONET Thresholds Settings, page 19-50
- DLP-C224 Change Optics Thresholds Settings for Optical Ports, page 19-22

Note To modify settings on the SONET STS tab, see the "DLP-C99 Enable Intermediate-Path Performance Monitoring" task on page 17-119.

Step 4 According to site practice, complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Stop. You have completed this procedure.

NTP-C130 Manage Pluggable Port Modules

Purpose	This procedure provisions, changes, and deletes Small Form-factor Pluggables (SFPs), which are known as pluggable port modules (PPMs) in Cisco Transport Controller (CTC). OC-3, OC-12, and multirate (OC-3/OC-12) PPMs are compatible with the ONS 15310-CL and ONS 15310-MA. OC-48 PPMs are compatible with the ONS 15310-MA only. Single-rate PPMs do not require provisioning or changing.
Tools/Equipment	None
Prerequisite Procedures	DLP-C16 Install SFP Connectors, page 17-22 or NTP-C9 Preprovision an SFP Slot, page 1-14
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node where you want to manage PPMs.

Step 2 Click the **Alarms** tab:

a. Verify that the alarm filter is not turned on. See the "DLP-C88 Disable Alarm Filtering" task on page 17-109 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 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

c. Complete the "DLP-C223 Export CTC Data" task on page 19-20 to export alarm and condition information.

Step 3 As needed, complete the "DLP-C192 Provision a Multirate Pluggable Port Module" task on page 18-92. If you preprovisioned a multirate SFP, skip this task and continue with Step 4.

Step 4 As needed, complete the "DLP-C193 Provision the Optical Line Rate" task on page 18-92 to assign an OC-3 or OC-12 line rate.

Step 5 As needed, complete the "DLP-C194 Change the Optical Line Rate" task on page 18-93 to change the line rate on a multirate PPM.

Step 6 As needed, complete the "DLP-C195 Delete Pluggable Port Modules" task on page 18-94.

Step 7 **Stop. You have completed this procedure.**

NTP-C92 Change Card or PPM Service State

Purpose	This procedure changes the card or port service state, which is an autonomously generated state that gives the overall condition of the port.
Tools/Equipment	None
Prerequisite Procedures	Chapter 1, "Install the Cisco ONS 15310-CL" Chapter 2, "Install the Cisco ONS 15310-MA"
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note On the ONS 15310-CL and ONS 15310-MA, the pluggable-port module (PPM) is equivalent to an optical port.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node where you want to change card or PPM service state.

Step 2 Click the **Inventory** tab.

Step 3 Click **Admin State** for the card or PPM that you want to change, and choose an administrative state from the drop-down list: **IS** or **OOS,MT**.

Step 4 Click **Apply**.

Step 5 If an error message appears indicating that the card or PPM service state cannot be changed from its current service 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 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Stop. You have completed this procedure.

NTP-C172 Provision the Soak Timer for an ML-100T-8 Card

Purpose	This procedure provisions the soak timer for ports on an ML-100T-8 card. The soak period is the amount of time that the ML-100T-8 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-C4 Install an Ethernet Card, page 1-7

Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node where you want to provision the soak timer for an ML-100T-8 card. If you are already logged in, continue with Step 2.

Step 2 In node view, double-click the ML-100T-8 card that you want to provision.

Step 3 Click the **Provisioning** tab.

Step 4 Click the **Ether Ports** or **POS Ports** subtabs and complete the following:

- PSAS—Check 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—Choose the desired soak time (in hours and minutes). 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.

Step 5 Click **Apply**.

Stop. You have completed this procedure.

CHAPTER 11

Change Node Settings

This chapter explains how to modify node provisioning for the Cisco ONS 15310-CL and Cisco ONS 15310-MA. To provision a new node, see Chapter 4, "Turn Up a Node." To change default card-level and node-level settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Before You Begin

Before performing the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* as necessary.

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

1. NTP-C78 Change Node Management Information, page 11-2—As needed, complete this procedure to change the node name, contact information, latitude, longitude, date, time, and login legal disclaimer.
2. NTP-C79 Change CTC Network Access, page 11-2—As needed, complete this procedure to change the IP address, default router, subnet mask, network configuration settings, and static routes.
3. NTP-C133 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-C80 Customize the CTC Network View, page 11-4—As needed, complete this procedure to customize the appearance of the network map, including specifying the default map, selecting your own map or image, consolidating links, and changing the background color.
5. NTP-C143 Modify or Delete Card Protection Settings, page 11-5—Complete as needed.
6. NTP-C82 Change Node Timing, page 11-6—Complete as needed.
7. NTP-C83 Modify Users and Change Security, page 11-6—As needed, complete this procedure to change the security policy on one or more nodes, change the node access and PM clearing privilege, grant superuser privileges to provisioning users, change the user password and security settings on one or more nodes, delete and logout users on one or more nodes, and configure the node for RADIUS authentication.
8. NTP-C84 Change SNMP Settings, page 11-7—Complete as needed.
9. NTP-C85 Modify or Delete Communications Channel Terminations and Provisionable Patchcords, page 11-8—Complete as needed.

NTP-C78 Change Node Management Information

Purpose	This procedure changes basic information about the node such as node name, date, time, contact information, and the login legal disclaimer.
Tools/Equipment	None
Prerequisite Procedures	NTP-C20 Set Up Name, Date, Time, and Contact Information, page 4-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Step 3 As needed, complete the "DLP-C123 Change the Node Name, Date, Time, and Contact Information" task on page 18-33.

Step 4 As needed, complete the "DLP-C124 Change the Login Legal Disclaimer" task on page 18-34.

Step 5 After confirming the changes, complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Stop. You have completed this procedure.

NTP-C79 Change CTC Network Access

Purpose	This procedure changes essential network information, including IP settings, static routes, and OSPF options.
Tools/Equipment	None
Prerequisite Procedures	NTP-C21 Set Up CTC Network Access, page 4-6
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Additional ONS 15310-CL and ONS 15310-MA networking information and procedures, including IP addressing examples, static route scenarios, Open Shortest Path First (OSPF) protocol, routing information protocol options, and Open System Interconnection (OSI) information, are provided in the "Management Network Connectivity" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Step 3 Perform any of the following tasks as needed:

- DLP-C125 Change IP Settings, page 18-35
- DLP-C40 Create a Static Route, page 17-55
- DLP-C126 Modify a Static Route, page 18-36
- DLP-C127 Delete a Static Route, page 18-36
- DLP-C128 Disable Open Shortest Path First Protocol, page 18-37
- DLP-C41 Set Up or Change Open Shortest Path First Protocol, page 17-56
- DLP-C47 Provision a Proxy Tunnel, page 17-64
- DLP-C129 Delete a Proxy Tunnel, page 18-37
- DLP-C48 Provision a Firewall Tunnel, page 17-65
- DLP-C130 Delete a Firewall Tunnel, page 18-38

Step 4 Complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Stop. You have completed this procedure.

NTP-C133 Modify OSI Provisioning

Purpose	This procedure modifies the ONS 15310-CL and ONS 15310-MA OSI parameters including the OSI routing mode, TARP, routers, subnets, and IP-over-CLNS tunnels.
Tools/Equipment	None
Prerequisite Procedures	NTP-C131 Provision OSI, page 4-16
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The "Management Network Connectivity" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* includes additional information about the ONS 15310-CL or ONS 15310-MA implementation of OSI.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Step 3 Perform any of the following tasks as needed:

- DLP-C201 Provision or Modify TARP Operating Parameters, page 19-2
- DLP-C202 Add a Static TID to NSAP Entry to the TARP Data Cache, page 19-4
- DLP-C203 Remove a Static TID to NSAP Entry from the TARP Data Cache, page 19-4
- DLP-C204 Add a TARP Manual Adjacency Table Entry, page 19-5
- DLP-C209 Remove a TARP Manual Adjacency Table Entry, page 19-9
- DLP-C235 Change the OSI Routing Mode, page 19-38

- DLP-C211 Edit the OSI Router Configuration, page 19-10
- DLP-C212 Edit the OSI Subnetwork Point of Attachment, page 19-10
- DLP-C208 Create an IP-Over-CLNS Tunnel, page 19-8
- DLP-C214 Delete an IP-Over-CLNS Tunnel, page 19-12

Step 4 Complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Stop. You have completed this procedure.

NTP-C80 Customize the CTC Network View

Purpose	This procedure modifies the CTC network view, including grouping nodes into domains for a clearer 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	Superuser

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 Complete the following tasks, as needed:

- DLP-C131 Change the Network View Background Color, page 18-38
- DLP-C132 Change to the Default Network View Background Map, page 18-39
- DLP-C133 Apply a Custom Network View Background Map, page 18-39
- DLP-C134 Create Domain Icons, page 18-40
- DLP-C135 Manage Domain Icons, page 18-41
- DLP-C136 Enable Dialog Box Do-Not-Display Option, page 18-42
- DLP-C229 Consolidate Links in Network View, page 19-28

Stop. You have completed this procedure.

NTP-C143 Modify or Delete Card Protection Settings

Purpose	This procedure modifies or deletes card protection settings.
Tools/Equipment	None
Prerequisite Procedures	NTP-C141 Create Optical Protection Groups for the ONS 15310-CL, page 4-12 or NTP-C142 Create Protection Groups for the ONS 15310-MA, 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-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Step 3 For the ONS 15310-CL, perform any of the following tasks as needed:

- DLP-C137 Modify a 1+1 Protection Group, page 18-43
- DLP-C138 Delete a Protection Group, page 18-43

Step 4 For the ONS 15310-MA, perform any of the following tasks as needed:

- DLP-C245 Modify a 1:1 Protection Group for the ONS 15310-MA, page 19-57
- DLP-C137 Modify a 1+1 Protection Group, page 18-43
- DLP-C244 Modify an Optimized 1+1 Protection Group for the ONS 15310-MA, page 19-56
- DLP-C138 Delete a Protection Group, page 18-43

Note 1:1 protection groups are created automatically and can only be deleted when the protect card of a 1:1 protection group is deleted.

Step 5 Complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Stop. You have completed this procedure.

NTP-C82 Change Node Timing

Purpose	This procedure changes the SONET timing settings for the ONS 15310-CL and ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	NTP-C23 Set Up Timing, page 4-11
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 15310-CL and ONS 15310-MA nodes should be timed to a Stratum 2 or better primary reference source.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Step 3 As needed, complete the "DLP-C139 Change the Node Timing Source" task on page 18-44.

Step 4 If you need to change any internal timing settings, follow the "DLP-C46 Set Up Internal Timing" task on page 17-63 for the settings you need to modify.

Step 5 If you need to verify timing after removing a node from a path protection configuration, see the "DLP-C140 Verify Timing in a Reduced Ring" task on page 18-45.

Step 6 Complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Stop. You have completed this procedure.

NTP-C83 Modify Users and Change Security

Purpose	This procedure modifies user and security properties for the ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	NTP-C19 Create Users and Assign Security, page 4-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Step 3 Perform any of the following tasks as needed:

- DLP-C141 Change the Security Policy on a Single Node, page 18-46

- DLP-C142 Change the Security Policy on Multiple Nodes, page 18-47
- DLP-C143 Change Node Access and PM Clearing Privilege, page 18-48
- DLP-C234 Grant Superuser Privileges to Provisioning Users, page 19-37
- DLP-C144 Change User Password and Security Settings on a Single Node, page 18-50
- DLP-C145 Change User Password and Security Settings on Multiple Nodes, page 18-50
- DLP-C146 Delete a User on a Single Node, page 18-51
- DLP-C147 Delete a User on Multiple Nodes, page 18-52
- DLP-C148 Log Out a User on a Single Node, page 18-52
- DLP-C149 Log Out a User on Multiple Nodes, page 18-53
- DLP-C196 Configure the Node for RADIUS Authentication, page 18-95

Step 4 Complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Stop. You have completed this procedure.

NTP-C84 Change SNMP Settings

Purpose	This procedure modifies SNMP settings for the ONS 15310-CL and ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	NTP-C25 Set Up SNMP, page 4-15
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Step 3 Perform any of the following tasks as needed:

- DLP-C150 Modify SNMP Trap Destination, page 18-54
- DLP-C151 Delete SNMP Trap Destinations, page 18-55

Step 4 Complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Stop. You have completed this procedure.

NTP-C85 Modify or Delete Communications Channel Terminations and Provisionable Patchcords

Purpose	This procedure changes or deletes SDCCs and LDCCs, and deletes provisionable patchcords (PPCs) on the ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C52 Provision Section DCC Terminations, page 17-68 DLP-C53 Provision Line DCC Terminations, page 17-70 DLP-C49 Create a Provisionable Patchcord, page 17-66
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 Complete the "DLP-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the following tasks to modify data communication channel settings:

- DLP-C152 Change a Section DCC Termination, page 18-55
- DLP-C153 Change a Line DCC Termination, page 18-56

Step 3 As needed, complete the following tasks to delete data communication channel terminations:

- DLP-C154 Delete a Section DCC Termination, page 18-56.
- DLP-C155 Delete a Line DCC Termination, page 18-57.

Step 4 As needed, complete the "DLP-C156 Delete a Provisionable Patchcord" task on page 18-57.

Stop. You have completed this procedure.

CHAPTER 12

Upgrade Cards and Spans

This chapter explains how to upgrade a DS1-28/DS3-EC1-3 card to a DS1-84/DS3-EC1-3 card, and optical spans in a Cisco ONS 15310-MA.

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* as necessary.

Before You Begin

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

1. NTP-C165 Upgrade a DS1-28/DS3-EC1-3 Card to a DS1-84/DS3-EC1-3 Card, page 12-1—Complete as needed.
2. NTP-C170 Upgrade OC-N Spans Automatically, page 12-4—Complete as needed.

NTP-C165 Upgrade a DS1-28/DS3-EC1-3 Card to a DS1-84/DS3-EC1-3 Card

Purpose	This task upgrades a DS1-28/DS3-EC1-3 card in a 1:1 protection scheme) to a DS1-84/DS3-EC1-3 card.
Tools/Equipment	DS1-28/DS3-EC1-3 card(s), DS1-84/DS3-EC1-3 card(s)
Prerequisite Procedures	NTP-C155 Install the Electrical Cards, page 2-20
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 The ONS 15310-MA prefers to designate the cards in Slots 1 and 5 as working. If a protection group can be created with Slots 1 or 5 as the working slots, then it will do so. If Slot 1 or 5 cannot be working (due to violation of one of the other protection rules), then Slot 2 or 6 can be working. Refer to the *Cisco ONS 15310-CL and the Cisco ONS 15310-MA Reference Manual* for more information about card protection.

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-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

Step 3 In node view, double-click the current protect card. The card view appears.

Step 4 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 5 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 6 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 7 Right-click the protect slot and change the DS1-28/DS3-EC1-3 card to the DS1-84/DS3-EC1-3 card:

a. Choose **Change Card** from the drop-down list.

b. Choose the new card type (DS1_84_DS3_EC1_3) from the Change to drop-down list.

c. Click **OK**.

Step 8 Physically insert the new DS1-84/DS3-EC1-3 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 DS1-84/DS3-EC1-3 card to become standby. For more information about LED behavior during the DS1-84/DS3-EC1-3 card boot-up, see the "NTP-C155 Install the Electrical Cards" procedure on page 2-20.

Step 9 Because the DS1-28/DS3-EC1-3 card is now active, switch traffic away from the DS1-28/DS3-EC1-3 card:

a. In node view, double-click the DS1-28/DS3-EC1-3 card you are upgrading.

b. Click the **Maintenance > Protection** tabs.

c. Double-click the protection group that contains the working card.

d. Click the working card.

e. Click **Switch** and **Yes** in the Confirmation dialog box.

Step 10 Physically remove the DS1-28/DS3-EC1-3 card you are upgrading.

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 11 Change the DS1-28/DS3-EC1-3 card to the DS1-84/DS3-EC1-3 card in CTC:

a. Right-click the slot where you removed the DS1-28/DS3-EC1-3 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 12 Insert the DS1-84/DS3-EC1-3 card into the empty. 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 DS3/EC1-48 card bootup, see the "NTP-C155 Install the Electrical Cards" procedure on page 2-20.

Step 13 Clear the switch you performed in Step 9:

a. In node view, double-click the slot where you just installed the DS1-84/DS3-EC1-3 card.

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.

Step 14 As necessary, repeat Steps 3 through 13 for other DS1-28/DS3-EC1-3 cards you want to upgrade.

Stop. You have completed this procedure.

NTP-C170 Upgrade OC-N Spans Automatically

Purpose	This procedure upgrades 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	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

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 2-1 on page 2-29.

Note During the upgrade, the IMPROPRMVL alarm might be raised. It will clear automatically.

Step 1 Determine the type of upgrade you need to make and be sure you have the necessary cards. Valid span upgrades include:

- OC-3 to OC-12
- OC-12 to OC-48

Step 2 Complete the "DLP-C29 Log into CTC" task on page 17-44. If you are already logged in, continue with Step 3.

Step 3 According to local site practice, complete the "NTP-C102 Back Up the Database" procedure on page 15-2.

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-C163 Check the Network for Alarms and Conditions" task on page 18-58 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. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* for information about alarms.

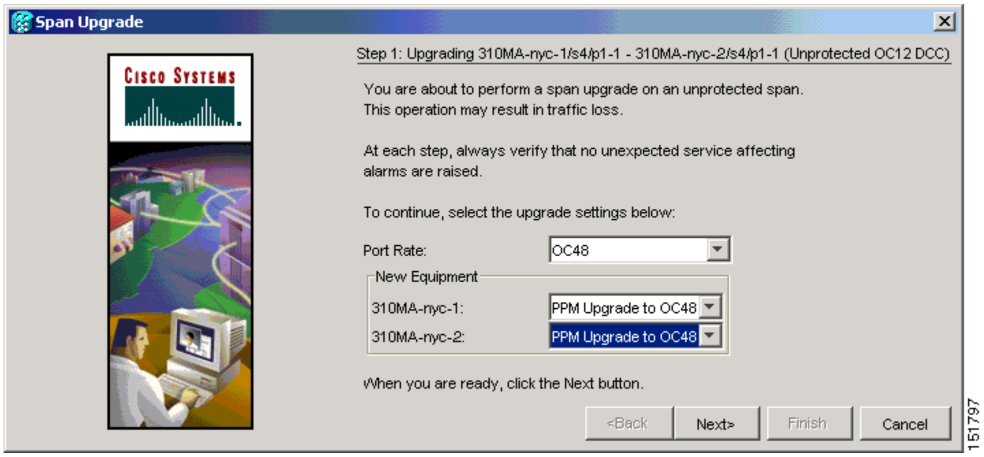
Step 5 In network view, right-click the span you want to upgrade.

Step 6 Choose **Span Upgrade** from the drop-down list.

Step 7 The first Span Upgrade dialog box appears (Figure 12-1). Follow the instructions in the dialog box and the wizard will lead you through the rest of 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



Step 1: Upgrading 310MA-nyc-1/s4/p1-1 - 310MA-nyc-2/s4/p1-1 (Unprotected OC12 DCC)

You are about to perform a span upgrade on an unprotected span.
This operation may result in traffic loss.

At each step, always verify that no unexpected service affecting alarms are raised.

To continue, select the upgrade settings below:

Port Rate: OC48

New Equipment

310MA-nyc-1: PPM Upgrade to OC48

310MA-nyc-2: PPM Upgrade to OC48

When you are ready, click the Next button.

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 8 Repeat Steps 5 through 7 for additional spans in the ring.

Stop. You have completed this procedure.

CHAPTER 13

Convert Network Configurations

This chapter explains how to convert from one SONET topology to another in a Cisco ONS 15310-CL or Cisco ONS 15310-MA 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-C136 Convert a Point-to-Point to a Linear ADM Automatically, page 13-2—Complete as needed.
2. NTP-C93 Convert a Point-to-Point to a Linear ADM Manually, page 13-4—Complete as needed if the in-service topology upgrade wizard is not available or you need to back out of the wizard.
3. NTP-C96 Convert an Unprotected Point-to-Point or Linear ADM to a Path Protection Configuration Automatically, page 13-6—Complete as needed.
4. NTP-C95 Convert a Point-to-Point or Linear ADM to a Path Protection Manually, page 13-7—Complete as needed if the in-service topology upgrade wizard is not available or you need to back out of the wizard.

NTP-C136 Convert a Point-to-Point to a Linear ADM Automatically

Purpose	This procedure converts a point-to-point configuration (two nodes) to a linear ADM (three or more nodes) by adding a third node between two nodes in a 1+1 configuration. The node being added must be an ONS 15454, ONS 15454 SDH, ONS 15327, ONS 15310-MA, or ONS 15600 because the ONS 15310-CL has only two optical ports and therefore cannot be added between two other nodes. If you have an ONS 15310-MA with only two optical ports in use, you can also follow this procedure.
Tools/Equipment	None
Prerequisite Procedures	The in-service topology upgrade procedure requires that the node being added is reachable (has IP connectivity with CTC). If the PC running CTC and the ONS 15310-CL or ONS 15310-MA nodes are not at the same location, two technicians who can communicate with each other during the upgrade might be needed.
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 1-1 on page 1-13 for the ONS 15310-CL, or Table 2-1 on page 2-29 for the ONS 15310-MA.

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-C29 Log into CTC" task on page 17-44 at a node on the point-to-point or linear ADM. 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. The Select Upgrade Protection dialog box appears.

Step 3 Select **Terminal to Linear** in the drop-down list. The first page of the wizard, Upgrade Protection: Terminal to Linear, appears.

Step 4 The Upgrade Protection: Terminal to Linear page lists the following conditions that must be met before 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 a 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 communications channel has been provisioned on these four ports.

Note The ONS 15310-CL has two optical ports and therefore cannot be added in between two other nodes. It can only be configured as an end node in a linear ADM. The ONS 15310-MA has four optical ports and therefore does not have this restriction.

- 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, and any existing DCC terminations as described in the procedure guide for the device you are adding.

Step 5 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 6 Click **Next**. The Select Protection Group Ports page appears.

Step 7 Select the working and protect ports on the new node that you want to connect to each terminal node from the drop-down lists.

Step 8 Click **Next**. The Re-fiber the Protected Path dialog box appears.

Step 9 Follow the instructions in the dialog box for connecting the fibers between the nodes.

Step 10 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 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 11 Click **Next** on the Update Circuit(s) on *Node-Name* dialog box.

The Force Traffic to Protect Path dialog box appears. This dialog box states that it is about to force the traffic from the working to protect path for the terminal nodes.

Step 12 When you are ready to proceed, click **Next**.

Step 13 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. The final dialog box informs you when you have completed the procedure of upgrading from terminal to linear protection.

Step 14 Click **Finish**.

Stop. You have completed this procedure.

NTP-C93 Convert a Point-to-Point to a Linear ADM Manually

Purpose	This procedure upgrades a point-to-point configuration (two nodes) to a linear ADM configuration (3 or more nodes) manually, that is, without using the in-service topology upgrade wizard. Use this procedure if the wizard is unavailable or you need to back out of the wizard.
Tools/Equipment	None
Prerequisite Procedures	NTP-C141 Create Optical Protection Groups for the ONS 15310-CL, page 4-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution This procedure is service-affecting.

Note The node being added must be an ONS 15454, ONS 15454 SDH, ONS 15327, ONS 15310-MA, or ONS 15600 because the ONS 15310-CL has only two optical ports and therefore cannot be added between two other nodes.

Note Optical transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in Table 1-1 on page 1-13 for the ONS 15310-CL, or Table 2-1 on page 2-29 for the ONS 15310-MA.

Note In a point-to-point configuration, two OC-N cards/ports are connected to two OC-N cards/ports on a second node.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at one of the two point-to-point nodes. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-C163 Check the Network for Alarms and Conditions" task on page 18-58.

Step 3 In node view, display one of the point-to-point node that will connect to the new node.

Step 4 Create a 1+1 protection group for the OC-N cards/ports that will connect to the new node. See the "NTP-C141 Create Optical Protection Groups for the ONS 15310-CL" procedure on page 4-12 or "NTP-C142 Create Protection Groups for the ONS 15310-MA" procedure on page 4-13 for instructions.

Step 5 Create DCC terminations on the working OC-N card/port that will connect to the new node. See the "DLP-C52 Provision Section DCC Terminations" task on page 17-68. (Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-C53 Provision Line DCC Terminations" task on page 17-70.) In the Create SDCC Termination dialog box, set the port state to **IS**.

Step 6 From the View menu, choose **Go to Node View** to display the new node in node view.

Step 7 Verify the card installation for the new node as specified in the documentation for that device.

Step 8 Set up timing for the new node as specified in the documentation for that device. If the new node is using line timing, set the working OC-N card/port as the timing source.

Step 9 Turn up the new node as specified in the documentation for that device.

Step 10 Physically connect the fibers between the point-to-point node and the new node. The fiber connections should be connected working port to working port and protect port to protect port.

Step 11 On the new node, create a 1+1 protection group for the OC-N cards/ports that will connect to the neighbor nodes. For 1+1 provisioning procedures, refer to the documentation specific to the device you are adding.

Step 12 Provision section DCC terminations on the new node's working OC-N cards/ports as specified in the documentation for that device. Make sure to set the Port State in the Create SDCC Termination dialog box to **IS**.

Note Data communications channel (DCC) failure alarms appear until you create DCC terminations in the point-to-point node.

Step 13 From the View menu, choose **Go to Network View** to verify that the newly created linear ADM configuration is correct. One green line should appear between each linear node.

Step 14 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-C88 Disable Alarm Filtering" task on page 17-109 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms are present, investigate and resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

Step 15 Repeat the procedure to add an additional node to the linear ADM.

Stop. You have completed this procedure.

NTP-C96 Convert an Unprotected 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 configuration. This option is a single circuit operation.
Tools/Equipment	None
Prerequisite Procedures	NTP-C27 Provision a Point-to-Point Network, page 5-3 NTP-C29 Provision a Linear ADM Network, page 5-6
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, 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-C29 Log into CTC" task on page 17-44 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-C138 Delete a Protection Group" task on page 18-43. If the point-to-point or linear ADM is unprotected, continue with Step 4.

Step 3 Complete the "DLP-C52 Provision Section DCC Terminations" task on page 17-68 at the nodes that support the point-to-point or linear ADM span. (Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-C53 Provision Line DCC Terminations" task on page 17-70.) Provision the pluggable port module that is not already in the SDCC Terminations list.

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-C57 Provision Path Protection Selectors During Circuit Creation" task on page 17-75.

Step 7 Click **Next**.

Step 8 Complete one of the following tasks:

a. To route the new path protection circuit manually, complete "DLP-C164 Manually Route a Path Protection Circuit in a Topology Upgrade" task on page 18-59.

b. To route the new path protection circuit automatically, complete "DLP-C165 Automatically Route a Path Protection Circuit in a Topology Upgrade" task on page 18-59.

Stop. You have completed this procedure.

NTP-C95 Convert a Point-to-Point or Linear ADM to a Path Protection Manually

Purpose	This procedure upgrades a point-to-point system to a path protection manually, that is, without using the in-service topology upgrade wizard. Use this procedure if the wizard is unavailable or you need to back out of the wizard.
Tools/Equipment	None
Prerequisite Procedures	NTP-C27 Provision a Point-to-Point Network, page 5-3 or NTP-C29 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-C29 Log into CTC" task on page 17-44 at a node on the point-to-point or linear ADM.

Step 2 Complete the "DLP-C163 Check the Network for Alarms and Conditions" task on page 18-58.

Step 3 Complete the "DLP-C115 Delete Circuits" task on page 18-21 for each circuit. The circuits will be recreated after the 1+1 protection groups are deleted.

Step 4 Complete the "DLP-C138 Delete a Protection Group" task on page 18-43 for each 1+1 protection group that supports the point-to-point or linear ADM span.

Step 5 Complete the "NTP-C47 Create an Automatically Routed Optical Circuit" procedure on page 6-34 to recreate the circuits one at a time.

Step 6 Complete the "DLP-C52 Provision Section DCC Terminations" task on page 17-68 at the protect ports in all nodes that will be part of the path protection configuration. Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-C53 Provision Line DCC Terminations" task on page 17-70.

Note If you want to add additional nodes to the path protection configuration, see the "NTP-C97 Add a Path Protection Node" procedure on page 14-1.

Note Path protection is the default configuration if the cards are installed and the DCCs are configured.

Stop. You have completed this procedure.

CHAPTER 14

Add and Remove Nodes

This chapter explains how to add and remove Cisco ONS 15310-CL or Cisco ONS 15310-MA nodes from path protection configurations and linear add-drop multiplexers.

Before You Begin

Before performing any of the following procedures, complete the "NTP-C56 Document Existing Provisioning" procedure on page 9-2. Also investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* as necessary.

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

1. NTP-C97 Add a Path Protection Node, page 14-1—Complete as needed.
2. NTP-C98 Remove a Path Protection Node, page 14-4—Complete as needed.
3. NTP-C99 Add an End Node to a Linear ADM, page 14-6—Complete as needed.
4. NTP-C135 Add a Non-ONS 15310-CL Node to a Linear ADM, page 14-8—Complete as needed to add an ONS 15600, ONS 15454, or ONS 15310-MA node to a linear configuration where an ONS 15310-CL or ONS15310-MA is an end node.
5. NTP-C101 Remove an In-Service Node from a Linear ADM, page 14-9—Complete as needed to remove an node from a linear ADM without disrupting traffic.

NTP-C97 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 1, "Install the Cisco ONS 15310-CL," or Chapter 2, "Install the Cisco ONS 15310-MA," and Chapter 4, "Turn Up a Node."
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser only

Step 1 According to local site practice, complete the "NTP-C102 Back Up the Database" procedure on page 15-2 for all the nodes in the ring.

Step 2 Verify the card installation on the new node. See the "NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL" procedure on page 4-2.

Note In Cisco Transport Controller (CTC), SFPs are called pluggable port modules (PPMs).

Step 3 Verify that the OC-N ports (or cards in non-310 nodes) that will serve as the path protection trunk (span) ports 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-12 ports, the new node must have OC-12 ports.

Step 4 Verify that fiber is available to connect the new node to the existing nodes.

Step 5 Complete the "NTP-C26 Verify Node Turn-Up" procedure on page 5-2.

Step 6 Log into a node in the path protection configuration where you want to add a node. See the "DLP-C29 Log into CTC" task on page 17-44 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 7 Complete the "DLP-C163 Check the Network for Alarms and Conditions" task on page 18-58 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 Chapter 9, "Manage Alarms" or, if necessary, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

Step 8 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 9 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 10, 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 10 Log into the new node:

- If the node has a LAN connection and does not appear on the network map, from the File menu, choose **Add Node**, then enter the IP address or the DNS name of the new node and click **OK**. Wait for the new node to initialize and appear on the network map. Proceed to the next bullet point.
- If the node has a LAN connection and appears on the network map, from the View menu, choose **Go to Other Node**, then choose the new node from the Select Node to Go to drop-down list on the Select Node dialog box and click **OK**.
- If the new node is not connected to the network, log into it directly using the "DLP-C29 Log into CTC" task on page 17-44.

Step 11 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-C88 Disable Alarm Filtering" task on page 17-109 as necessary.

b. 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 Chapter 9, "Manage Alarms" or, if necessary, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

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 Complete the following steps if the node is on the same subnet as other path protection nodes, it is not provisioned as an ENE (see the "NTP-C21 Set Up CTC Network Access" procedure on page 4-6), and a CTC computer will directly connect to the node while other CTC computers are directly connected to other path protection nodes. If not, continue with Step 14.

a. Click the **Provisioning > Network > General** tabs. View the IP Address and Net/Subnet Mask Length fields to verify the node is on the same subnet as other path protection nodes.

b. Click the **Static Routing** tab and click **Create**.

c. In the Create Static Route dialog box, enter the following settings:

- Destination IP address: *Local-PC-IP-address*
- Net Mask: **255.255.255.255**
- Next Hop: *IP-address-of-the-Cisco-ONS-15310-CL or MA*
- Cost: **1**

d. Click **OK**.

Step 14 (Optional) Create test circuits, making sure they pass through the path protection line ports, and run test traffic through the node to ensure the ports are functioning properly. See the "NTP-C48 Create a Manually Routed Optical Circuit" procedure on page 6-39 and the "NTP-C50 Test Optical Circuits" procedure on page 6-44 for information.

Step 15 Create the DCC terminations on the new node. See the "DLP-C52 Provision Section DCC Terminations" task on page 17-68.

Step 16 From the View menu, choose **Go to Network View**.

Step 17 Complete the "DLP-C166 Initiate a Path Protection Force Switch on a Span" task on page 18-60 to switch traffic away from the span that will be broken to connect to the new node.

Step 18 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 19 Replace the removed fibers with the fibers that are connected to the new node.

Step 20 Log out of CTC and log back into a node in the network.

Step 21 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 22 Click the **Circuits** tab and wait for all the circuits to appear, including spans. Count the number of partial circuits.

Step 23 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 24 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 24 does not create the overlay ring circuits that route traffic around multiple rings passing through one or more nodes more than once, on the new node.

Step 24 In the network view, right-click the new node and choose **Update Circuits With New Node** from the list of options. 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 8).

Step 25 Click the **Circuits** tab and verify that no partial circuits appear. However, if the partial circuits still exist in the network, verify whether they were present in Step 9 and Step 12. This will ensure that no additional partial circuits are created by this procedure.

Step 26 Complete the "DLP-C167 Clear a Path Protection Force Switch" task on page 18-61.

Step 27 (Optional) Complete the "NTP-C32 Path Protection Acceptance Test" procedure on page 5-12.

Stop. You have completed this procedure.

NTP-C98 Remove a Path Protection Node

Purpose	This procedure removes a node from a path protection configuration.
Tools/Equipment	None
Prerequisite Procedures	NTP-C102 Back Up the Database, page 15-2
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 which 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 target node)
- The node that is connected through its east port to the target node

Step 2 Log into a node in the network where you want to remove a path protection node. See the "DLP-C29 Log into CTC" task on page 17-44 for instructions.

Step 3 Complete the "DLP-C163 Check the Network for Alarms and Conditions" task on page 18-58 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 9, "Manage Alarms" or, if necessary, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

Step 4 Complete the "DLP-C115 Delete Circuits" task on page 18-21 for circuits that originate or terminate in the target node. (If a circuit has multiple drops, delete only the drops that terminate on the node you are deleting.)

Step 5 Complete the "DLP-C168 Verify Pass-Through Circuits" task on page 18-62 to verify that circuits passing through the target node enter and exit the node on the same STS or VT.

Step 6 Complete the "DLP-C166 Initiate a Path Protection Force Switch on a Span" task on page 18-60 for all spans connected to the node you are removing.

Step 7 Remove all fiber connections between the target node and the two neighboring nodes.

Step 8 Reconnect the fiber of the two neighboring nodes directly, west port to east port.

Note If you delete a node that was in a login node group, you will see partial circuits for that node in 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.)

Step 9 Exit CTC and log back in. See the "DLP-C29 Log into CTC" task on page 17-44 for instructions.

Step 10 Log into each newly connected node and open the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-C88 Disable Alarm Filtering" task on page 17-109 as necessary.

b. Verify that the trunk cards/ports are free of alarms. Resolve any alarms before proceeding. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

Step 11 Complete the "DLP-C140 Verify Timing in a Reduced Ring" task on page 18-45.

Step 12 Complete the "DLP-C167 Clear a Path Protection Force Switch" task on page 18-61.

Step 13 Click the **Circuits** tab and verify that no partial circuits are present.

Step 14 (Optional) Complete the "NTP-C32 Path Protection Acceptance Test" procedure on page 5-12.

Stop. You have completed this procedure.

NTP-C99 Add an End Node to a Linear ADM

Purpose	This procedure adds a single ONS 15310-CL node or ONS 15310-MA to the end of an ONS 15310 linear add-drop multiplexer (ADM) network. To add a non-ONS 15310-CL node in the middle of a linear ADM, use the "NTP-C135 Add a Non-ONS 15310-CL Node to a Linear ADM" procedure on page 14-8.
Tools/Equipment	None
Prerequisite Procedures	NTP-C29 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 1-1 on page 1-13 for the ONS 15310-CL, or Table 2-1 on page 2-29 for the ONS 15310-MA.

Note In a linear ADM configuration, two OC-N ports in 1+1 protection are connected to two OC-N ports in 1+1 protection on a second node. On the second node, two more OC-N ports 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. The ONS 15310-CL has only two optical ports. This restricts an ONS 15310-CL to being the end node in a linear ADM network since both ports are necessary to create the 1+1 protection group to the neighbor node. The ONS 15310-MA has four optical ports and can be added as an end node or in the middle of a linear ADM.

Note The two optical ports on the ONS 15310-CL are present on Slot 2 of the chassis. The two optical ports on the ONS 15310-MA are present on either Slot 3 or Slot 4 of the chassis. Other ONS 15xxx platforms do not allow a 1+1 protection group to be created if the working and protect ports are on the same slot. This restriction is not applicable to the ONS 15310-CL because it only has optical ports on Slot 2. Any of these ports (Slot 2, Port 1-1 or slot 2, Port 2-1 for the ONS 15310-CL or Slot 3, Port 1-1 or Port 2-1 or Slot 4, Port 1-1 or Port 2-1 for the ONS 15310-MA) can be designated as the working port, depending on your configuration and fiber connections.

Caution If the linear ADM carries traffic, you cannot add a node between two linear nodes unless you delete and recreate the circuits. Use this procedure to add a node to the end of the linear ADM.

Step 1 According to local site practice, complete the "NTP-C102 Back Up the Database" procedure on page 15-2 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-C26 Verify Node Turn-Up" procedure on page 5-2.

Step 3 Verify that the new node has two available optical ports with the same rate as the linear ADM. If the optical ports are not installed, complete the "DLP-C16 Install SFP Connectors" task on page 17-22. If the optical ports have different line rates, complete the "DLP-C194 Change the Optical Line Rate" task on page 18-93.

Step 4 For the ONS 15310-CL, complete "NTP-C141 Create Optical Protection Groups for the ONS 15310-CL" procedure on page 4-12 for the two OC-N ports that will connect to the linear ADM node.

Step 5 For the ONS 15310-MA, complete "NTP-C142 Create Protection Groups for the ONS 15310-MA" procedure on page 4-13 for the two OC-N ports that will connect to the linear ADM node.

Step 6 Complete the "DLP-C52 Provision Section DCC Terminations" task on page 17-68 for the working OC-N port at the new node. Make sure to set the Port State in the Create SDCC Termination dialog box to **IS**. (Do not create a DCC termination on the protect port.)

Note DCC failure alarms appear after you create DCC terminations in the linear ADM node until you connect the fiber during Step 14.

Step 7 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the linear ADM node that will connect to the new node. If you are already logged in, continue with Step 8.

Step 8 Complete the "DLP-C163 Check the Network for Alarms and Conditions" task on page 18-58.

Step 9 Install the OC-N port that will connect to the new node. See "DLP-C16 Install SFP Connectors" task on page 17-22. If the ports are already installed, continue with Step 10.

Note If the new node is not an ONS 15310-CL or ONS 15310-MA, refer to the corresponding user documentation for installation procedures.

Step 10 Connect the working port at the existing linear ADM node to the working port at the new node. See "DLP-C18 Install Fiber-Optic Cables in a 1+1 Configuration" task on page 17-24.

Step 11 Connect the protect port at the existing linear ADM node to the protect port at the new node.

Step 12 Complete "NTP-C141 Create Optical Protection Groups for the ONS 15310-CL" procedure on page 4-12 for the two OC-N ports that connect to the new node.

Step 13 Complete the "NTP-C142 Create Protection Groups for the ONS 15310-MA" procedure on page 4-13 for the two OC-N ports that connect to the new node.

Step 14 Complete the "DLP-C52 Provision Section DCC Terminations" task on page 17-68 for the working OC-N port that connects to the working port on the new node. Make sure to set the Port State in the Create SDCC Termination dialog box to **IS**. (Do not create a DCC termination for the protect port.)

Step 15 From the View menu, choose **Go to Network View.** Verify that the newly created linear ADM configuration is correct. A green span line should appear between each linear node.

Step 16 Complete the "DLP-C163 Check the Network for Alarms and Conditions" task on page 18-58 to verify that no unexpected alarms or conditions are present.

Stop. You have completed this procedure.

NTP-C135 Add a Non-ONS 15310-CL Node to a Linear ADM

Purpose	This procedure adds an ONS 15600, ONS 15454, or ONS 15310-MA between two nodes in a 1+1 configuration. Because the ONS 15310-CL has only two optical ports, it cannot be added as a middle node. The ONS 15310-MA has four optical ports and therefore does not have this restriction.
Tools/Equipment	None
Prerequisite Procedures	This procedure requires that the node to be added is reachable (has IP connectivity with CTC). If the PC running CTC and the ONS 15310-CL or ONS 15310-MA nodes are not at the same location, two technicians who can communicate with each other during the upgrade might be needed.
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 1-1 on page 1-13 for the ONS 15310-CL, or Table 2-1 on page 2-29 for the ONS 15310-MA.

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-C29 Log into CTC" task on page 17-44 at a node on the point-to-point or linear ADM. 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 the new node. The Select Upgrade Protection dialog box appears.

Step 3 Select **Terminal to Linear** from the drop-down list. The first page of the wizard, Upgrade Protection: Terminal to Linear, appears.

Step 4 The Upgrade Protection: Terminal to Linear page lists the following conditions that must be met before 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 a compatible software version with that of the terminal nodes.
- The node has four unused optical ports matching the speed of the 1+1 protection group and no communications channel has been provisioned on these four ports.

Note The ONS 15310-CL has two optical ports and therefore cannot be added in between two other nodes. It can only be configured as an end node in a linear ADM. The ONS 15310-MA has four optical ports and therefore does not have this restriction.

- 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 into the unreachable node using a separate CTC session and configure that node.

Step 5 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 6 Click **Next**. The Select Protection Group Ports page appears.

Step 7 Select the working and protect ports on the new node that you want to connect to each terminal node from the drop-down lists.

Step 8 Click **Next**. The Re-fiber the Protected Path dialog box appears.

Step 9 Follow the instructions in the dialog box for connecting the fibers between the nodes.

Step 10 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 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 11 Click **Next** on the Update Circuit(s) on *Node-Name* dialog box.

The Force Traffic to Protect Path dialog box appears. This dialog box states that it is about to force the traffic from the working to protect path for the terminal nodes.

Step 12 When you are ready to proceed, click **Next**.

Step 13 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. The final dialog box informs you when you have completed the procedure.

Step 14 Click **Finish.**

Stop. You have completed this procedure.

NTP-C101 Remove an In-Service Node from a Linear ADM

Purpose	This procedure removes a single ONS 15600, ONS 15454, pr ONS 15310-MA node from a linear ADM that contains an ONS 15310-CL or an ONS 15310-MA as an end node(s).
Tools/Equipment	None
Prerequisite Procedures	NTP-C29 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-C137 Modify a 1+1 Protection Group" task on page 18-43 to change it to unidirectional. After you have removed the node from the linear group you can then change the protection setting back to bidirectional.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 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-C88 Disable Alarm Filtering" task on page 17-109 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 15310-CL and Cisco ONS 15310-MA 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 15310-CL and Cisco ONS 15310-MA 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 (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 protect ports of 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 15310-CL and the Cisco ONS 15310-MA.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* as necessary.

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

1. NTP-C102 Back Up the Database, page 15-2—Complete as needed.
2. NTP-C103 Restore the Database, page 15-3—Complete as needed.
3. NTP-C132 View and Manage OSI Information, page 15-4—Complete as needed.
4. NTP-C104 Restore the Node to Factory Configuration, page 15-5—Complete as needed to clear the database and upload a blank database and the latest software.
5. NTP-C105 View the Audit Trail Records, page 15-6—Complete as needed.
6. NTP-C106 Offload the Audit Trail Record, page 15-8—Complete as needed.
7. NTP-C107 Off-Load the Diagnostics File, page 15-9—Complete as needed.
8. NTP-C108 Initiate or Clear an External Switching Command, page 15-9—Complete as needed.
9. NTP-C109 Clean Fiber Connectors, page 15-10—Complete as needed.
10. NTP-C145 Replace the Fan-Tray Assembly, page 15-11—Complete as needed.
11. NTP-C134 Reset Cards Using CTC, page 15-13—Complete as needed to reset cross-connect, electrical, and Ethernet cards.
12. NTP-C114 View the Loopback Status on a Port, page 15-13—Complete as needed to view the loopback status on electrical and optical ports.
13. NTP-C115 Switch the Node Timing Reference, page 15-14—Complete as needed to switch the node timing reference in order to perform maintenance or return to normal timing operation.
14. NTP-C116 View the Timing Report, page 15-15—Complete as needed.
15. NTP-C137 Edit Network Element Defaults, page 15-18—Complete as needed to edit the factory-configured (default) network element (NE) settings.

16. NTP-C138 Import Network Element Defaults, page 15-19—Complete as needed to import the factory-configured (default) NE settings.
17. NTP-C139 Export Network Element Defaults, page 15-20—Complete as needed to export the factory-configured (default) NE settings.

NTP-C102 Back Up the Database

Purpose	This procedure stores a backup version of the Cisco Transport Controller (CTC) software database on the workstation running 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, IP address, subnet mask and gateway, 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-C29 Log into CTC" task on page 17-44 at the node you want to back up. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Maintenance > Database** tabs.

Step 3 Click **Backup**.

Step 4 In the Backup Database window, click **Browse**.

Step 5 In the Save window, navigate to a local PC directory or network directory and type a database name (such as database.db) in the File name field.

Note The database file must have a *.db extension.

Step 6 Click **Save**.

Step 7 Click **OK** to confirm the path and file name.

Step 8 If you are overwriting an existing file, click **OK** in the confirmation dialog box.

Stop. You have completed this procedure.

NTP-C103 Restore the Database

Purpose	This procedure restores the 15310-CL-CTX (ONS 15310-CL) or CTX2500 (ONS 15310-MA) software database.
Tools/Equipment	None
Prerequisite Procedures	NTP-C102 Back Up the Database, page 15-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning (if granted privilege through NE Defaults) or higher.

Note The following parameters are not backed up and restored: 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.

Note Ethernet cards must be reset after a database restore. For information on restoring Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Caution If you are restoring the database on multiple nodes, wait approximately one minute after the 15310-CL-CTX or CTX2500 reboot has completed on each node before proceeding to the next node.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node where you are restoring the database. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Maintenance > Database** tabs.

Step 3 Click **Restore**.

Step 4 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 software CD.

Step 5 Click the database file to highlight it.

Step 6 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 7 If you need a complete database restore, check the **Complete database (System and Provisioning)** check box. Continue with Step 9.

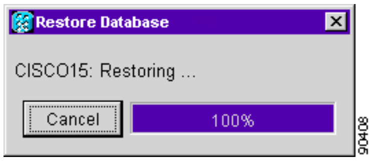
Note Complete database restore may be used only on a node that is removed from the network, and does not carry live provisioning traffic. This operation needs to be done by a live operator onsite, and must not use a remote connection.

Step 8 If you need to restore only the provisioning database (partial restore), do not check the **Complete database (System and Provisioning)** checkbox.

Step 9 Click **Ok**.

The Restore Database dialog box monitors the file transfer (Figure 15-1).

Figure 15-1 Restoring the Database—In-Process Notification



Restore Database

CISCO15: Restoring ...

Step 10 Wait for the file to complete the transfer to the 15310-CL-CTX or CTX2500 card. When the transfer completes, CTC switches to network view. Wait for the node to reconnect.

Stop. You have completed this procedure.

NTP-C132 View and Manage OSI Information

Purpose	This procedure allows you to view and manage Open System Interconnection (OSI) including the End System-to-Intermediate System (ES-IS) and Intermediate System-to-Intermediate System (IS-IS) routing information tables, the TID Address Resolution Protocol (TARP) data cache, and the manual area table.
Tools/Equipment	None
Prerequisite Procedures	NTP-C102 Back Up the Database, page 15-2 NTP-C13 Set Up Computer for CTC, page 3-2 NTP-C131 Provision OSI, page 4-16
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher can view OSI information. Maintenance or higher can manage OSI information.

Note Additional information about OSI is provided in the “Management Network Connectivity” chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 1 Complete the “DLP-C29 Log into CTC” task on page 17-44. If you are already logged in, continue with Step 2.

Step 2 Perform any of the following tasks as needed:

- DLP-C215 View IS-IS Routing Information Base, page 19-13
- DLP-C216 View ES-IS Routing Information Base, page 19-13
- DLP-C217 Manage the TARP Data Cache, page 19-14

Stop. You have completed this procedure.

NTP-C104 Restore the Node to Factory Configuration

Purpose	This procedure reinitializes the ONS 15310-CL or ONS 15310-MA using the CTC reinitialization tool. Reinitialization uploads a new software package to the 15310-CL-CTX or CTX2500 card, clears the node database, and restores the factory default parameters.
Tools/Equipment	Cisco ONS 15310-CL System Software CD, Version 8.5.x or Cisco ONS 15310-MA System Software CD, Version 8.5.x JRE 5.0 must be installed on the computer to log into the node at the completion of the reinitialization. The reinitialization tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 5.0.
Prerequisite Procedures	NTP-C102 Back Up the Database, page 15-2 NTP-C13 Set Up Computer for CTC, page 3-2 One of the following: • NTP-C14 Set Up CTC Computer for Local Craft Connection to the Node, page 3-3 • NTP-C15 Set Up a CTC Computer for a Corporate LAN Connection to the Node, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
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 database in the specified directory if you use the Search Path field instead of the Package and Database fields. It is possible to 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 If you are restoring the database on multiple nodes, wait until the 15310-CL-CTX or CTX2500 card has rebooted on each node before proceeding to the next node.

Caution Cisco recommends that you take care to save the node database to safe location if you are not 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 are using Microsoft Windows, complete the "DLP-C169 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)" task on page 18-63.

Step 2 If you are using UNIX, complete the "DLP-C170 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)" task on page 18-65.

Stop. You have completed this procedure.

NTP-C105 View the Audit Trail Records

Purpose	This procedure explains how to view audit trail records. Audit trail records prove 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 (if granted privilege through NE Defaults) or higher.

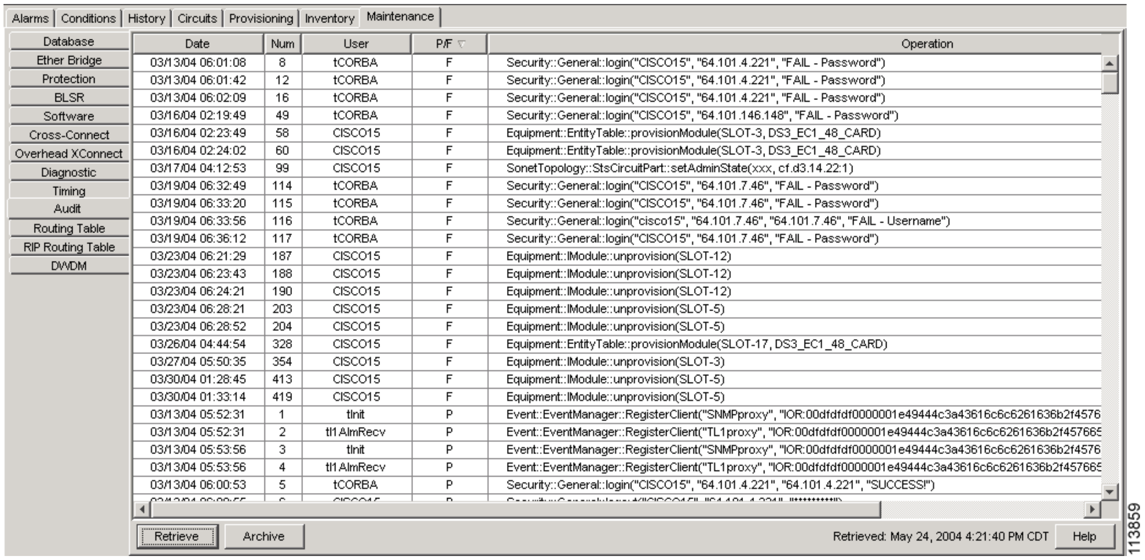
Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node where you want to view the audit trail log. If you are already logged in, continue with Step 2.

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 15-2.

Figure 15-2 Viewing Audit Trail Records



Date	Num	User	P/F	Operation
03/13/04 06:01:08	8	tCORBA	F	Security::General::login("CISCO15", "64.101.4.221", "FAIL - Password")
03/13/04 06:01:42	12	tCORBA	F	Security::General::login("CISCO15", "64.101.4.221", "FAIL - Password")
03/13/04 06:02:09	16	tCORBA	F	Security::General::login("CISCO15", "64.101.4.221", "FAIL - Password")
03/16/04 02:19:49	49	tCORBA	F	Security::General::login("CISCO15", "64.101.146.148", "FAIL - Password")
03/16/04 02:23:49	58	CISCO15	F	Equipment::EntityTable::provisionModule(SLOT-3, DS3_EC1_48_CARD)
03/16/04 02:24:02	60	CISCO15	F	Equipment::EntityTable::provisionModule(SLOT-3, DS3_EC1_48_CARD)
03/17/04 04:12:53	99	CISCO15	F	SonetTopology::StsCircuitPart::setAdminState(xxx, cf.d3.14.22:1)
03/19/04 06:32:49	114	tCORBA	F	Security::General::login("CISCO15", "64.101.7.46", "FAIL - Password")
03/19/04 06:33:20	115	tCORBA	F	Security::General::login("CISCO15", "64.101.7.46", "FAIL - Password")
03/19/04 06:33:56	116	tCORBA	F	Security::General::login("cisco15", "64.101.7.46", "64.101.7.46", "FAIL - Username")
03/19/04 06:36:12	117	tCORBA	F	Security::General::login("CISCO15", "64.101.7.46", "FAIL - Password")
03/23/04 06:21:29	187	CISCO15	F	Equipment::IModule::unprovision(SLOT-12)
03/23/04 06:23:43	188	CISCO15	F	Equipment::IModule::unprovision(SLOT-12)
03/23/04 06:24:21	190	CISCO15	F	Equipment::IModule::unprovision(SLOT-12)
03/23/04 06:28:21	203	CISCO15	F	Equipment::IModule::unprovision(SLOT-5)
03/23/04 06:28:52	204	CISCO15	F	Equipment::IModule::unprovision(SLOT-5)
03/26/04 04:44:54	328	CISCO15	F	Equipment::EntityTable::provisionModule(SLOT-17, DS3_EC1_48_CARD)
03/27/04 05:50:35	354	CISCO15	F	Equipment::IModule::unprovision(SLOT-3)
03/30/04 01:28:45	413	CISCO15	F	Equipment::IModule::unprovision(SLOT-5)
03/30/04 01:33:14	419	CISCO15	F	Equipment::IModule::unprovision(SLOT-5)
03/13/04 05:52:31	1	tInit	P	Event::EventManager::RegisterClient("SNMPproxy", "IOR:00dfdfdf0000001e49444c3a43616c6c6261636b2f4576
03/13/04 05:52:31	2	tl1AlmRecv	P	Event::EventManager::RegisterClient("TL1proxy", "IOR:00dfdfdf0000001e49444c3a43616c6c6261636b2f45766
03/13/04 05:53:56	3	tInit	P	Event::EventManager::RegisterClient("SNMPproxy", "IOR:00dfdfdf0000001e49444c3a43616c6c6261636b2f4576
03/13/04 05:53:56	4	tl1AlmRecv	P	Event::EventManager::RegisterClient("TL1proxy", "IOR:00dfdfdf0000001e49444c3a43616c6c6261636b2f45766
03/13/04 06:00:53	5	tCORBA	P	Security::General::login("CISCO15", "64.101.4.221", "64.101.4.221", "SUCCESS!")

Retrieved: May 24, 2004 4:21:40 PM CDT

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, or task name for system generated actions
P/F	Pass/Fail (that is, whether or not the action was executed)
Operation	Action that was taken

Step 4 Right-click the column headings if you want to display the list in ascending-to-descending or descending-to-ascending order.

Step 5 Left-click the column heading to display a shortcut menu containing 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 the column heading if you want to display an incrementally sorted list.

Stop. You have completed this procedure.

NTP-C106 Offload the Audit Trail Record

Purpose	This procedure describes how to offload 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-C29 Log into CTC" task on page 17-44 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.

Use .txt.gz as the extension. This creates a .gzip file. Use WinZip or GNU gzip to uncompress the file. The uncompressed file is readable in any application that supports text files, such as WordPad, Microsoft Word (imported), etc.

Step 7 Click **Save**.

Entries not saved in the previous archive 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. View the log in a different application.

Stop. You have completed this procedure.

NTP-C107 Off-Load the Diagnostics File

Purpose	This procedure describes how to off-load a diagnostics file. The diagnostics file contains a set of debug commands run on a node and their result. This file is useful to the Cisco Technical Assistance Center (TAC) when they troubleshoot problems with the node.
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-C29 Log into CTC" task on page 17-44 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 **Retrieve**.

Step 4 In the Saving Diagnostic File dialog box, navigate to the directory (local or network) where you want to save the file.

Step 5 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 (.gzip) that can be read by Cisco TAC.

Step 6 Click **Save**.

The Retrieve Tech Support Log status window shows a progress bar indicating the percentage of the file being saved, then shows "Retrieve Tech Support Log complete."

Step 7 Click **OK**.

Stop. You have completed this procedure.

NTP-C108 Initiate or Clear an External Switching Command

Purpose	This procedure describes how to apply an external switching command to an optical port, including Manual and Force switches, lock-ons, and lockouts. Path protection Force switches are also included.
Tools/Equipment	None
Prerequisite Procedures	NTP-C141 Create Optical Protection Groups for the ONS 15310-CL, page 4-12 or NTP-C31 Provision Path Protection Nodes, page 5-10
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node where you want to apply a lock-on or lockout. If you are already logged in, continue with Step 3.

Step 2 To initiate a Manual or Force switch in a 1+1 protection group, complete the "DLP-C179 Initiate an Optical Protection Switch" task on page 18-72.

Step 3 To prevent traffic on a working or protect port from switching to the other port in the pair, complete the "DLP-C171 Apply a Lock-on" task on page 18-67.

Step 4 To prevent traffic from switching to the protect port, complete the "DLP-C172 Apply a Lockout" task on page 18-68.

Step 5 To remove a lock-on or lockout and return a protection group to its usual switching method, complete the "DLP-C173 Clear a Lock-on or Lockout" task on page 18-68.

Note A nonalarmed event (INHSWWKG or INHSWPR) is raised when a port is placed in a lock-on or lockout state.

Step 6 As needed, complete the "DLP-C166 Initiate a Path Protection Force Switch on a Span" task on page 18-60.

Step 7 As needed, complete the "DLP-C167 Clear a Path Protection Force Switch" task on page 18-61.

Note Refer to the "Port Protection" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for a description of protection switching and switch state priorities.

Stop. You have completed this procedure.

NTP-C109 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 **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

Caution Do not reuse the optical swabs. Keep unused swabs off of work surfaces.

Note Replace all dust caps whenever the equipment is not to be immediately used.

Step 1 Using an inspection microscope, inspect each fiber connector for dirt, cracks, or scratches.

Step 2 Replace any damaged fiber connectors.

Step 3 Complete the "DLP-C175 Clean Fiber Connectors with CLETOP" task on page 18-70 as necessary.

Step 4 Complete the "DLP-C176 Clean the Fiber Adapters" task on page 18-70 as necessary.

Note To clean multi-fiber optic connectors, complete the "DLP-C174 Clean Multi Fiber-Optic Cable Connectors" task on page 18-69 as necessary.

Stop. You have completed this procedure.

NTP-C145 Replace the Fan-Tray Assembly

Purpose	This procedure replaces a malfunctioning fan-tray assembly in an ONS 15310-MA. The fan-tray assembly in the ONS 15310-CL cannot be removed or replaced.
Tools/Equipment	None
Prerequisite Procedures	NTP-C152 Install the Fan-Tray Assembly, page 2-14
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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 To replace the fan-tray assembly (FTA), it is not necessary to move any of the cable management facilities.

Step 1 Remove the front door on the ONS 15310-MA by unscrewing the two screws, detaching the door ground strap, and sliding the door up and away from the shelf assembly.

Step 2 Use a Phillips screwdriver to unscrew each screw at either end of the fan tray.

Step 3 Pull the fan tray ejector all the way out, and use the ejector to slide the fan tray out the shelf assembly one inch (25.4 mm), and wait until the fans stop.

Step 4 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

Step 5 On the fan-tray assembly you want to install, pull the fan tray ejector all the way out.

Step 6 Use the ejector to slide the fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.

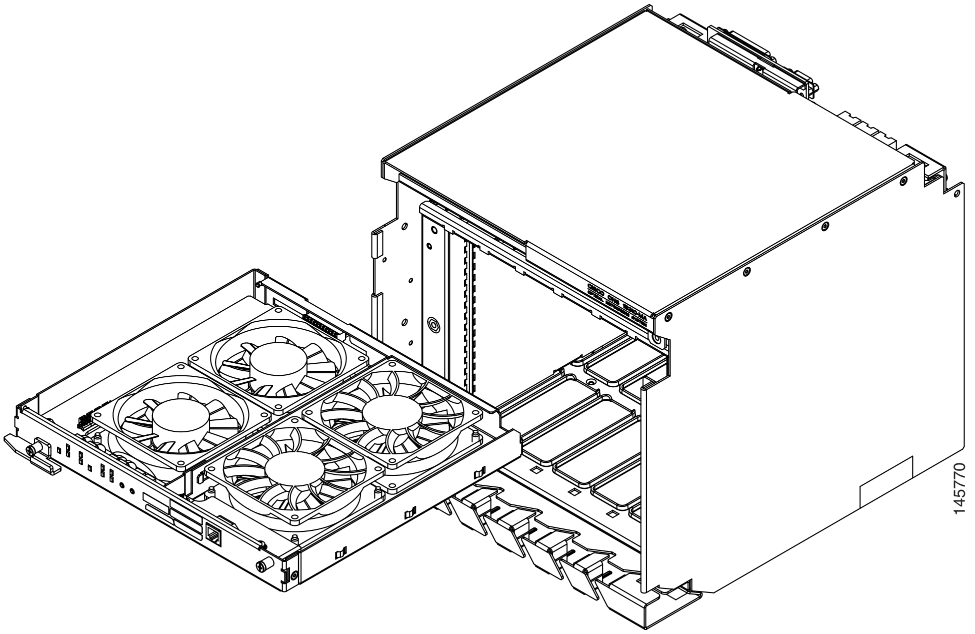
Step 7 Close the ejector.

Step 8 Use a Phillips screwdriver to tighten the screws at either end of the fan-tray assembly.

Step 9 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 15-3 shows the location of the fan tray.

Figure 15-3 Installing the Fan-Tray Assembly



Step 10 If you replace the door, be sure to reattach the ground strap.

Stop. You have completed this procedure. Esitmated time of replacement by a skilled technician is 2 minutes.

NTP-C134 Reset Cards Using CTC

Purpose	This procedure resets a 15310-CL-CTX, CTX2500, electrical, or Ethernet card using soft and hard resets. A soft reset reboots the card and reloads the operating system and the application software. A hard reset temporarily removes power from the card and clears all buffer memory before it is physically reseated. (15310-CL-CTX cards cannot be physically reseated.)
Tools/Equipment	None
Prerequisite Procedures	Card installation procedure(s)
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Caution Do not soft reset more than one ONS 15310-MA card at a time. Instead, issue a soft reset command for a single card, then wait until CTC shows that the card is initialized. You can then issue a soft reset on another card if needed. Completing soft resets in sequence helps to avoid unexpected traffic hits.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node where you are performing the software reset. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-C218 Soft-Reset a 15310-CL-CTX or CTX2500 Card Using CTC" task on page 19-15.

Step 3 As needed, complete the "DLP-C219 Hard-Reset the 15310-CL-CTX or CTX2500 Card Using CTC" task on page 19-16.

Step 4 As needed, complete the "DLP-C220 Soft-Reset an Ethernet or Electrical Card Using CTC" task on page 19-17.

Step 5 As needed, complete the "DLP-C221 Hard-Reset an Ethernet or Electrical Card Using CTC" task on page 19-18.

Stop. You have completed this procedure.

NTP-C114 View the Loopback Status on a Port

Purpose	Use this task to view the loopback status on a selected ports.
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-C29 Log into CTC" task on page 17-44 at the node where you want to view the loopback status. If you are already logged in, continue with Step 2.

Step 2 In node view, double-click the card where you want to view the loopback status on a port. The card view displays.

Step 3 Depending on the port where the loopback is located, click one of the following tab sequences:

- Maintenance > DS1 > Loopback
- Maintenance > DS3 > Loopback
- Maintenance > EC1 > Loopback
- Maintenance > Optical > Loopback

The Number (#) and Service State columns identify the port number and current operating state (In-Service and Normal [IS-NR]; Out-of-Service and Management, Maintenance [OOS-MA,MT]; and Out-of-Service and Management, Disabled [OOS-MA,DSBLD]) of each port on the card. The Loopback Type column identifies the type of loopback (None, Terminal, or Facility) applied to each port on the card.

Stop. You have completed this procedure.

NTP-C115 Switch the Node Timing Reference

Purpose	This procedure switches the node timing reference to enable maintenance on a timing reference or to return the node timing to normal operation.
Tools/Equipment	None
Prerequisite Procedures	NTP-C23 Set Up Timing, page 4-11
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node that you want to monitor. If you are already logged in, continue with Step 2.

Step 2 As needed, use the following tasks to change the display of node timing maintenance information:

- DLP-C177 Manual or Force Switch the Node Timing Reference, page 18-71
- DLP-C178 Clear a Manual or Force Switched Node Timing Reference, page 18-71

Stop. You have completed this procedure.

NTP-C116 View the Timing Report

Purpose	This procedure displays the current status of the ONS 15310-CL or ONS 15310-MA timing references.
Tools/Equipment	None
Prerequisite Procedures	NTP-C23 Set Up Timing, page 4-11
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 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-C75 Display Alarms and Conditions Using Time Zone" task on page 17-93. Table 15-2 describes the report fields and entries.

Step 4 To update the report, click **Refresh**.

Table 15-2 ONS 15310-CL and ONS 15310-MA Timing Report

Item	Description	Options	Option Descriptions
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.

Table 15-2 ONS 15310-CL and ONS 15310-MA Timing Report (continued)

Item	Description	Options	Option Descriptions
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 15310-CL-CTX or CTX2500 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. Free-run 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 defaults 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 uses the same timing source as the NE. This appears when NE Reference is selected for BITS-1 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 state 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.
		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.	—	—
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 are available on the Provisioning > Timing tab.	The timing references are One and Two, which correspond to BITS-1, BITS-2, and Internal Clock respectively.

Table 15-2 ONS 15310-CL and ONS 15310-MA Timing Report (continued)

Item	Description	Options	Option Descriptions
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/DS-1	If the node is set to line timing, this is the OC-N or DS-1 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.
		LOS	Loss of signal; the reference is valid on a DS1, OC-3, or OC-12 facility used for timing.
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	Synchronization status messaging (SSM) is enabled.
		Disabled	SSM is not enabled.
SSM Quality	Indicates the SSM timing quality.	Eight to ten SSM quality messages can appear.	For a list of SSM message sets, refer to the "Timing" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA 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-C137 Edit Network Element Defaults

Purpose	This procedure explains how to edit factory-configured NE defaults using the NE Defaults editor. The new defaults can be applied only to the node on which they are edited. They can also be 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 15310-CL and Cisco ONS 15310-MA Reference Manual*. To change card settings individually (that is, without changing the defaults), see Chapter 10, "Change Port Settings." To change node settings, see Chapter 11, "Change Node Settings."

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 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 the defaults for a given card type from a node-level or CTC-level, you can drill down the Defaults Selector tree structure.

Step 4 Locate a default that 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 list (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.

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 Port 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.

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**.

Step 8 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**.

Stop. You have completed this procedure.

NTP-C138 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 NE defaults, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 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 navigate to the file that you are importing.

Step 5 When the correct file name and location appear in the dialog box (the correct file name is 15310-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 tests, 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 tests successfully.

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 pre-provisioned slots, see Chapter 10, "Change Port 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.

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**.

Step 9 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**.

Stop. You have completed this procedure.

NTP-C139 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	Retrieve or higher.

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-C29 Log into CTC" task on page 17-44 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.

CHAPTER 16

Power Down the Node

This chapter explains how to power down a Cisco ONS 15310-CL and Cisco ONS 15310-MA node and stop all node activity.

NTP-C120 Power Down the ONS 15310-CL and ONS 15310-MA

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, the Provisioning level or higher is required. For hardware steps, any level is allowed.

⚠ **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 15310-CL or ONS 15310-MA. Plug the wristband into the ESD jack located on left side of the chassis.

Step 1 Identify the node that you want to power down. If no cards are installed, go to Step 13. If a card is installed, log into the node. See the "DLP-C29 Log into CTC" task on page 17-44 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-C98 Remove a Path Protection Node" procedure on page 14-4 or the "NTP-C101 Remove an In-Service Node from a Linear ADM" procedure on page 14-9. Continue with Step 4.

b. If the node is not connected to a working network and the current configurations are no longer required, continue with Step 4.

Note Current configurations will be saved if Steps 4 through 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-C71 Modify and Delete Circuits" procedure on page 7-3 to delete all the circuits that originate or terminate in the node. Repeat until no circuits appear.

Step 5 Complete the "NTP-C143 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-C154 Delete a Section DCC Termination" task on page 18-56 or the "DLP-C155 Delete a Line DCC Termination" task on page 18-57 for all ports. Repeat until no SDCC or LDCC terminations exist.

Step 7 Complete the "DLP-C50 Change the Service State for a Port" task on page 17-67 to change all ports to the Out-of-Service and Management,Disabled (OOS-MA,DSBLD) service state.

Step 8 Remove all fiber connections to the cards.

Step 9 Complete the "DLP-C17 Remove SFP Connectors" task on page 17-23 if there are any SFPs installed.

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.

Step 13 Shut off the power from the power supply that feeds the node.

Step 14 Disconnect the node from its external fuse source.

Note For the AC version of ONS 15310-CL or ONS 15310-MA, unplug the chassis from the local AC power supply.

Step 15 Store all of the cards you removed and update inventory records according to local site practice.

Stop. You have completed this procedure.

CHAPTER 17

DLPs C1 to C99

DLP-C1 Unpack and Verify the Shelf Assembly

Purpose	This task removes the ONS 15310-CL or ONS 15310-MA 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 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 shelf assembly (wrapped in plastic) and a smaller box containing items needed for installation.

Step 3 To remove the shelf, grasp both sides of the shelf and slowly lift it out of the box.

Step 4 Open the smaller box containing installation materials, and verify that you have all items listed in the "Included Materials" section on page 1-3 (ONS 15310-CL) or "Included Materials" section on page 2-3 (ONS 15310-MA).

Step 5 Return to your originating procedure (NTP).

DLP-C2 Inspect the Shelf Assembly

Purpose	This task verifies that all parts of the ONS 15310-CL or ONS 15310-ma shelf assembly are in good condition.
Tools/Equipment	None
Prerequisite Procedures	DLP-C1 Unpack and Verify the Shelf Assembly, page 17-1
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify the following:

- Pins are not bent or broken
- Frame is not bent

Step 2 If the pins are bent or broken, or the frame is bent, call your Cisco sales engineer for a replacement.

Step 3 Return to your originating procedure (NTP).

DLP-C3 Mount the ONS 15310-CL in a Rack

Purpose	This task allows one person to mount the shelf assembly in a rack.
Tools/Equipment	Two sets of #12-24 mounting screws #2 Phillips screwdriver Fuse and alarm panel, if not installed (DC power only)
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Mounting the ONS 15310-CL in a rack requires a minimum of 2.75 inches of vertical rack space (plus 1 inch for air flow). To ensure the mounting is secure, use two #12-24 mounting screws for each side of the shelf assembly.

Step 1 If you will install DC power, 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 instructions. A fuse panel with two fuses per shelf (amperage depends on the fuse and alarm panel you are using) is required for Power A and B feeds.

Step 2 Install the appropriate bracket for the desired rack size (either 19 or 23 inches). Screw two screws through the bracket into the rack and 4 screws to adhere the bracket to the ONS 15310-CL chassis Figure 17-1 shows the mounting bracket orientations for a 19-inch rack.

Figure 17-1 Mounting Brackets (19-Inch Orientation)

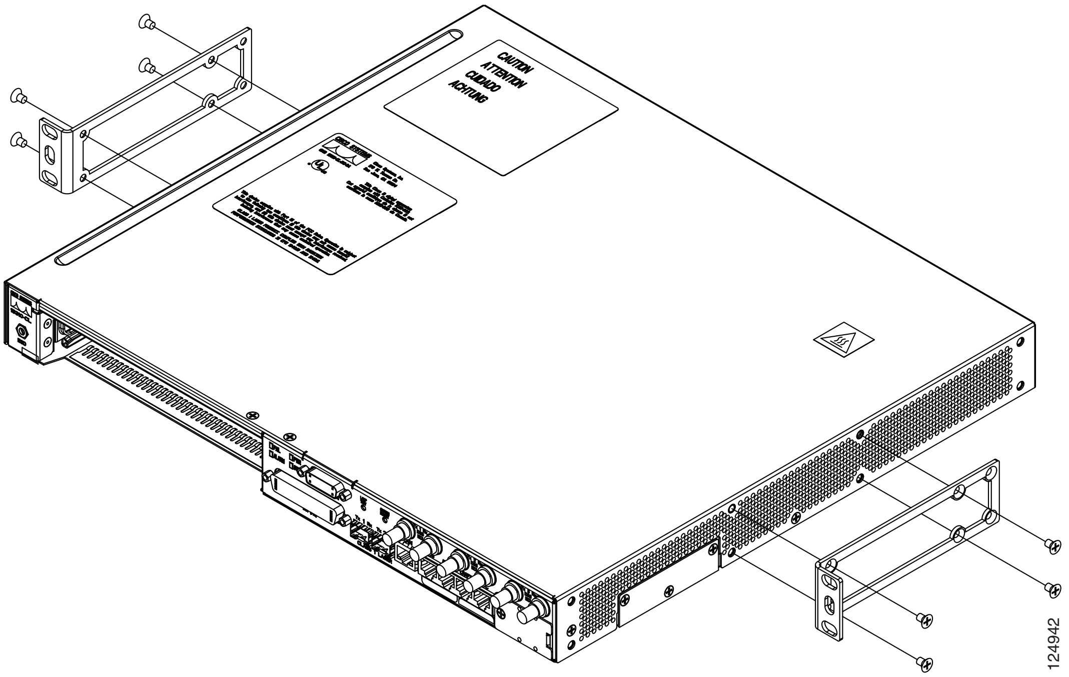
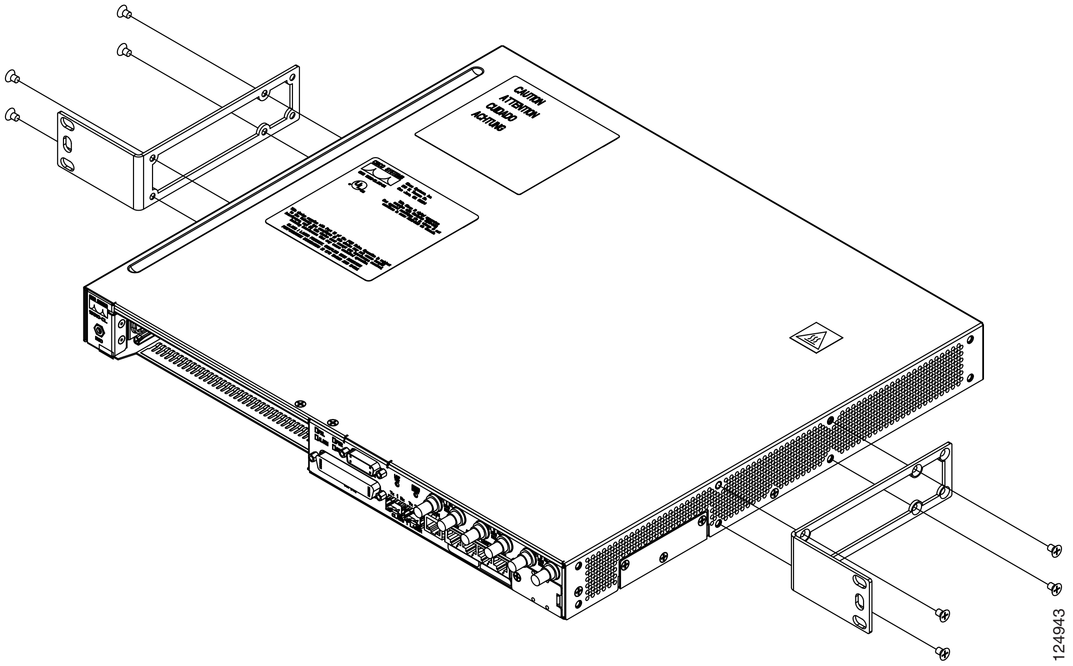


Figure 17-2 shows the mounting bracket orientations for a 23-inch rack. The brackets are installed in the same mounting holes.

Figure 17-2 Mounting Brackets (23-Inch Orientation)



Step 3 Lift the shelf assembly to the desired rack position and set it on the set screws.

Step 4 Align the screw holes on the mounting ears with the mounting holes in the rack.

Step 5 Using the Phillips screwdriver, install one mounting screw in each side of the assembly.

Step 6 When the shelf assembly is secured to the rack, install the remaining mounting screws.

Step 7 Return to your originating procedure (NTP).

DLP-C4 Mount Multiple ONS 15310-CL Shelf Assemblies in a Rack

Purpose	This task installs multiple ONS 15310-CL shelf assemblies in a 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

Step 1 If DC power will be applied, 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 instructions. A fuse panel with two 5-amp (minimum) fuses per shelf is required for Power A and B feeds.

Caution Maximum amp rating of the fuse is determined by the rated ampacity of the selected power cable (refer to manufacturer's instructions). The fuse rating should not exceed 20 amps.

Step 2 Mount the first ONS 15310-CL using the "DLP-C3 Mount the ONS 15310-CL in a Rack" task on page 17-2.

Note If you want to install a tie-down bar on the rack, be sure to leave 1 RU spacing between the ONS 15310-CL and any adjacent equipment you plan to install on the rack. This will provide adequate space for the tie-down bar and cabling.

Step 3 Repeat the task with the remaining ONS 15310-CL nodes.

Step 4 Return to your originating procedure (NTP).

DLP-C5 Connect the Office Ground to the ONS 15310-CL

Purpose	This task connects ground to the ONS 15310-CL shelf assembly.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Screws Ground cable, #6 AWG, copper conductors, 194°F [90°C]) #6 AWG dual-hole, 5/8 in.-spaced grounding lug 10-32 screws Crimp tool Wire strippers Wire cutter
Prerequisite Procedures	DLP-C3 Mount the ONS 15310-CL in a Rack, page 17-2
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify that the office ground cable (#6 AWG stranded) is connected to the top of the rack according to local site practice.

Note Additional ground cables may be added depending on the local site practice. The ONS 15310-CL is designated for a Common Bonding Network (CBN) only, according to definitions in section 9.3 of GR1089 issue 4.

Step 2 Ensure to remove paint and other nonconductive coatings from the surfaces between the shelf ground and the rack frame ground posts. Clean the mating surfaces and apply an appropriate antioxidant compound to the bare conductors.

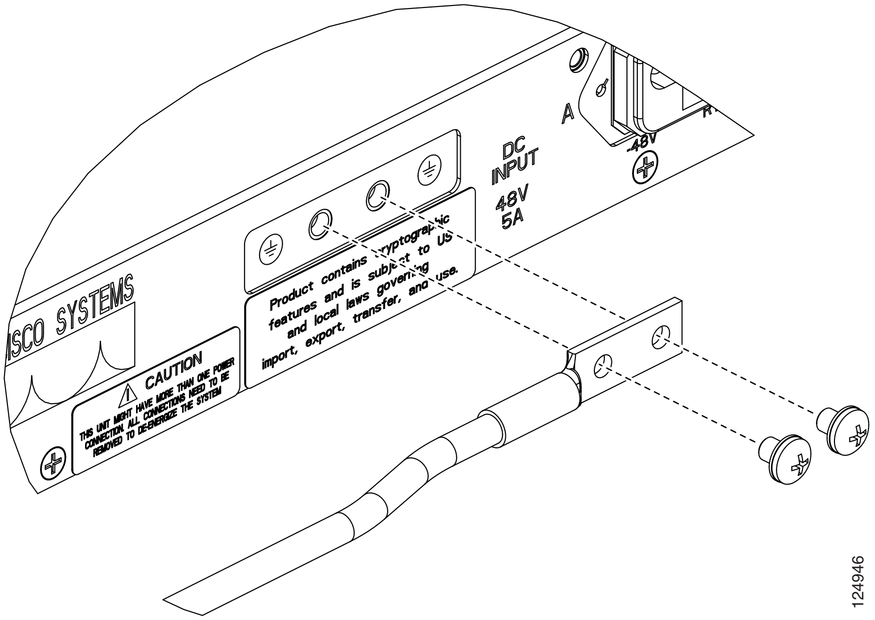
Step 3 Using the 10-32 screws that came with the ship kit, attach one end of the shelf ground cable (#6 AWG) to the ground connection point located on the center of the rear panel as you face the ONS 15310-CL.

Step 4 Using a wire stripper, strip 0.875 inches (2.22 cm) from the end of a #6 AWG ground cable.

Step 5 Crimp the two-hole lug to the #6 AWG ground cable.

Step 6 Line up the holes on the lug with the holes on the ground connection point, located at the center of the rear panel as you face the ONS 15310-CL. Use two 10-32 screws to attach the lug to the ground connection point (Figure 17-3).

Figure 17-3 Installing the Chassis Ground


ISCO SYSTEMS
CAUTION
THIS UNIT MIGHT HAVE MORE THAN ONE POWER CONNECTION. ALL CONNECTIONS NEED TO BE REMOVED TO DE-ENERGIZE THE SYSTEM
Product contains cryptographic features and is subject to US and local laws governing import, export, transfer, and use.
DC INPUT
48V
5A
A
-48V
124946

Step 7 Attach the other end of the shelf ground cable to the rack.

Step 8 Return to your originating procedure (NTP).

DLP-C6 Connect AC Office Power to the ONS 15310-CL

Purpose	This task connects AC power to the ONS 15310-CL shelf.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver AC power cord Strain-relief bracket
Prerequisite Procedures	DLP-C5 Connect the Office Ground to the ONS 15310-CL, page 17-5
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **Read the installation instructions before connecting the system to the power source.** Statement 1004

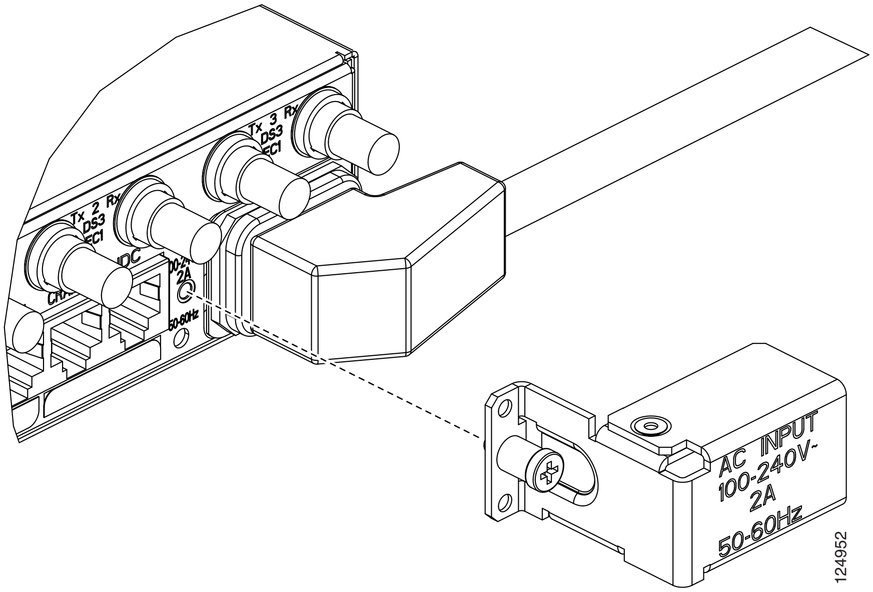
Warning **Use copper conductors only.** Statement 1025

Note If you encounter problems with the power supply, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

Step 1 Plug the AC power cord into the AC power connection on the front of the ONS 15310-CL.

Step 2 Install the strain-relief bracket over the power connector by using a Phillips screwdriver to screw the screw on the left of the bracket (Figure 17-4).

Figure 17-4 Installed AC Power and Strain Relief Bracket



Step 3 Return to your originating procedure (NTP).

DLP-C7 Connect DC Office Power to the ONS 15310-CL

Purpose	This task connects DC power to the ONS 15310-CL shelf.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Wire wrapper Wire cutters Wire strippers Hand crimper (Molex P/N 63811-1100) Fuse and alarm panel Connector housing (Cisco P/N 29-5116-01 or Molex P/N 50-29-1608) Connector terminal (Cisco P/N 27-1919-01 or Molex P/N 18-12-1602)) Power cable (from fuse and alarm panel to assembly), 14 AWG, stranded (41 strands, 0.010 in.) Listed pressure terminal connectors such as ring and fork types; 14 AWG, stranded (41 strands, 0.010 in.)
Prerequisite Procedures	DLP-C5 Connect the Office Ground to the ONS 15310-CL, page 17-5
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

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 in this manner, but always keep them clean and free of contaminants.

Note If you encounter problems with the power supply, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

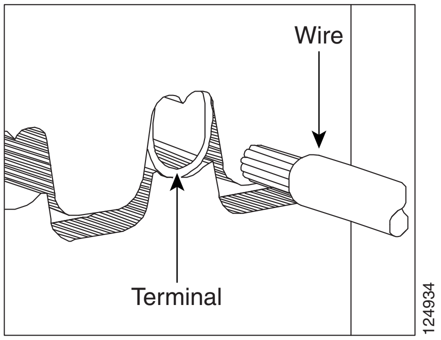
Step 1 Connect the office power according to the fuse panel engineering specifications.

Step 2 Measure and cut the cables as needed to reach the ONS 15310-CL from the fuse panel.

Step 3 Strip away 0.2 inches of insulation at one end of two 14 AWG wires.

Figure 17-5 shows the stripped 14 AWG wires.

Figure 17-5 Insulation Stripped from Wires



Step 4 Open the Molex crimping tool by squeezing the handles together. The ratchet mechanism will release the handles and the tool will open.

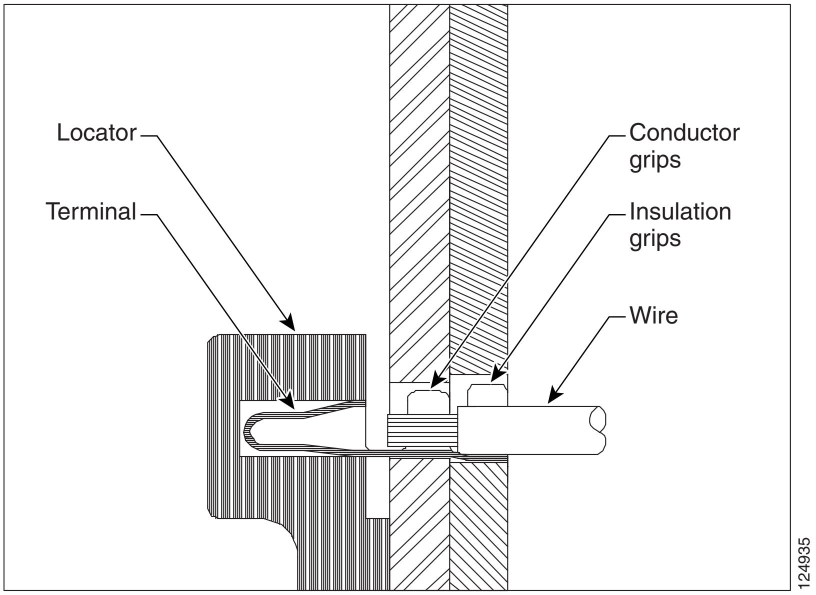
Step 5 Place the terminal into the correct die profile A until it is stopped by the locator.

Step 6 Partially close the tool until the terminal is held in place.

Step 7 Place a wire into the terminal and align the wire with the conductor and insulation grips.

Figure 17-6 shows the location of conductor and insulation grips.

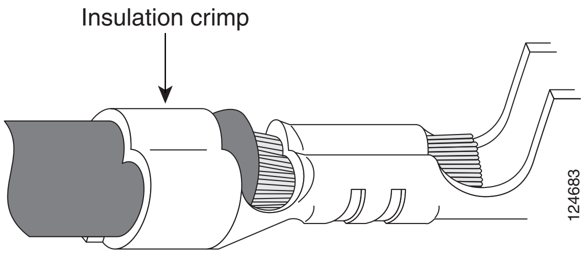
Figure 17-6 Crimping Tool



Step 8 Close the tool until the ratchet releases.

Figure 17-7 shows the terminal crimped to the power cable.

Figure 17-7 Terminal Connector Crimped to the Power Cable



Step 9 Carefully remove the crimped terminal.

Step 10 Insert crimped terminal into outside holes of the supplied 3-pin receptacle. Leave the center hole empty. The D-shaped terminal is for BAT (–48V). The O-shaped terminal on the other side of the connector is for RET.

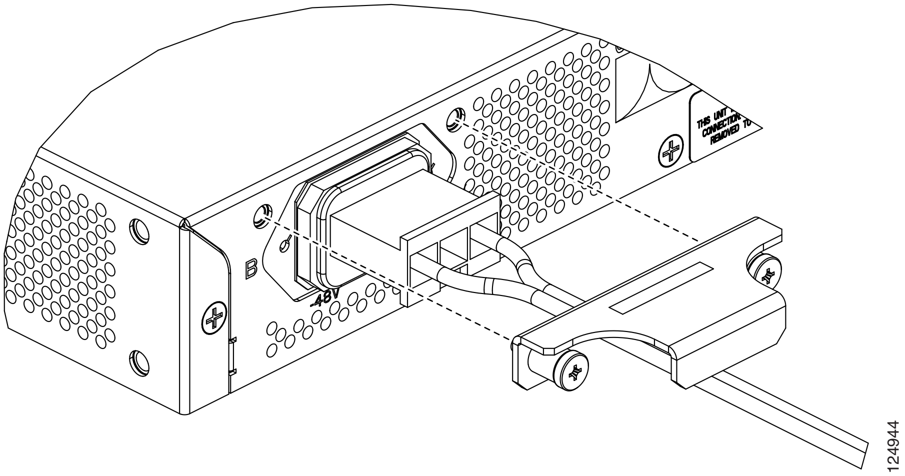
Note This power cable is suitable for maximum 5A, 60 VDC.

Note The battery return connection (+48Vdc) can be treated as DC-I , as defined in Telcordia GR-1089-CORE Issue 4. Connect the battery return (+48Vdc) to ground at the power source level.

Step 11 Plug the DC power connector into either plug on the rear of the chassis at the outside corners of the ONS 15310-CL.

Step 12 Install the strain-relief bracket over the power connector by using a Phillips screwdriver to screw the two screws at the top left and right of the bracket (Figure 17-8).

Figure 17-8 Installed DC Power and Strain Relief Bracket



Step 13 If you want to provide redundant power supplies, repeat for the other power plug. If not, install the solid metal bracket over the extra plug, using two screws to the top left and right of the plug.

Step 14 Return to your originating procedure (NTP).

DLP-C8 Turn On and Verify DC Office Power on the ONS 15310-CL

Purpose	This task verifies the ONS 15310-CL chassis LED activity and measures the DC power to verify correct power and returns.
Tools/Equipment	Voltmeter
Prerequisite Procedures	DLP-C5 Connect the Office Ground to the ONS 15310-CL, page 17-5 DLP-C7 Connect DC Office Power to the ONS 15310-CL, page 17-8
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 After applying power to the ONS 15310-CL chassis, verify the chassis LED activity (Figure 17-9 on page 17-12):

a. The FAIL LED blinks red for 20 to 30 seconds, then turns off.

b. The ALARM LED is off.

c. The PWR LED is green. (It is amber only if one DC power source is on and operating.)

d. The SYNC LED is green.

Step 2 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 -44 VDC and -52 VDC. Next, place the red test lead on the B-side connection and verify that it is between -44 VDC and -52 VDC.

Note The voltages -44 VDC and -52 VDC are the minimum and maximum voltages required to power the chassis. The nominal steady-state voltage is -48 VDC.

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. Place the red test lead on the B-side return ground and verify that no voltage is present.

Step 3 According to site practice insert a fuse into the fuse position.

Step 4 Using a voltmeter, verify the shelf for –48 VDC battery and ground:

a. To verify the A-side of the shelf, place the black lead of the voltmeter to the frame ground. Place the red test lead to the BAT1 (A-side battery connection) red cable. Verify that it reads between –44 VDC and –52 VDC. Then place the red test lead of the voltmeter to the RET1 (A-side return ground) black cable and verify that no voltage is present.

b. To verify the B-side of the shelf, place the black test lead of the voltmeter to the frame ground. Place the red test lead to the BAT2 (B-side battery connection) red cable. Verify that it reads between –44 VDC and -52 VDC. Then place the red test lead of the voltmeter to the RET2 (B-side return ground) black cable and verify that no voltage is present.

Step 5 Return to your originating procedure (NTP).

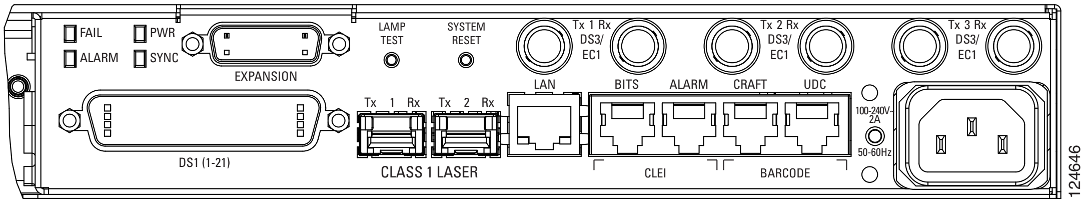
DLP-C9 Install External Alarm Cables on the ONS 15310-CL

Purpose	This task installs alarm cables on the ONS 15310-CL so that you can provision external (environmental) alarms and controls.
Tools/Equipment	Alarm cable, CAT-5 terminated with RJ-45 for all alarm connections
Prerequisite Procedures	NTP-C2 Install the Shelf Assembly, page 1-4
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the alarm cable into the ALARM port on the front of the ONS 15310-CL.

Figure 17-9 shows the connectors located on the front panel of the ONS 15310-CL.

Figure 17-9 ONS 15310-CL Front Panel



Step 2 Plug the other end of the cable into the alarm-collection equipment according to local site practice.

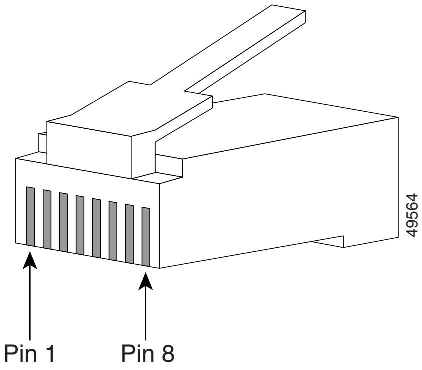
Step 3 To define the six external alarm inputs and two external alarm outputs using CTC, see the "NTP-C63 Provision External Alarms and Controls" procedure on page 9-8. Table 17-1 shows the default input alarm pinouts and the corresponding alarm numbers assigned to each port. Refer to this table when connecting alarm cables to the ONS 15310-CL.

Table 17-1 Default Alarm Pin Assignments

RJ-45 Pin Number	Function
1	Alarm Contact 1+
2	Alarm Contact 1–
3	Alarm Contact 2+
4	Alarm Contact 2–
5	Alarm Input 1
6	Alarm Input 2
7	Alarm Input 3
8	Common (DC power return)

Figure 17-10 shows RJ-45 pin numbering.

Figure 17-10 Pins 1 and 8 on the RJ-45 Connector



Step 4 Return to your originating procedure (NTP).

DLP-C10 Install Timing Cables on the ONS 15310-CL

Purpose	This task installs timing cables so that you can provide BITS timing to the ONS 15310-CL.
Tools/Equipment	Timing cable, CAT-5 RJ-45 connector
Prerequisite Procedures	NTP-C2 Install the Shelf Assembly, page 1-4
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the timing cable into the BITS port on the front of the 15310-CL (Figure 17-9 on page 17-12).

Step 2 Plug the other end of the cable into the BITS clock according to local site practice. Table 17-2 shows the BITS cable pin assignments.

Table 17-2 BITS Cable Pin Assignments

RJ-45 Pin Number	Function
1	BITS Output+
2	BITS Output–
3	BITS Input+
4	—
5	—
6	BITS Input–

Table 17-2 BITS Cable Pin Assignments (continued)

RJ-45 Pin Number	Function
7	—
8	—

Figure 17-11 shows the BITS IN pins on the RJ-45 connector.

Figure 17-11 BITS In Pins on the RJ-45 Connector

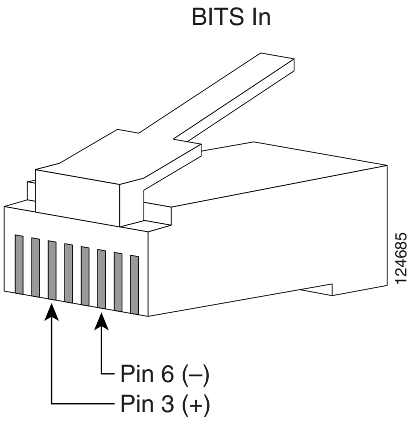
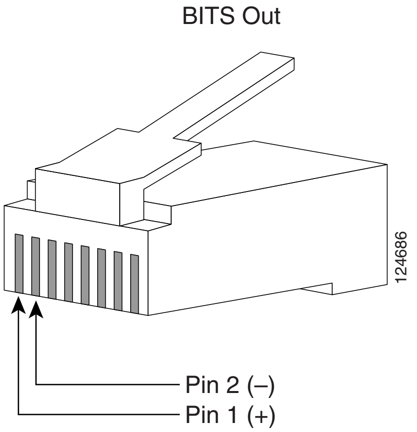


Figure 17-12 shows the BITS out pins on the RJ-45 connector.

Figure 17-12 BITS Out Pins on the RJ-45 Connector



Note For more detailed information about timing, refer to the "Timing" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual.* To set up system timing, see the "NTP-C23 Set Up Timing" procedure on page 4-11.

Step 3 Return to your originating procedure (NTP).

DLP-C11 Install the Serial Cable for an ONS 15310-CL TL1 Craft Interface

Purpose	This task installs the TL1 craft interface cable on an ONS 15310-CL.
Tools/Equipment	CAT-5 RJ-45 cable
Prerequisite Procedures	NTP-C2 Install the Shelf Assembly, page 1-4
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the TL1 cable into the CRAFT port on the front of the ONS 15310-CL (Figure 17-9 on page 17-12).

Step 2 Connect the other end to the PC you want to use to access the craft.

Table 17-3 shows the serial cable pin assignments.

Table 17-3 TL1 Serial Cable Pin Assignments

RJ-45 Pin Number	Function
1	RTS
2	DTR
3	TXD
4	GND
5	GND
6	RXD
7	DSR
8	CTS

Step 3 Return to your originating procedure (NTP).

DLP-C12 Install the UDC Cable on the ONS 15310-CL

Purpose	This task installs the user data channel (UDC) cable on the ONS 15310-CL. A UDC circuit allows you to create a dedicated data channel between nodes.
Tools/Equipment	CAT-5 RJ-45 cable
Prerequisite Procedures	NTP-C2 Install the Shelf Assembly, page 1-4

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

Step 1 Plug one end of the UDC cable into the UDC port on the front of the 15310-CL (Figure 17-9 on page 17-12).

Step 2 Connect the other end to terminating equipment, such as a 64-Kbps codirectional G.703 equipment interface or a RS-232-compliant equipment.

Table 17-4 shows the serial cable pin assignments.

Table 17-4 UDC Cable Pin Assignments

RJ-45 Pin Number	RS-232 Mode	64K Mode
1	NC	TX +
2	DTR	TX –
3	TXD	RX +
4	GND	GND
5	GND	GND
6	RXD	RX –
7	NC	NC
8	NC	NC

Step 3 Return to your originating procedure (NTP).

DLP-C13 Install LFH Cables for ONS 15310-CL DS-1 Connections

Purpose	This task installs DS-1 cables on the ONS 15310-CL.
Tools/Equipment	96-pin LFH connector terminated to a 21-pair #26 AWG cable
Prerequisite Procedures	NTP-C5 Install Wires to Alarm, Timing, LAN, Craft, and UDC Pin Connections, page 1-9
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

⚠ **Caution** Always use the supplied ESD wristband when working with a powered ONS 15310-CL. Plug the wristband cable into the ESD jack located to the left of the expansion slot.

Step 1 Prepare a 96-pin LFH connector terminated to a 21-pair #26 AWG cable.

Step 2 See Table 17-5 for the ONS 15310-CL connector pin assignments.

Note Refer to the "Cisco ONS 15310-CL Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for specific information on DS-1 cables and DS-1 connectors, including product numbers and compatibility.

Table 17-5 DS1 Connector Pin Assignments

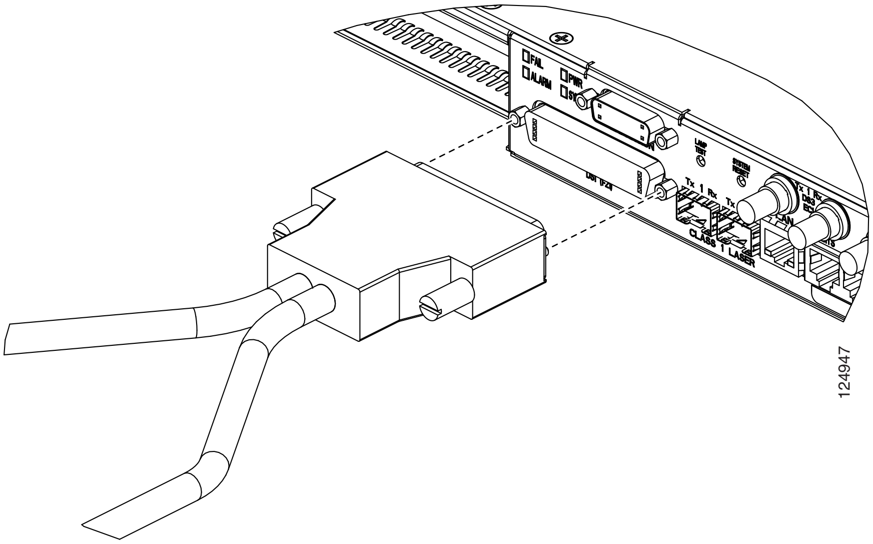
Pin	Transmit Cable Signal Connection	Conductor Color	Pin	Receive Cable Signal Connection	Conductor Color
1	TX11-	blue-black	49	TX21-	blue-violet
2	TX11+	black-blue	50	TX21+	violet-blue
3	TX10-	gray-red	51	TX20-	gray-yellow
4	TX10+	red-gray	52	TX20+	yellow-gray
5	TX9-	brown-red	53	TX19-	brown-yellow
6	TX9+	red-brown	54	TX19+	yellow-brown
7	TX8-	green-red	55	TX18-	green-yellow
8	TX8+	red-green	56	TX18+	yellow-green
9	TX7-	orange-red	57	TX17-	orange-yellow
10	TX7+	red-orange	58	TX17+	yellow-orange
11	TX6-	blue-red	59	TX16-	blue-yellow
12	TX6+	red-blue	60	TX16+	yellow-blue
13	TX5-	gray-white	61	TX15-	gray-black
14	TX5+	white-gray	62	TX15+	black-gray
15	TX4-	brown-white	63	TX14-	brown-black
16	TX4+	white-brown	64	TX14+	black-brown
17	TX3-	green-white	65	TX13-	green-black
18	TX3+	white-green	66	TX13+	black-green
19	TX2-	orange-white	67	TX12-	orange-black
20	TX2+	white-orange	68	TX12+	black-orange
21	TX1-	blue-white	69	Unused	—
22	TX1+	white-blue	70	Unused	—
23	Unused	—	71	Unused	—
24	Unused	—	72	Unused	—
25	RX11-	blue-black	73	RX21-	blue-violet
26	RX11+	black-blue	74	RX21+	violet-blue
27	RX10-	gray-red	75	RX20-	gray-yellow
28	RX10+	red-gray	76	RX20+	yellow-gray
29	RX9-	brown-red	77	RX19-	brown-yellow
30	RX9+	red-brown	78	RX19+	yellow-brown
31	RX8-	green-red	79	RX18-	green-yellow

Table 17-5 DS1 Connector Pin Assignments (continued)

Pin	Transmit Cable Signal Connection	Conductor Color	Pin	Receive Cable Signal Connection	Conductor Color
32	RX8+	red-green	80	RX18+	yellow-green
33	RX7-	orange-red	81	RX17-	orange-yellow
34	RX7+	red-orange	82	RX17+	yellow-orange
35	RX6-	blue-red	83	RX16-	blue-yellow
36	RX6+	red-blue	84	RX16+	yellow-blue
37	RX5-	gray-white	85	RX15-	gray-black
38	RX5+	white-gray	86	RX15+	black-gray
39	RX4-	brown-white	87	RX14-	brown-black
40	RX4+	white-brown	88	RX14+	black-brown
41	RX3-	green-white	89	RX13-	green-black
42	RX3+	white-green	90	RX13+	black-green
43	RX2-	orange-white	91	RX12-	orange-black
44	RX2+	white-orange	92	RX12+	black-orange
45	RX1-	blue-white	93	Unused	—
46	RX1+	white-blue	94	Unused	—
47	Unused	—	95	Unused	—
48	Unused	—	96	Unused	—

Step 3 Connect the male connector on the cable to the female connector at the center of the front of the ONS 15310-CL (Figure 17-13).

Figure 17-13 Installing the DS-1 Cable



Step 4 Tighten the two thumbscrews on the male connector.

Step 5 Return to your originating procedure (NTP).

DLP-C14 Install DS-3/EC-1 Cables With MiniBNC Connectors on the ONS 15310-CL

Purpose	This task installs the DS-3/EC-1 cables to connect DS-3/EC-1 signals to the ONS 15310-CL. The DS-3/EC-1 cables should be terminated with miniBNC connectors on the ONS 15310-CL side and BNC connectors on the client side.
Tools/Equipment	Shielded coaxial cable terminated with miniBNC connectors for DS-3/EC-1 ports
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

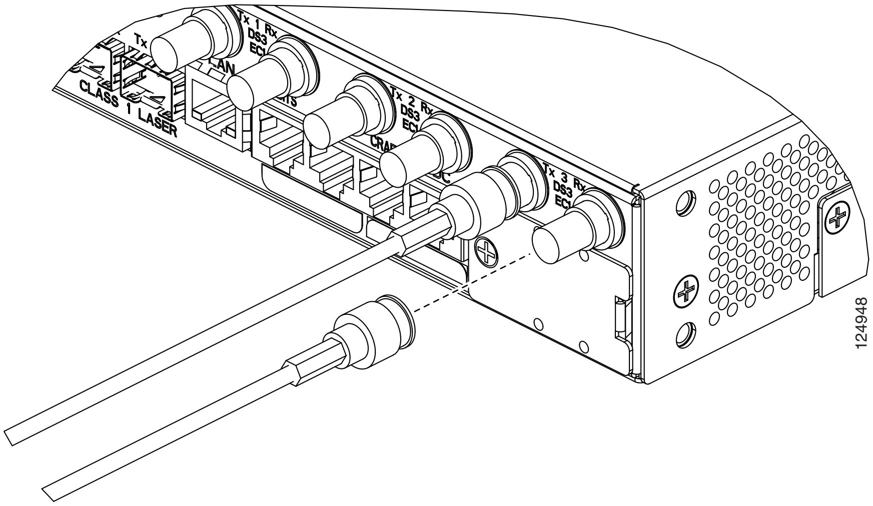
Caution Always use the supplied ESD wristband when working with a powered ONS 15310-CL. Plug the wristband cable into the ESD jack located to the left of the expansion slot.

Note Cisco recommends you use Cisco-orderable miniBNC cables to ensure interoperability between the cables and miniBNC connectors on the ONS 15310-CL.

Step 1 Place a miniBNC cable connector over the connector on the front of the ONS 15310-CL.

Figure 17-14 shows how to connect a coaxial cable to an ONS 15310-CL.

Figure 17-14 Installing a DS-3/EC-1 Cable with MiniBNC Connectors



Step 2 Position the cable connector so that the slot in the connector is above the corresponding notch on the ONS 15310-CL connection point.

Step 3 Gently push the connector down until the notch on the ONS 15310-CL connector slides into the slot on the cable connector.

Step 4 Turn the cable connector until the notch clicks into place.

Step 5 Return to your originating procedure (NTP).

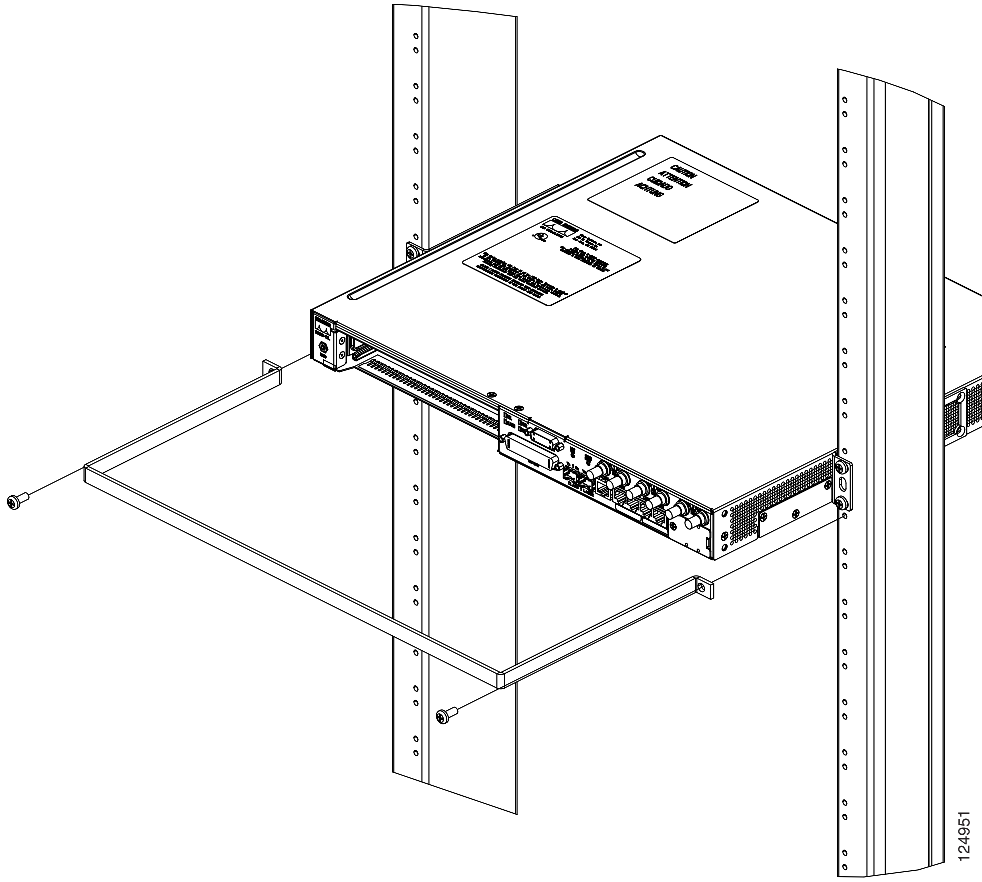
DLP-C15 Route Cables on the ONS 15310-CL

Purpose	This task routes electrical, optical, alarm, and timing cables away from the ONS 15310-CL. You can install optional tie-bars specifically designed for the ONS 15310-CL.
Tools/Equipment	Tie-wraps or other securing devices, according to local practice Tie-bar(s) (15310-TIE-BAR-19; 15310-TIE-BAR-23)
Prerequisite Procedures	NTP-C6 Install the Electrical Cables, page 1-10 NTP-C8 Install Optical Cables, page 1-12 NTP-C5 Install Wires to Alarm, Timing, LAN, Craft, and UDC Pin Connections, page 1-9
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 As needed, install a tie-bar or other strain-relief device, according to local site practice.

Figure 17-15 shows how to install a tie-bar on an ONS 15310-CL rack.

Figure 17-15 Installing a Tie-Bar



Caution You must provide some type of strain-relief for the ONS 15310-CL cabling.

Step 2 Route the cables to the right side of the shelf assembly according to local site practice, avoiding blocking the front of the expansion card.

Step 3 Secure the cables to the strain-relief device using tie-wraps or other site-specific methods.

Step 4 Label all cables at each end of the connection to avoid confusion with cables that are similar in appearance.

Step 5 Return to your originating procedure (NTP).

DLP-C16 Install SFP Connectors

Purpose	This task installs OC-3, OC-12, OC-48, or OC-3/OC-12 (multirate) Small Form-factor Pluggables (SFPs). SFPs are hot-swappable input/output devices that plug into SFP slots on the ONS 15310-CL or ONS 15310-MA faceplate to link the port to the fiber-optic network.
Tools/Equipment	SFPs compatible with the ONS 15310-CL or ONS 15310-MA
Prerequisite Procedures	NTP-C2 Install the Shelf Assembly, page 1-4 NTP-C3 Install the Power and Ground, page 1-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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**

Warning **Class 1 laser product.** Statement 1008

Note SFPs are hot-swappable and can therefore be installed and removed while the card/shelf assembly is powered and running.

Note SFPs are generically called pluggable port modules (PPMs) in CTC. After installing the SFP, multirate PPMs must be provisioned in CTC. See the "NTP-C130 Manage Pluggable Port Modules" procedure on page 10-3.

Step 1 Verify that the SFP is correct for your network. Refer to the "Card Reference" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for card compatibility and SFP information.

Step 2 Remove the SFP from its protective packaging.

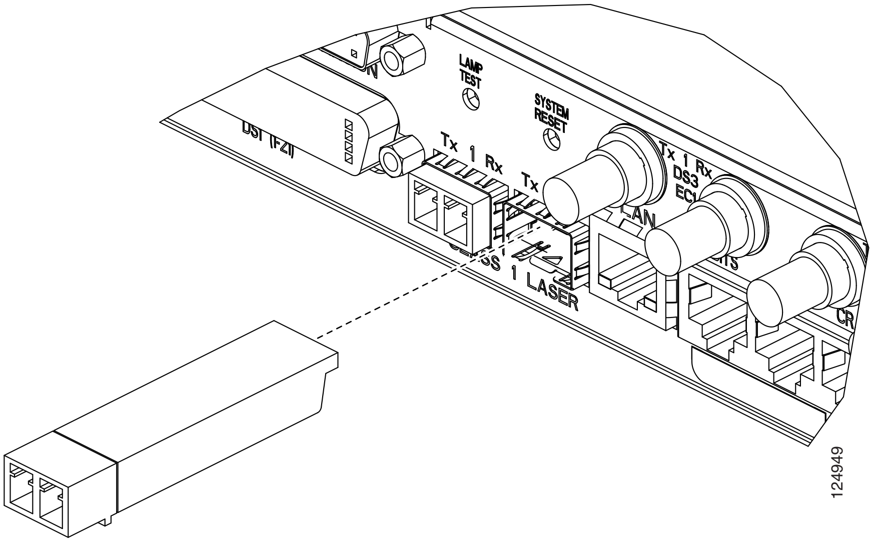
Step 3 Orient the SFP so that the Cisco serial number label is facing away from the shelf (to the right).

Step 4 Move the bail clasp to the left to unlatch it before inserting it into the slot.

Step 5 Slide the SFP into the slot and move the bail clasp to the right to secure the SFP.

Figure 17-16 shows SFP installation on the ONS 15310-CL. (Installation on the ONS 15310-MA is similar. SFPs are installed on the faceplate of the CTX2500 card.)

Figure 17-16 Installing the SFP on the ONS 15310-CL



Caution Do not remove the protective caps until you are ready to attach the network fiber-optic cable.

Note You must set the normalized optical power received (OPR) value whenever you replace or insert an SFP. After you click Set for the port you are observing, the LBC (%), OPR (%), and OPT (%) values under the Performance > Optical tabs should be close to 100 percent. Only Cisco-approved SFPs should be used. See the "NTP-C87 Modify Line Settings and PM Parameter Thresholds for Optical Ports" procedure on page 10-2 for more information about changing optical port settings, and the "NTP-C66 Monitor Optical Performance" procedure on page 8-4 for more information about viewing performance monitoring parameters.

Step 6 Return to your originating procedure (NTP).

DLP-C17 Remove SFP Connectors

Purpose	This task disconnects fiber attached to an SFP and removes the SFP.
Tools/Equipment	None
Prerequisite Procedures	DLP-C16 Install SFP Connectors, page 17-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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 1 Disconnect the network fiber cable from the SFP connector. Squeeze the sides of the fiber cable firmly to unlatch it.

Step 2 Pull the bail clasp to the left to release the SFP.

Step 3 Slide the SFP out of the slot.

Step 4 Return to your originating procedure (NTP).

DLP-C18 Install Fiber-Optic Cables in a 1+1 Configuration

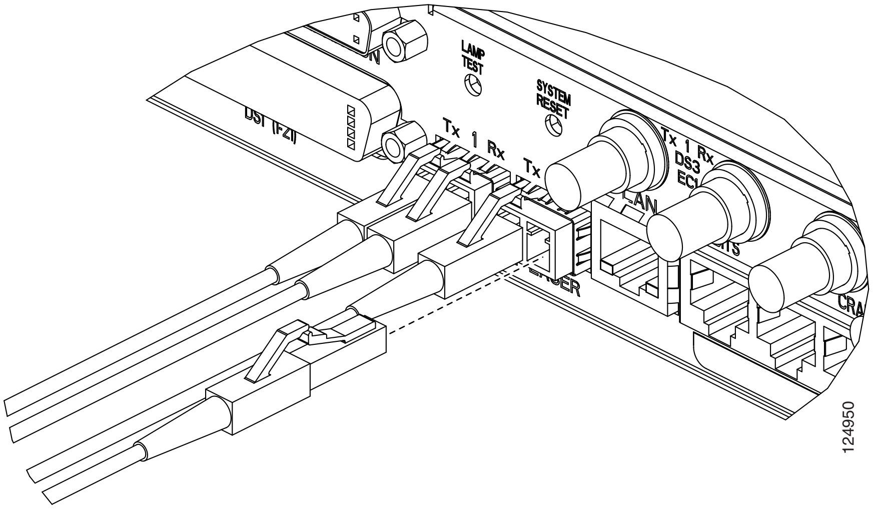
Purpose	This task installs fiber-optic cables on optical (OC-N) ports in a 1+1 linear configuration.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-C109 Clean Fiber Connectors, page 15-10
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note On ONS 15310-CL optical ports, the left connector is the transmit port and the right connector is the receive port. On ONS 15310-MA ports, the transmit and receive fiber for each optical signal are contained within a single SFP port.

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 port at one node (Figure 17-17) and plug the other end of the fiber into the receive (Rx) connector of a working OC-N port at the adjacent node. The card displays an SF LED if the transmit and receive fibers are mismatched (one fiber connects a receive port to a receive port, or a transmit port to a transmit port).

Figure 17-17 Installing an Optical Cable in the ONS 15310-CL



Step 3 Repeat Steps 1 and 2 for the corresponding protect ports on the two nodes and all other working/protect port pairs you want to place in a 1+1 configuration.

Step 4 Return to your originating procedure (NTP).

DLP-C19 Install Fiber-Optic Cables for Path Protection Configurations

Purpose	This task installs 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-C109 Clean Fiber Connectors, page 15-10
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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

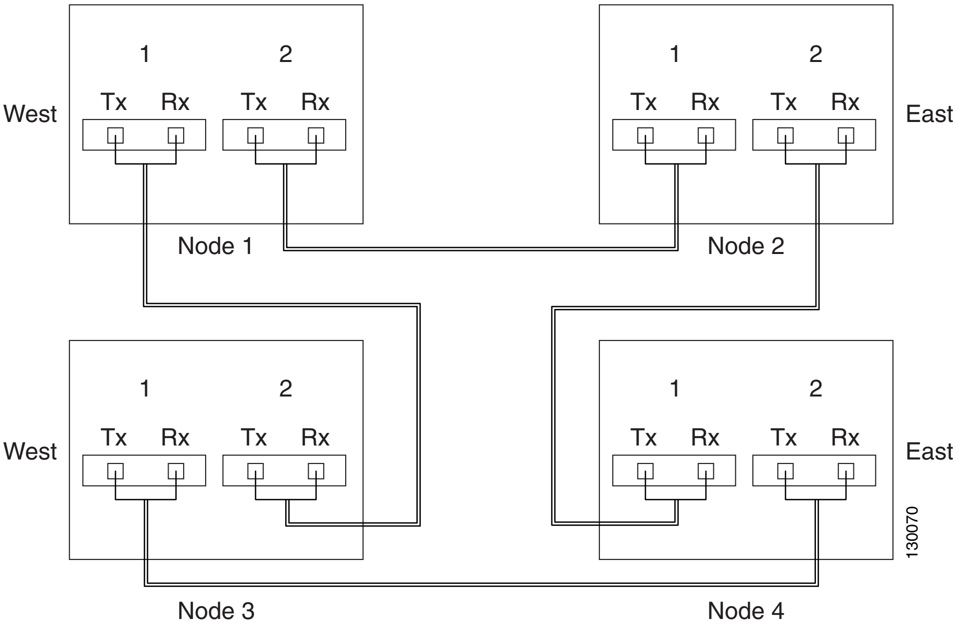
Step 1 Plan your fiber connections. Use the same plan for all path protection nodes.

Step 2 Plug the fiber into the Tx port at one node and plug the other end of the fiber into the Rx port at the adjacent node. The card will display a signal fail (SF) LED if the transmit and receive fibers are mismatched (for example, one fiber connects a receive port to a receive port, or a transmit port to a transmit port).

Step 3 Repeat Step 2 until you have configured the entire ring.

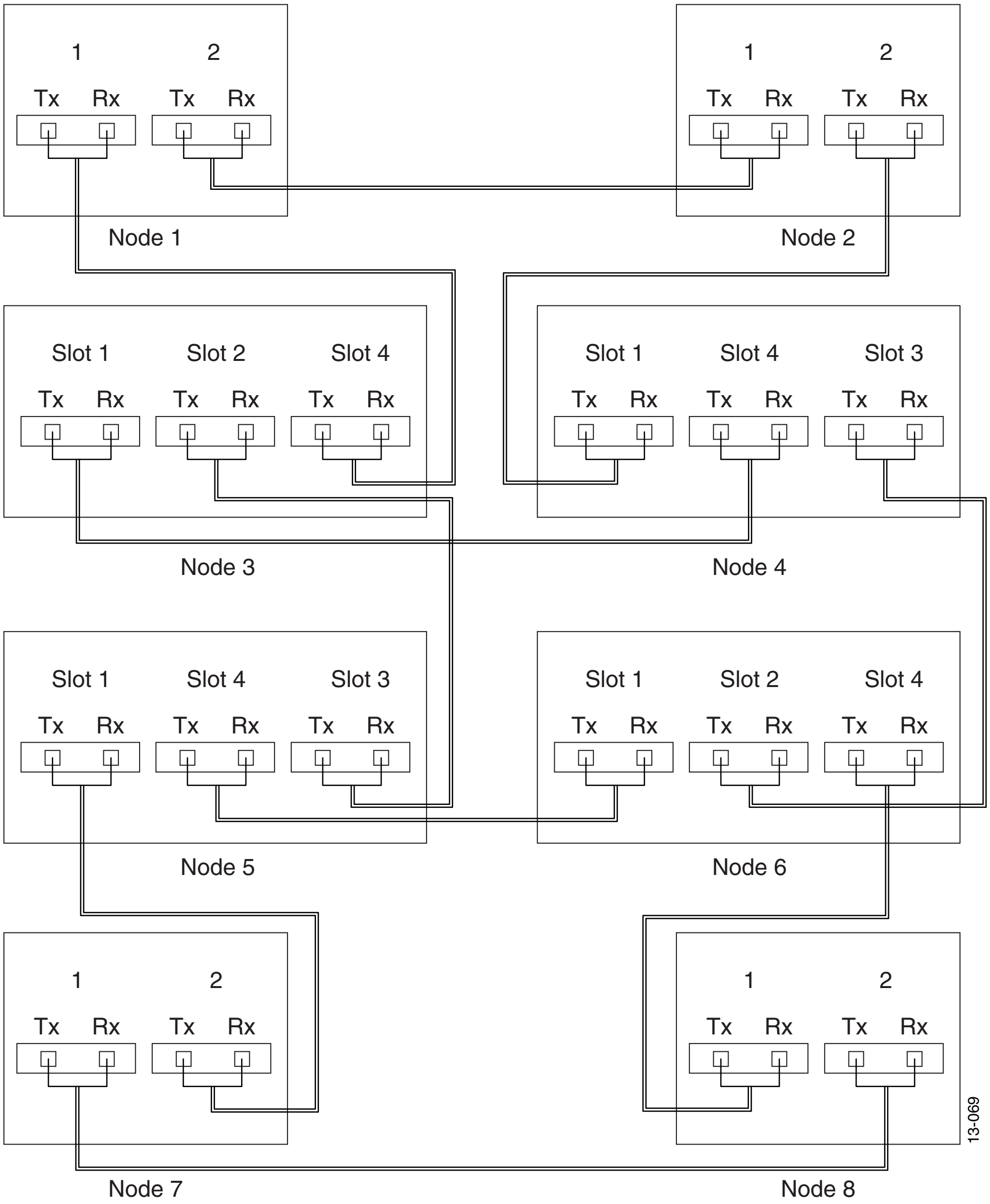
Figure 17-18 shows fiber connections for a four-node path protection with trunk (span) cards in Slot 5 (west) and Slot 12 (east).

Figure 17-18 Connecting Fiber to a Four-Node Path Protection Configuration



If you are creating a path protection dual-ring interconnect (DRI), Figure 17-19 shows a traditional DRI example. Because the ONS 15310-CL has only two optical ports, in Figure 17-19 it can be represented by Nodes 1, 2, 7, or 8. Nodes 3, 4, 5, and 6 must represent other terminating equipment, such as the ONS 15310-MA, ONS 15327, ONS 15454, or ONS 15600.

Figure 17-19 Connecting Fiber to an Eight-Node Traditional Path Protection DRI



Step 4 Return to your originating procedure (NTP).

DLP-C20 Measure Voltage

Purpose	This task measures power so you can verify correct power and returns.
Tools/Equipment	Voltmeter
Prerequisite Procedures	NTP-C3 Install the Power and Ground, page 1-5 or NTP-C151 Install the Power and Ground, page 2-12 Table 1-2 on page 1-17 or Table 2-2 on page 2-30
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Using a voltmeter, verify the office ground and power shows the power terminals:

a. Place the black lead (positive) on the frame ground on the rack. 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 –44 VDC and –52 VDC (power) and 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 –44 VDC and –52 VDC. If there is no voltage, check the following:

- Battery and ground 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-C21 Run the CTC Installation Wizard for Windows

Purpose	This task installs the CTC online user manuals, Acrobat Reader 6.0.1, JRE 5.0, and the CTC JAR (Java Archive) files. JRE 5.0 is required to run Release 8.5. The CTC JAR files contain the ONS 15310-CL and ONS 15310-MA client software. CTC JAR files are normally downloaded from the ONS 15310-CL or ONS 15310-MA the first time you log in. Pre-installing the JAR files saves time at initial login. It also allows you to log into ONS 15454s running earlier CTC software releases to manage ONS 15310-CL or ONS 15310-MA nodes that are connected to the ONS 15454 network.
Tools/Equipment	Cisco ONS 15310-CL System Software CD, Version 8.5 or Cisco ONS 15310-MA System Software CD, Version 8.5
Prerequisite Procedures	None
Required/As Needed	This task is required if any one of the following is true: • JRE 5.0 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

Step 1 Verify that your computer has the following:

- Processor—Pentium III, 700 Mhz or faster
- RAM—384 MB recommended, 512 MB optimum
- Hard drive—20 GB hard drive recommended with at least 50 MB of space available
- Operating system—Windows 98 (1st and 2nd editions), Windows NT 4.0 (with Service Pack 6a), Windows 2000 (with Service Pack 3), or Windows XP Home

  If your operating system is Windows NT 4.0, verify that Service Pack 6a or later is installed. From the 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. If your operating system is Windows Vista please complete DLP-C276 Configuring Windows Vista to Support CTC, page 19-91 before proceeding further.
- Processor and RAM requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM.

Step 2 Insert the software CD into your computer CD drive. The installation program begins running automatically. If it does not start, navigate to your computer's 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 1.4.2
- Acrobat Reader 6.0.1
- Online User Manuals
- CTC JAR files

Note If you use the delete CTC cache function at any later time, the JAR files will be removed. You must complete this task again to re-install the JAR files.

Note You can also install the JAR files by starting a command prompt session, changing to the CD directory, and typing **Run java -jar LDCACHE.jar**.

Step 3 Click **Next**.

Step 4 Complete one of the following:

- Click **Typical** to install all three components. If you already have JRE version 5.0 installed on your computer, choose Custom.
- Click **Custom** if you want to install either the JRE or the online user manuals.

Step 5 Click **Next**.

Step 6 Complete the following, as applicable:

- If you selected Typical, skip this step and continue with Step 7.
- If you selected Custom in Step 4, check the CTC component that you want to install and click **Next**.
  - If you selected Online User Manuals, continue with Step 7.
  - If you did not select Online User Manuals, continue with Step 9.

Step 7 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 8 Click **Next**.

Step 9 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 4, click **Back** twice to return to the installation setup type page. Choose **Custom** and repeat Steps 5 through 8.
- If you selected Custom in Step 4, click **Back** once or twice (depending on the components selected) until the component selection page appears. Repeat Steps 6 through 8.

Step 10 Click **Next**. It may take a few minutes for the JRE installation wizard to appear. If you selected Custom in Step 4 need to install the JRE, continue with Step 12.

Step 11 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 12.

Note If JRE 5.0 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 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 may cause problems with these browsers.

h. Click **Next**.

i. Click **Finish**.

Note If you are uninstalling the JRE, click Remove.

Step 12 In the Cisco Transport Controller Installation Wizard, click **Next**. The online user manuals install.

Step 13 Click **Finish**.

Step 14 Return to your originating procedure (NTP).

DLP-C22 Run the CTC Installation Wizard for UNIX

Purpose	This task installs the CTC online user manuals, Acrobat Reader 6.0.1, JRE 5.0, and the CTC JAR (Java Archive) files. JRE 5.0 is required to run Software Release 8.5. The CTC JAR files contain the ONS 15310-CL and ONS 15310-MA client software. CTC JAR files are normally downloaded from the ONS 15310-CL or ONS 15310-MA the first time you log in. Pre-installing the JAR files saves time at initial login. It also allows you to log into ONS 15454s running earlier CTC software releases to manage ONS 15310-CL or ONS 15310-MA nodes that are connected to the ONS 15454 network.
Tools/Equipment	Cisco ONS 15310-CL System Software CD, Version 8.5.x or Cisco ONS 15310-MA System Software CD, Version 8.5.x
Prerequisite Procedures	None
Required/As Needed	Required if any of the following are true: • JRE 5.0 is not installed. • CTC online user manuals are not installed and are needed.
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Verify that your computer has the following:

- RAM—384 MB recommended, 512 MB optimum
- Hard drive—20 GB hard drive recommended with at least 50 MB of space available
- 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 techdoc310 CD directory, type:

./setup.bat

The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer:

- Java Runtime Environment 1.4.2
- Acrobat Reader 6.0.1
- Online User Manuals
- CTC JAR files

Note If you use the delete CTC cache function at any later time, the JAR files will be removed. You must complete this task again to re-install the JAR files.

Note You can also install the JAR files by starting a command prompt session, changing to the CD directory, and typing **Run java -jar LDCACHE.jar**.

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 version 5.0 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, continue with Step 8.
- If you selected Custom in Step 5, check the CTC component that you want to install and click **Next**. If you will ever need to log into a node running an ONS release earlier than Software Release 5.0, uncheck Java Runtime Environment 1.4.2.
  - 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 may take a few minutes for the JRE installation wizard to appear. If you selected Custom in Step 4 and 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 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 1.4.2 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 may cause problems with these browsers.

h. Click **Next**.

i. Click **Finish**.

Note 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-C23 Set Up a Windows PC for Craft Connection to an ONS 15310-CL or ONS 15310-MA on the Same Subnet Using Static IP Addresses

Purpose	This task sets up your computer for a local craft connection to the ONS 15310-CL when: • You will connect to one ONS 15310-CL or ONS 15310-MA; if you will connect to multiple nodes, you might need to reconfigure your computer's IP settings each time you connect to a node. • You need to use non-ONS 15310-CL or 15310-MA applications such as ping and tracert (trace route).
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
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, select **TCP/IP** for your PC Ethernet 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 15310-CL/ONS 15310-MA IP address except for the last octet. For example, if the node IP address is 209.165.201.30, your IP address must be 209.165.201.xxx, where xxx is any number up to 255 excluding 30, which is used in the node IP address.

i. In the Subnet Mask field, type the same subnet mask as the ONS 15310-CL or ONS 15310-MA. 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 15310-CL/ONS 15310-MA 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 15310-CL/ONS 15310-MA IP address except for the last octet. The last octet must be 1 or 3 through 254.

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 15310-CL/ONS 15310-MA 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 current node ONS 15310-CL/ONS 15310-MA IP address except for the last octet. The last octet must be 1 or 3 through 254.

f. In the Subnet Mask field, type **255.255.255.0**.

g. In the Default Gateway field, type the ONS 15310-CL/ONS 15310-MA 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 15310-CL/ONS 15310-MA IP address except for the last octet. The last octet must be 1 or 3 through 254.

e. In the Subnet Mask field, type **255.255.255.0**.

f. In the Default Gateway field, type the ONS 15310-CL/ONS 15310-MA 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-C24 Set Up a Windows PC for Craft Connection to an ONS 15310-CL or ONS 15310-CL Using Dynamic Host Configuration Protocol

Purpose	This task sets up your computer for craft connection to the ONS 15310-CL/ONS 15310-MA using DHCP.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2 NTP-C21 Set Up CTC Network Access, page 4-6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution Do not use this task for initial node turn-up. Use the task only if DHCP forwarding is enabled on the ONS 15310-CL/ONS 15310-MA. By default, DHCP is not enabled. To enable it, see the "NTP-C21 Set Up CTC Network Access" procedure on page 4-6.

Note The ONS 15310-CL/ONS 15310-MA 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-C25 Set Up a Windows PC for Craft Connection to an ONS 15310-CL or ONS 15310-MA Using Automatic Host Detection

Purpose	This task sets up your computer for local craft connection to the ONS 15310-CL/ONS 15310-MA when: • You will connect to the ONS 15310-CL/ONS 15310-MA CRAFT port or its LAN port either directly or through a hub. • You will connect to multiple ONS 15310-CL/ONS 15310-MA nodes and do not want to reconfigure your IP address each time. • You do not need to access non-ONS 15310-CL/ONS 15310-MA applications such as ping and tracert (trace route).
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
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 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. The default node IP address is 192.1.0.2.

i. In the Subnet Mask field, type the same subnet mask as the ONS 15310-CL/ONS 15310-MA. 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 g. 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. The default node IP address is 192.1.0.2.

g. In the Subnet Mask field, type the same subnet mask as the ONS 15310-CL/ONS 15310-MA. 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 current node IP address. The default node IP address is 192.1.0.2.

f. In the Subnet Mask field, type the same subnet mask as the ONS 15310-CL/ONS 15310-MA. 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.
- **c.** From the Local Area Connection Properties dialog box, choose **Internet Protocol (TCP/IP)**, then click **Properties**.
- **d.** In the IP Address field, enter any legitimate IP address other than the current node IP address. The default node IP address is 192.1.0.2.
- **e.** In the Subnet Mask field, type the same subnet mask as the ONS 15310-CL/ONS 15310-MA. 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-C27 Disable Proxy Service Using Internet Explorer (Windows)

Purpose	This task disables proxy service for PCs running Internet Explorer.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 From the Start menu, select **Settings > Control Panel**.

Note If your computer is running Windows XP, you can select Control Panel directly from the Start menu. Make sure that you are in Classic View before continuing with this procedure. To switch to Classic View, right-click the Windows screen and choose **Properties** from the popup menu. Click the **Appearance** tab, then under Scheme, choose **Classic View**.

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.
- To bypass 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 15310-CL/ONS 15310-MA 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 15310-CL/ONS 15310-MA nodes on your network. Click **OK** to close each open dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-C28 Disable Proxy Service Using Netscape (Windows)

Purpose	This task disables proxy service for Windows PCs running Netscape.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
Required/As Needed	Required if your computer is connected to a network computer proxy server and your browser is Netscape.
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 15310-CL/ONS 15310-MA nodes that you will access. Separate each address with a comma. Click **OK** to close each open dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-C29 Log into CTC

Purpose	Use this task to log into CTC, the graphical user interface software used to manage the ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2 One of the following procedures: • NTP-C14 Set Up CTC Computer for Local Craft Connection to the Node, page 3-3, or • NTP-C15 Set Up a CTC Computer for a Corporate LAN Connection to the Node, page 3-5, or • NTP-C16 Set Up a Remote Access Connection to the Node, page 3-6
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note The ONS 15310-CL can be networked with ONS 15454 nodes running Software Release 4.1, 4.6, or later. The ONS 15310-MA can be networked with ONS 15454 nodes running Software Release 8.5 or later. You can log into the ONS 15454 nodes to manage the ONS 15310-CL or ONS 15310-MA nodes. However, you must complete the "DLP-C21 Run the CTC Installation Wizard for Windows" task on page 17-29 or the "DLP-C22 Run the CTC Installation Wizard for UNIX" task on page 17-32. These tasks install the Release 8.5 software JAR files on your computer. The tasks must be repeated anytime you delete the CTC cache.

Note For information about CTC views and navigation, see Appendix A, "CTC Information and Shortcuts."

Step 1 From the computer connected to the ONS 15310-CL or ONS 15310-MA, start Netscape (PC or UNIX) or Internet Explorer (PC only):

- If you are using a PC, launch Netscape or Internet Explorer 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 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** and **-ncols 32** command line options limit the number of colors that Netscape uses.

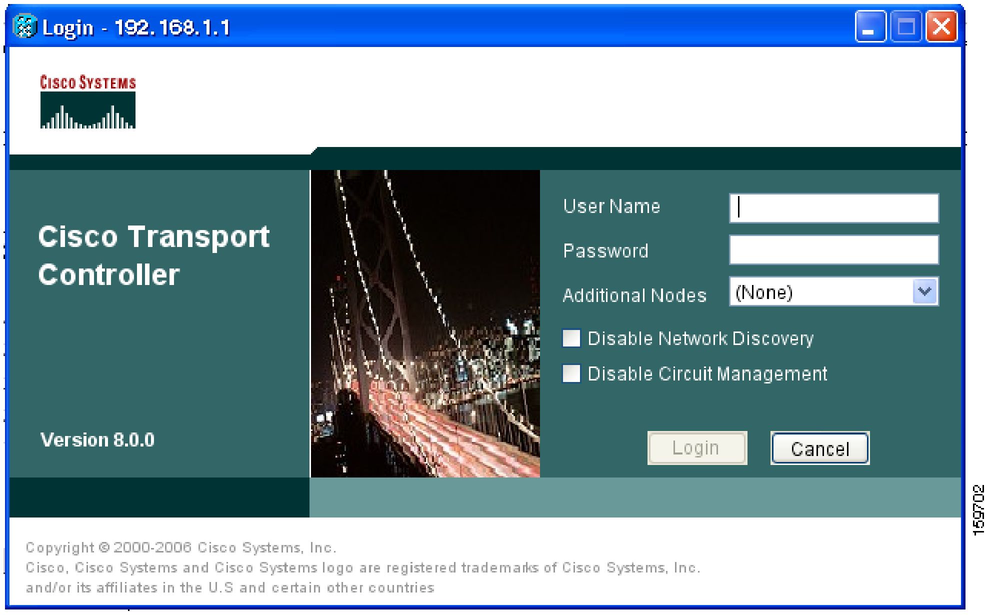
Step 2 In the Netscape or Internet Explorer web address (URL) field, enter the ONS 15310-CL or ONS 15310-MA IP address. For initial setup, this is the default address, 192.1.0.2. Press **Enter**.

Note If you are logging into ONS 15310-CL or ONS 15310-MA 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 15310-CL or ONS 15310-MA software version for each node visible on the network view. To resolve an alarm, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

If a Java Plug-in Security Warning dialog box appears, complete the "DLP-C30 Install Public-Key Security Certificate" task on page 17-47 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 15310-CL or ONS 15310-MA, this process can take several minutes. After the download, the CTC Login dialog box appears (Figure 17-20).

Figure 17-20 Logging into CTC



Login - 192.168.1.1

Cisco Transport Controller

Version 8.0.0

User Name

Password

Additional Nodes (None)

□ Disable Network Discovery

□ Disable Circuit Management

Copyright © 2000-2006 Cisco Systems, Inc.
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S and certain other countries

Step 3 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 15310-CL or ONS 15310-MA. 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 15310-CL or ONS 15310-MA users and assign security, go to the "NTP-C19 Create Users and Assign Security" procedure on page 4-4. Additional information about security is provided in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 4 Each time you log into an ONS 15310-CL or ONS 15310-MA, you can make selections for the following login options:

- Node Name—Displays the IP address entered in the web browser and a drop-down list of previously entered ONS 15310-CL/ONS 15310-MA IP addresses. You can select any ONS 15310-CL or ONS 15310-MA on the list for the login, or you can enter the IP address (or node name) of any new node where you want to log in.
- Additional Nodes—Displays a list of current login node groups. To create a login node group or to add additional groups, see the "DLP-C31 Create Login Node Groups" task on page 17-47).
- Disable Network Discovery—Check this box to view only the ONS 15310-CL or ONS 15310-MA (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 start-up time in networks with many DCC-connected nodes and reduces 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 reduces memory consumption. This option does not prevent the creation and management of new circuits.

Step 5 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 6 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 15310-CL or ONS 15310-MA. 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 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

Step 7 Return to your originating procedure (NTP).

DLP-C30 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-C29 Log into CTC" task on page 17-44. 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 15310-CL/ONS 15310-MA.
- No (Deny)—Denies permission to install certificate. If you choose this option, you cannot log into the ONS 15310-CL/ONS 15310-MA.
- 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 Return to your originating procedure (NTP).

DLP-C31 Create Login Node Groups

Purpose	This task creates a login node group to display ONS 15310-CL or ONS 15310-MA nodes that have an IP connection but not a DCC connection to the login node.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 **Login Node Group** and **Create Group**.

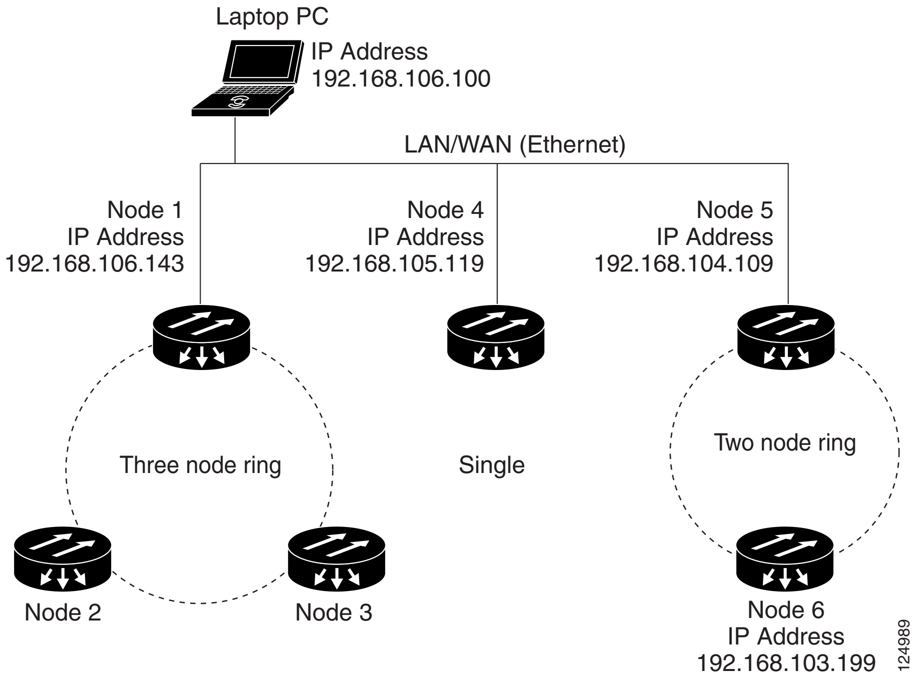
Step 3 Enter a name for the group in the Create Login Group Name dialog box. Click **OK**.

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 you want to add to the group.

Step 5 Click **OK**.

The next time you log into an ONS 15310-CL/ONS 15310-MA, the login node group will be available in the Additional Nodes list of the Login dialog box. For example, in Figure 17-21, 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, only 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 17-21 Login Node Group



Step 6 Return to your originating procedure (NTP).

DLP-C32 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-C29 Log into CTC, page 17-44
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).

Step 3 If you want to add the node to the current login group, check **Add node to current login group**. Otherwise, leave it unchecked.

Note 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-C33 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 specified login node group, see the "DLP-C34 Delete a Node from a Specified Login Node Group" task on page 17-49.
Tools	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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-C34 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-C33 Delete a Node from the Current Session or Login Group" task on page 17-49.
Tools	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 Select the node you want to remove, then click **Remove**.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-C35 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 or documentation 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-C29 Log into CTC, page 17-44
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-C29 Log into CTC" task on page 17-44.

Step 9 Return to your originating procedure (NTP).

DLP-C36 Configure the CTC Alerts Dialog for Automatic Popup

Purpose	This task sets up the CTC Alerts dialog box to open for all alerts, 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-C29 Log into CTC, page 17-44
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-C37 Create a New User on a Single Node

Purpose	This task creates a new user for one ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 Security window, click **Create**.

Step 3 In the Create User dialog box, enter the following:

- Name—Type the user name. The name must have a minimum of six and a maximum of 20 alphanumeric characters (a-z, A-Z, 0-9). For TL1 compatibility, the user name must have 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 characters. You can configure the default values in CTC node view using the Provisioning > NE Defaults > Node > security > password Complexity tabs. 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 have 6 to 10 characters, and the first character must be an alpha character. The password cannot 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 15310-CL and Cisco ONS 15310-MA 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. Default idle times are: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-C38 Create a New User on Multiple Nodes

Purpose	This task adds a new user to multiple ONS 15310-CL or ONS 15310-MA nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 Security window, click **Create**.

Step 4 In the Create User dialog box, enter the following:

- Name—Type the user name. The name must have a minimum of six and a maximum of 20 alphanumeric characters (a-z, A-Z, 0-9). For TL1 compatibility, the user name must have no more than 10 characters, and the first character must be an alpha character.
- Password—Type the user password. The password must have a minimum of 6 and a maximum of 20 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, and the first character must be an alpha character. The password cannot 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 15310-CL and Cisco ONS 15310-MA Reference Manual* for information about the capabilities provided with each level.

Note Each security level has a different idle time. The idle user timeout is the length of time that CTC can remain idle before it locks up and the password must be reentered. The default times are: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes. To change the idle user timeout values, see the "NTP-C83 Modify Users and Change Security" procedure on page 11-6.

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, click **OK**.

Step 8 Return to your originating procedure (NTP).

DLP-C39 Provision IP Settings

Purpose	This task provisions IP settings, which includes the IP address, default router, DHCP access, firewall access, and SOCKS proxy server settings.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution All network changes should be approved by your network (or LAN) administrator.

Step 1 In node view, click the **Provisioning** > **Network** > **General** tabs.

Step 2 Complete the following information in the fields listed:

- Node Address—Type the IP address assigned to the ONS 15310-CL or ONS 15310-MA node.
- 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 15310-CL/ONS 15310-MA nodes in the same subnet.
- MAC Address—(Display only) Displays the ONS 15310-CL/ONS 15310-MA IEEE 802 MAC address.
- Default Router— If the ONS 15310-CL or ONS 15310-MA is connected to a LAN, enter the IP address of the default router. The default router forwards packets to network devices that the ONS 15310-CL or ONS 15310-MA cannot directly access. This field is ignored if any of the following are true:

  - The ONS 15310 is not connected to a LAN.
  - SOCKS proxy server is enabled and the ONS 15310 is provisioned as an ENE.
  - OSPF is enabled on both the ONS 15310 and the LAN where the ONS 15310 is connected.
- Suppress CTC IP Display—Check this check box if you want to prevent the node IP address from being displayed in CTC to users with Provisioning, Maintenance, or Retrieve security levels. (The IP address suppression is not applied to users with Superuser security level.)
- Forward DHCP Request To—Check this check box to enable Dynamic Host Configuration Protocol (DHCP). Also, enter the DHCP server IP address in the Request To field. The check box is unchecked by default. If you will enable any of the gateway settings to implement the ONS 15310-CL/ONS 15310-MA SOCKS proxy server features, leave this field blank.

Note If you enable DHCP, computers connected to an ONS 15310-CL or ONS 15310-MA node can obtain temporary IP addresses from an external DHCP server. The ONS 15310 only forwards DHCP requests; it does not act as a DHCP server.

- CTX CORBA (IIOP) Listener Port—Sets the ONS 15310 IIOP (Internet Inter-Orb Protocol) listener port used for communication between the ONS 15310 and CTC computers. This field is generally not changed unless the ONS 15310 resides behind a firewall that requires a different port. See the "NTP-C22 Set Up the ONS 15310-CL or ONS 15310-MA for Firewall Access" procedure on page 4-8 for more information.
- Gateway Settings—Provisions the ONS 15310-CL or ONS 15310-MA SOCKS proxy server features. Do not select any of these options until you review the SOCKS proxy server scenario in the "Management Network Connectivity" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*. In SOCKS proxy server networks, the ONS 15310 is either an external network element (ENE), a gateway network element (GNE), or a proxy-only server. Provisioning must be consistent for each NE type.
- Enable SOCKS proxy server on port—If checked, the ONS 15310-CL or ONS 15310-MA serves as a proxy for connections between CTC clients and ONS 15310 nodes that are DCC-connected to the proxy ONS 15310. The CTC client establishes connections to data communications channel (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 15310. 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 15310 is not connected to a LAN but has DCC connections to other ONS nodes. A CTC computer connected to the ENE through the CRAFT or LAN 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 15310 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 15310 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. Click **Apply**.

Step 3 Click **Yes** in the confirmation dialog box.

The 15310-CL-CTX or CTX2500 reboots, which takes 4 to 6 minutes. Eventually, a “Lost node connection, switching to network view” message appears.

Step 4 Click **OK**. The network view appears. The node icon is displayed in gray, during which time you cannot access the node.

Step 5 Double-click the node icon when it becomes green.

Step 6 Return to your originating procedure (NTP).

DLP-C40 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-C29 Log into CTC, page 17-44
Required/As Needed	Required if either of the following is true: • CTC computers on one subnet need to connect to ONS 15310-CL or ONS 15310-MA nodes that are connected by a router to ONS 15310 nodes residing on another subnet. OSPF is not enabled and the External Network Element gateway setting is not checked. • You need to enable multiple CTC sessions among ONS 15310-CL and ONS 15310-MA nodes residing on the same subnet and the External Network Element gateway setting is not enabled.
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 **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 15310-CL or ONS 15310-MA 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 in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual.*

Step 5 Return to your originating procedure (NTP).

DLP-C41 Set Up or Change Open Shortest Path First Protocol

Purpose	This task enables the Open Shortest Path First (OSPF) routing protocol on the ONS 15310-CL or ONS 15310-MA. Perform this task if you want to include the ONS 15310 in OSPF-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 You will need the OSPF Area ID, Hello and Dead intervals, and authentication key (if OSPF authentication is enabled) provisioned on the router that the ONS 15310 is connected to.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From 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 15310 nodes as a unique OSPF area ID. It can be any number between 000.000.000.000 and 255.255.255.255. The number must be unique to the LAN OSPF area.
- SDCC Metric—This value is normally unchanged. It sets a cost for sending packets across the 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 15310-CL or ONS 15310-MA OSPF topology to be advertised to OSPF routers on the LAN. Enable this field on ONS 15310 nodes 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 15310-CL or ONS 15310-MA is connected. (This number is different from the DCC 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 Verify that the OSPF priority and intervals settings match the priority and interval settings used by the OSPF router where the ONS 15310-CL or ONS 15310-MA is connected. If not, change the settings, as needed.

- 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 Under OSPF Area Range Table, 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 15310 in the ONS 15310 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 15310 OSPF area.

a. Under OSPF Area Range Table, click **Create**.

b. In the Create Area Range dialog box, enter the following:

- Range Address—Enter the area IP address for the ONS 15310-CL or ONS 15310-MA nodes that reside within the OSPF area. For example, if the ONS 15310 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 15310-CL or ONS 15310-MA nodes. 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.
- Mask—The static route subnet mask value.
- Advertise—Check if you want to advertise the OSPF range table.

c. Click **OK**.

Step 7 If the ONS 15310-CL or ONS 15310-MA 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. Under OSPF Virtual Link Table, click **Create**.

b. In the Create Virtual Link dialog box, complete the following fields (OSPF settings must match OSPF settings for the ONS 15310 OSPF area):

- Neighbor—The router ID of the Area 0 router.

- Transmit Delay (sec)—The service speed. One second is the default.
- Retransmit Int (sec)—Sets the time that will elapse before a packet is resent. Five seconds is the default.
- Hello Int (sec)—The number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten 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.
- Auth Type—If the router where the ONS 15310-CL or ONS 15310-MA is connected uses authentication, choose **Simple Password**. Otherwise, choose **No Authentication**.
- Auth Key—If authentication type is set to Simple Password, the authentication key (password) is listed here.

c. Click **OK**.

Step 8 After entering ONS 15310-CL or ONS 15310-MA OSPF area data, click **Apply**.

Step 9 Return to your originating procedure (NTP).

DLP-C42 Set Up or Change Routing Information Protocol

Purpose	This task enables Routing Information Protocol (RIP) on the ONS 15310-CL or ONS 15310-MA. Perform this task if you want to include the node in RIP-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 You need to create a static route to the router adjacent to the ONS 15310-CL or ONS 15310-MA if the ONS 15310 needs 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 15310-CL or ONS 15310-MA 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 15310-CL or ONS 15310-MA is a GNE with multiple ONS 15310 ENEs 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.
- Cost—The RIP Priority level. The smaller the number, the higher the priority.

c. Click **OK.**

Step 7 Return to your originating procedure (NTP).

DLP-C43 Provision the IIOP Listener Port on the ONS 15310-CL or ONS 15310-MA

Purpose	This task sets the IIOP listener port on the ONS 15310-CL or ONS 15310-MA, which enables you to access ONS 15310 nodes that reside behind a firewall.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If the Enable Proxy Server on port 1080 check box is checked, CTC will use port 1080 and ignore the configured IIOP port setting. If Enable 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 CTX CORBA (IIOP) Listener Port area, choose a listener port option:

- Default - CTX Fixed—Select this option if the ONS 15310-CL or ONS 15310-MA nodes are on the same side of the firewall as the CTC computer or if no firewall is used (default). This option sets the 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 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**.

The 15310-CL-CTX or CTX2500 card reboots. The reboot takes approximately 4 to 6 minutes.

Step 5 Return to your originating procedure (NTP).

DLP-C44 Provision the IIOP Listener Port on the CTC Computer

Purpose	This task selects the IIOP listener port on CTC.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 TCC CORBA (IIOP) Listener Port area, choose a listener port option:

- Default - Variable—Select this option if the ONS 15310-CL or ONS 15310-MA nodes are on the same side of the firewall as the CTC computer or if no firewall is used (default). This option sets the CTX 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 provided by your administrator. Unavailable ports are listed in the "Management Network Connectivity" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

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 To access the ONS 15310-CL or ONS 15310-MA using the IIOP port, log out of CTC by choosing Exit from the File menu.

Step 7 Log back into CTC. See the "DLP-C29 Log into CTC" task on page 17-44 for instructions.

Step 8 Return to your originating procedure (NTP).

DLP-C45 Set Up External or Line Timing

Purpose	This task defines the external or line SONET timing source for the ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, click the **Provisioning > Timing > General** tabs.

Step 2 In the General Timing area, complete the following information:

- Timing Mode—Choose **External** if the ONS 15310-CL or ONS 15310-MA derives its timing from a BITS source wired to the port on the 15310; choose **Line** if timing is derived from the OC-N, DS1-28, or DS1-84 port. A third option, Mixed, allows you to set external and line timing references.

Note Because Mixed timing can 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 15310-CL and ONS 15310-MA nodes can translate Generation 2 message sets, so choose Generation 2 if the ONS 15310 is connected to other ONS 15310 nodes. Choose Generation 1 only when the ONS 15310 is connected to equipment that does not support Generation 2. If a node that has its SSM Message Set 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 become an ST3.
- 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 in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for more information about SSM, including definitions of the SONET timing levels.
- Revertive—Check this check box if you want the ONS 15310-CL or ONS 15310-MA 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 the ONS 15310-CL or ONS 15310-MA will wait before reverting to its primary timing source. Five minutes is the default.

Step 3 In the Reference Lists area, complete the following information:

Note You can define up to three timing references for the node and up to three BITS-1 Out references. BITS-1 Out reference defines the timing reference used by equipment that can be attached to the node’s BITS Out connection. If you attach equipment to the BITS Out connection, 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 15310-CL-CTX or the CTX2500. The options displayed depend on the Timing Mode setting.
- If the Timing Mode is set to External, your options are BITS1 and Internal Clock.
- If the Timing Mode is set to Line, your options are the 15310-CL-CTX or the CTX2500 and Internal Clock. Choose the port that is directly or indirectly connected to the node wired to the BITS source, that is, the BITS port on the ONS 15310-CL or ONS 15310-MA. Set Reference 1 to the port that is closest to the BITS source. For example, if the DS1 port is connected to the node wired to the BITS source, choose Slot 2 (CTX), Port 1 (DS1) as Reference 1.
- If the Timing Mode is set to Mixed, both BITS and the 15310-CL-CTX or CTX2500 are available, allowing you to set a mixture of external BITS and the CTX as timing references.
- BITS-1 Out—Define the timing references for equipment wired to the BITS Out connection on the 15310-CL-CTX or CTX2500. BITS-1 Out is enabled when BITS-1 facilities are put in service. If Timing Mode is set to external, choose the port used to set the timing. If Timing Mode is set to Line, you can choose a port or choose NE Reference to have the BITS-1 Out follow the same timing references as the NE.

Step 4 Click **Apply**.

Note Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* for timing-related alarms.

Step 5 In the node view, click the **Provisioning > Timing > BITS Facilities** tabs.

Step 6 In the BITS Facilities area, complete the following information:

Note The BITS Facilities section sets the parameters for your BITS1 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 Facility Type—Provisions the BITS In facility type (DS1).
- BITS In State—If Timing Mode is set to External or Mixed, set the BITS In State for BITS-1 to **IS** (in service) if the BITS input port is connected to the external timing source. If Timing Mode is set to Line, set the BITS In State to **OOS** (out of service).
- BITS Out Facility Type—Provisions the BITS Out facility type (DS1).
- BITS Out State—If equipment is connected to the node's BITS output pins and you want to time the equipment from a node reference, set the BITS Out State for BITS-1 to **IS**, if the BITS Out connection is used for the external equipment. If equipment is not attached to the BITS output connector, set the BITS Out State to **OOS**.

Step 7 If the state is set to OOS, continue with Step 8. If the 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.
- 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 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 15310-CL/ONS 15310-MA. 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 8 Return to your originating procedure (NTP).

DLP-C46 Set Up Internal Timing

Purpose	This task sets up internal Stratum 3 timing for an ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed (use only if a BITS source is not available)
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Internal timing is Stratum 3 and not intended for permanent use. All ONS 15310-CL or ONS 15310-MA 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—Not relevant to internal timing; ignore this field.
- Revertive—Not relevant to internal timing; ignore this field.
- Reversion Time—Not relevant to internal timing; ignore this field.

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—Set to None.

Step 4 Click **Apply**.

Step 5 In node view, click the **Provisioning > Timing > BITS Facilities** tabs.

Step 6 In the BITS In State drop-down list, change State to **OOS**. Disregard the other BITS Facilities settings; they are not relevant to internal timing.

Step 7 Click **Apply**.

Step 8 Return to your originating procedure (NTP).

DLP-C47 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 SOCKS 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-C29 Log into CTC, page 17-44 DLP-C52 Provision Section DCC Terminations, page 17-68
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note If the SOCKS 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).
- Source 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).
- Destination Length—Choose the length of the destination subnet mask.

Step 4 Click **OK**.

Step 5 Continue with your originating procedure (NTP).

DLP-C48 Provision a Firewall Tunnel

Purpose	This task provisions destinations that will not be blocked by the firewall. Firewall tunnels are only necessary when the SOCKS 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-C29 Log into CTC, page 17-44 DLP-C52 Provision Section DCC Terminations, page 17-68 or DLP-C40 Create a Static Route, page 17-55
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note If the SOCKS 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).
- Source 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).
- Destination Length—Choose the length of the destination subnet mask.

Step 4 Click **OK**.

Step 5 Continue with your originating procedure (NTP).

DLP-C49 Create a Provisionable Patchcord

Purpose	This task creates a provisionable patchcord, also called a virtual link. Patchcords are used for network communication when a DCC/GCC is not available. They appear as dashed lines in CTC network view. For the specific situations in which a patchcord is necessary, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.
Tools/Equipment	For for information about patchcords, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note To set up a provisionable patchcord between an optical port and an ONS node transponder/muxponder, an 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-C52 Provision Section DCC Terminations" task on page 17-68.

Note An optical port requires two patchcords when the remote end is Y-cable protected or is an add/drop multiplexer or multiplexer/demultiplexer port.

Step 1 In node view, click the **Provisioning > Comm Channels > PPCs** tabs. If you are in network view, click the **Provisioning > Provisionable Patchcords (PPC)** 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-C50 Change the Service State for a Port

Purpose	This task puts a port in service or removes a port from service.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the node view shelf graphic, double-click the card that contains the ports that you want to put in or out of service. The card view appears.

Step 2 Click the **Provisioning > DS1**, **DS3**, **EC1**, or **Optical** 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. 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 port service states, refer to the "Administrative and Service States" appendix of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA 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.

Note A continuously valid signal must be received for the duration of the soak period before the OOS-AU,AINS port makes a transition to the IS-NR state. For example, if the soak timer is set for eight hours, and you receive an error after two hours, the timer is reset for another eight-hour period. This cycle continues until an error-free signal is received for an eight-hour period.

Step 6 Click **Apply**.

Step 7 As needed, repeat this task for each port.

Step 8 Return to your originating procedure (NTP).

DLP-C52 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.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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 DCC 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 15310-CL or ONS 15310-MA DCC terminations. The SONET Line DCCs and the Section DCC (when not used as a DCC termination by the ONS 15310-CL or ONS 15310-MA) can be provisioned as DCC tunnels. See the "DLP-C67 Create a DCC Tunnel" task on page 17-84.

Step 4 In the Port Admin State area, click the **Set to IS** radio button.

Step 5 Verify that the Disable OSPF on 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-C152 Change a Section DCC Termination" task on page 18-55.

Step 7 In the Layer 3 box, perform one of the following:

- Check the IP box only—if the SDCC is between the ONS 15310-CL or ONS 15310-MA 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 15310-CL or ONS 15310-MA 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 are present until you create all network DCC terminations and put the DCC termination optical ports in service.

Note There are four possibilities for the appearance of DCCs: green/solid, green/dashed, gray/solid, gray/dashed. DCC appearance corresponds to the following states: active/routable, active/nonroutable, failed/routable, or failed/nonroutable. Circuit provisioning uses active/routable links. Selecting a node or span in the graphic area displays information about the node and span in the status area.

Step 10 Return to your originating procedure (NTP).

DLP-C53 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.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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 DCC 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 node DCC terminations. The SONET Line DCCs and the Section DCC (when not used as a DCC termination by the ONS node) can be provisioned as DCC tunnels. See the "DLP-C67 Create a DCC Tunnel" task on page 17-84.

Step 4 In the Port Admin State area, click the **Set to IS** radio button.

Step 5 Verify that the Disable OSPF on Link check box is unchecked.

Step 6 If the LDCC 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.

Step 7 In the Layer 3 box, perform one of the following:

- Check the IP box only—if the LDCC is between the ONS 15310-CL/ONS 15310-MA 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 15310-CL/ONS 15310-MA 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 (DCC Termination Failure) and LOS (Loss of Signal) alarms are present until you create all network DCC terminations and put the DCC termination optical ports in service.

Note There are four possibilities for the appearance of DCCs: green/solid, green/dashed, gray/solid, gray/dashed. DCC appearance corresponds to the following states: active/routable, active/nonroutable, failed/routable, or failed/nonroutable. Circuit provisioning uses active/routable links. Selecting a node or span in the graphic area displays information about the node and span in the status area.

Step 10 Return to your originating procedure (NTP).

DLP-C54 Optical 1+1 Protection Test

Purpose	This task verifies that a 1+1 protection group will switch traffic properly.
Tools/Equipment	The test set specified by the acceptance test procedure.
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44; a test circuit created as part of the topology acceptance test.
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-C88 Disable Alarm Filtering" task on page 17-109 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms are present, investigate and resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

Step 3 Click the **Conditions** tab. Verify that the network does not have any unexplained conditions. If unexplained conditions are present, resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA 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 the node 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, IS-NR

Working port - Working/Active, IS-NR

Step 12 Return to your originating procedure (NTP).

DLP-C55 Path Protection Switching Test

Purpose	This task verifies that a path protection span is switching correctly.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 Network View**.

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box displays 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:

a. Click the **Perform path protection span switching** field and choose **FORCE SWITCH AWAY** from the drop-down list.

b. Click **Apply**.

c. In the Confirm Path Protection Switch dialog box, click **Yes**.

d. 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 and choose **CLEAR** from the drop-down list.

b. Click **Apply**.

c. Click **Yes** to confirm.

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-C56 Assign a Name to a Port

Purpose	This task assigns a name to a port on any ONS 15310-CL or ONS 15310-MA card.
Tools/Equipment	None
Prerequisite Procedures	NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2 NTP-C148 Verify Card and SFP Installation for the ONS 15310-MA, page 4-3 DLP-C29 Log into CTC, page 17-44
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 Complete the following, as necessary:

- For 15310-CL-CTX DS-1 ports, click the **DS1** subtab.
- For 15310-CL-CTX DS-3 ports, click the **DS3** subtab.
- For 15310-CL-CTX EC-1 ports, click the **EC1** subtab.
- For 15310-CL-CTX OC-N ports, click the **Optical** subtab.
- For CE-100T-8 or ML-100T-8 cards, click the **Ether Ports** or **POS Ports** subtab.

Step 4 Click the **Port Name** column for the port number you are assigning a name to and enter the desired port name.

The port name can be up to 32 alphanumeric/special characters and is blank by default.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

DLP-C57 Provision Path Protection Selectors During Circuit Creation

Purpose	This task provisions path protection selectors during circuit creation. Complete this task only if the circuit will be routed on a path protection configuration.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 The Circuit Creation wizard Circuit Attributes page must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Provisioning SD-P or SF-P thresholds in the Circuit Attributes page of the Circuit Creation wizard sets the values only for path-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 Circuit Attributes area of the Circuit Creation wizard, set the path protection path 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 check 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 (SF) bit error rate (BER) thresholds. VT thresholds only apply to circuits with 15310-CL-CTX or CTX2500 ports as path protection selectors.
- SD threshold—Set the path protection path-level signal degrade BER thresholds. VT thresholds only apply to circuits with 15310-CL-CTX or CTX2500 ports as path protection selectors.
- Switch on PDI-P—For STS circuits, check this check box if you want traffic to switch when an STS payload defect indicator is received. Unavailable for VT circuits.

Step 2 Return to your originating procedure (NTP).

DLP-C58 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-C29 Log into CTC, page 17-44 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

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 where the circuit will originate.

Step 3 From the Port drop-down list, choose **DS1**.

Step 4 If you are creating a VT circuit, choose the source DS-1 port from the DS-1 drop-down list.

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.

Step 9 Depending on the destination card, choose the destination port, STS, VT, or DS-1 from the drop-down lists that appear based on the card selected in Step 8. See Table 6-2 on page 6-2 for a list of valid options. CTC does not display ports, STSs, VTs, or DS-1s already used by other circuits. If you and a user working on the same network choose the same port, STS, VT, port, or DS-1 simultaneously, one of you will receive a Path in Use error and be unable to complete the circuit. The user with the incomplete 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-C59 Provision STS and VT Grooming Nodes

Purpose	This task provisions the STS and VT grooming nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 The Circuit Creation wizard VT Optimization Matrix page must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the Select Optimization area of the VT Matrix Optimization page, choose one of the following:

- Create VT tunnel on transit nodes—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 nodes 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 "Circuits and Tunnels" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for more information.
- Create VT aggregation point—This option is available if the circuit source or destination is on an OC-N port on a 1+1 or unprotected node. VAPs aggregate circuits onto an STS for handoff to non-ONS networks or equipment, such as an IOF, switch, or digital access and cross-connect system

(DACS). It allows VT1.5 circuits to be routed through the node using one STS connection on the 15310-CL-CTX (cross-connect) card matrix rather than multiple VT connections on the 15310-CL-CTX card VT matrix. If you want to aggregate the circuit you are creating with others onto an STS for transport outside the ONS network, choose one of the following:

  - STS grooming node is *source node*, VT grooming node is *destination node*—Creates the VAP on the circuit source node. This option is available only if the circuit originates on an OC-N port.
  - STS grooming node is *destination node*, VT grooming node is *source node*—Creates the VAP on the circuit destination node. This option is available only if the circuit terminates on an OC-N port.

- 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 2 Return to your originating procedure (NTP).

DLP-C60 Provision a DS-1, DS-3, or EC-1 Circuit Route

Purpose	This task provisions the circuit route for manually routed DS-1, DS-3, or EC-1 circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 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 and 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 white. In the Selected Span area, the From and To fields display span information. The source STS and VT appear.

- 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 1+1 portions of the route from the source to the destination.
- For circuits routed on path protection dual ring interconnect topologies, provision the working and protect paths as well as the spans between the DRI nodes.

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, adjust the Source VT field; otherwise, continue with Step 5.

Step 5 Repeat Steps 2 through 4 until the circuit is provisioned from the source to the destination node through all intermediary nodes.

Step 6 Return to your originating procedure (NTP).

DLP-C61 Provision a DS-3 or EC-1 Circuit Source and Destination

Purpose	This task provisions an electrical circuit source and destination for a DS-3 or EC-1 circuit.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 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

Note After you have selected the circuit properties in the Circuit Source page 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 where the circuit will originate.

Step 3 From the Port drop-down list, choose the source port as appropriate.

Step 4 If you are creating a VT circuit, choose the VT from the VT drop-down list.

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.

Step 9 Depending on the destination card, choose the destination port or STS from the drop-down lists that display based on the card selected in Step 2. See Table 6-2 on page 6-2 for a list of valid options. CTC does not display ports, STSs, VTs, or DS-1s if they are already in use by other circuits. If you and a user working on the same network choose the same port, STS, VT, port, or DS-1 simultaneously, one of you will receive a Path in Use error and be unable to complete the circuit. The user with the incomplete 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-C62 Provision a VT Tunnel Route

Purpose	This task provisions the route for a manually routed VT tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
	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, 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 white. In the Selected Span area, the From and To fields display 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-C63 Provision an OC-N Circuit Source and Destination

Purpose	This task provisions the source and destination cards for an OC-N circuit.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
	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 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 from the Port and STS drop-down lists. STSs do not appear if they are already in use by other circuits.

Step 4 If you are creating a VT circuit, choose the VT from the VT drop-down list.

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.

Step 6 Click **Next**.

Step 7 From the Node drop-down list, choose the destination node.

Step 8 From the Slot drop-down list, choose the slot where the circuit will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the list.)

Step 9 Depending on the card selected in Step 2, choose the destination port and/or STS from the Port and STS drop-down lists.

Step 10 If you are creating a VT circuit, choose the VT from the VT drop-down list.

Step 11 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 7 through 10 to define the secondary destination.

Step 12 Click **Next**.

Step 13 Return to your originating procedure (NTP).

DLP-C64 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-C29 Log into CTC, page 17-44 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, 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 white. In the Selected Span area, the From and To fields display span information. The source STS and if applicable, VT appears.

Step 3 If you want to change the source STS, choose a different STS from the Source STS drop-down list; otherwise, continue with Step 4.

Step 4 If you want to change the source VT, choose a different VT from the Source VT drop-down list; otherwise, continue with Step 5.

Step 5 Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

Step 6 Repeat Steps 2 through 5 until the circuit is provisioned from the source to the destination node through all intermediary nodes. If Fully Protect Path is checked on the Circuit Routing Preferences page, you must complete the following:

- 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 1+1 portions of the route from the source to the destination.

Step 7 Return to your originating procedure (NTP).

DLP-C65 Provision a VCAT Circuit Source and Destination

Purpose	This task provisions a VCAT circuit source and destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 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 ML-100T-8 or CE-100T-8 card where the circuit will originate. (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, STS, and VT 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. VTs do not appear for STS-V circuits or if they are already in use by other 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 ML-100T-8 or CE-100T-8 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 6, choose the source port and/or STS and, if applicable, VT from the Port, STS, and VT 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. VTs do not appear for STS-V circuits or if they are already in use by other circuits.

Step 8 Click **Next**.

Step 9 Return to your originating procedure (NTP).

DLP-C66 Provision a VCAT Circuit Route

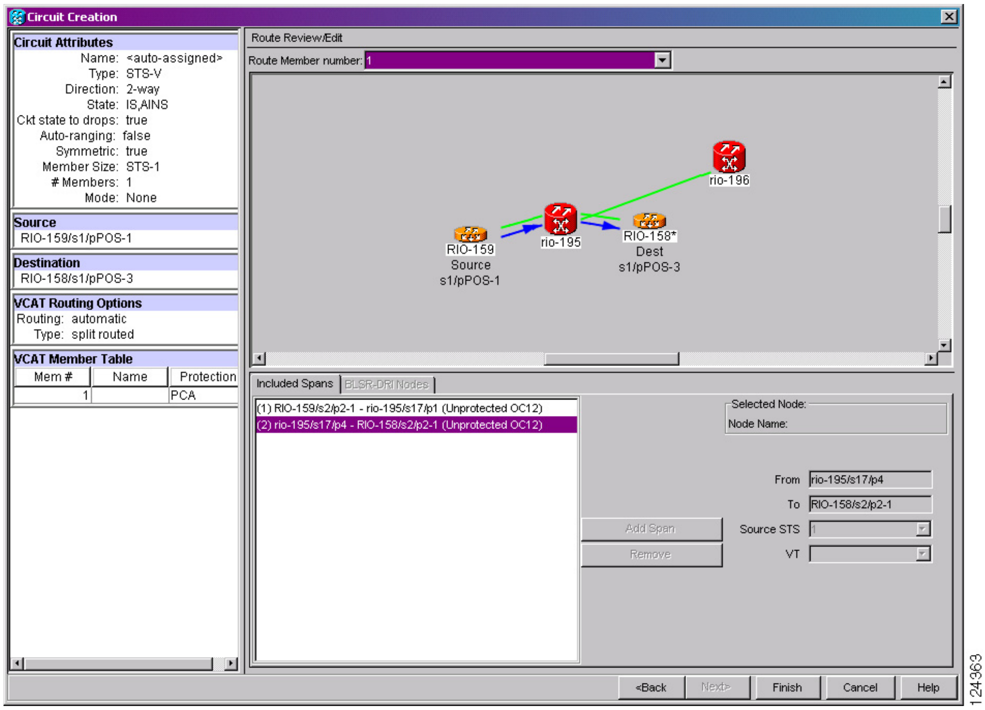
Purpose	This task provisions the circuit route for manually routed OC-N circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 The Circuit Creation wizard Route Review/Edit page must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning 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 white. In the Selected Span area, the From and To fields provide span information. The source STS appears. Figure 17-22 shows an example.

Figure 17-22 Manually Routing a VCAT Circuit



Circuit Creation

Circuit Attributes

Name: <auto-assigned>
Type: STS-V
Direction: 2-way
State: IS,AINS
Ckt state to drops: true
Auto-ranging: false
Symmetric: true
Member Size: STS-1
Members: 1
Mode: None

Source
RIO-159/s1/pPOS-1

Destination
RIO-158/s1/pPOS-3

VCAT Routing Options
Routing: automatic
Type: split routed

VCAT Member Table

Mem #	Name	Protection
1		PCA

Route Review/Edit

Route Member number: 1

Included Spans

(1) RIO-159/s2/p2-1 - rio-195/s17/p1 (Unprotected OC12)
(2) rio-195/s17/p4 - RIO-158/s2/p2-1 (Unprotected OC12)

Selected Node:
Node Name:

From: rio-195/s17/p4
To: RIO-158/s2/p2-1
Source STS: 1
VT:

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 this task for each member.

Step 7 Return to your originating procedure (NTP).

DLP-C67 Create a DCC Tunnel

Purpose	This task creates a DCC tunnel to transport traffic from third-party SONET equipment across ONS networks. Tunnels can be created on the Section DCC (SDCC) channel (D1-D3) (if not used by the ONS 15310-CL/ONS 15310-MA as a terminated DCC), or any Line DCC (LDCC) channel (D4-D6, D7-D9, or D10-D12).
Tools/Equipment	None
Prerequisite Procedures	NTP-C36 Verify Network Turn-Up, page 6-4 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Each ONS 15310-CL/ONS 15310-MA can have two DCC tunnel connections. Terminated SDCCs used by the ONS 15310-CL/ONS 15310-MA cannot be used as DCC tunnel endpoints, and an SDCC 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)**—Section DCC
  - **DCC2 (D4-D6)**—Line DCC 1
  - **DCC3 (D7-D9)**—Line DCC 2
  - **DCC4 (D10-D12)**—Line DCC 3

DCC options do not appear if they are being used by the ONS 15310-CL/ONS 15310-MA (DCC1) or other tunnels.

Step 6 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)**—Section DCC
  - **DCC2 (D4-D6)**—Line DCC 1
  - **DCC3 (D7-D9)**—Line DCC 2
  - **DCC4 (D10-D12)**—Line DCC 3

  DCC options do not appear if they are used by the ONS 15310-CL/ONS 15310-MA (DCC1) or other tunnels.

Step 7 Click **Finish**.

Step 8 Put the ports that are hosting the DCC tunnel in service. See the "DLP-C50 Change the Service State for a Port" task on page 17-67 for instructions.

Step 9 Return to your originating procedure (NTP).

DLP-C68 Create a User Data Channel Circuit

Purpose	This task creates a user data channel (UDC) circuit on the ONS 15310-CL/ONS 15310-MA. A UDC circuit allows you to create a dedicated data channel between nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-C12 Install the UDC Cable on the ONS 15310-CL, page 17-15 DLP-C29 Log into CTC, page 17-44
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. In the Endpoints area, choose the source and destination nodes and the source and destination OC-N ports and slots from the drop-down lists.

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-C69 Create an IP-Encapsulated Tunnel

Purpose	This task creates an IP-encapsulated tunnel to transport traffic from third-party SONET equipment across ONS networks. IP-encapsulated tunnels are created on the Section DCC channel (D1-D3) (if not used by the ONS node as a terminated DCC).
Tools/Equipment	OC-N cards must be installed.
Prerequisite Procedures	NTP-C36 Verify Network Turn-Up, page 6-4 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Each ONS 15310-CL or ONS 15310-MA can have one IP-encapsulated tunnel. Terminated Section DCCs used by the ONS 15310-CL or ONS 15310-MA cannot be used as tunnel endpoints, and a Section DCC that is used as a tunnel endpoint cannot be terminated. A tunnel connection is 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-C39 Provision IP Settings" task on page 17-53.

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-C50 Change the Service State for a Port" task on page 17-67 for instructions.

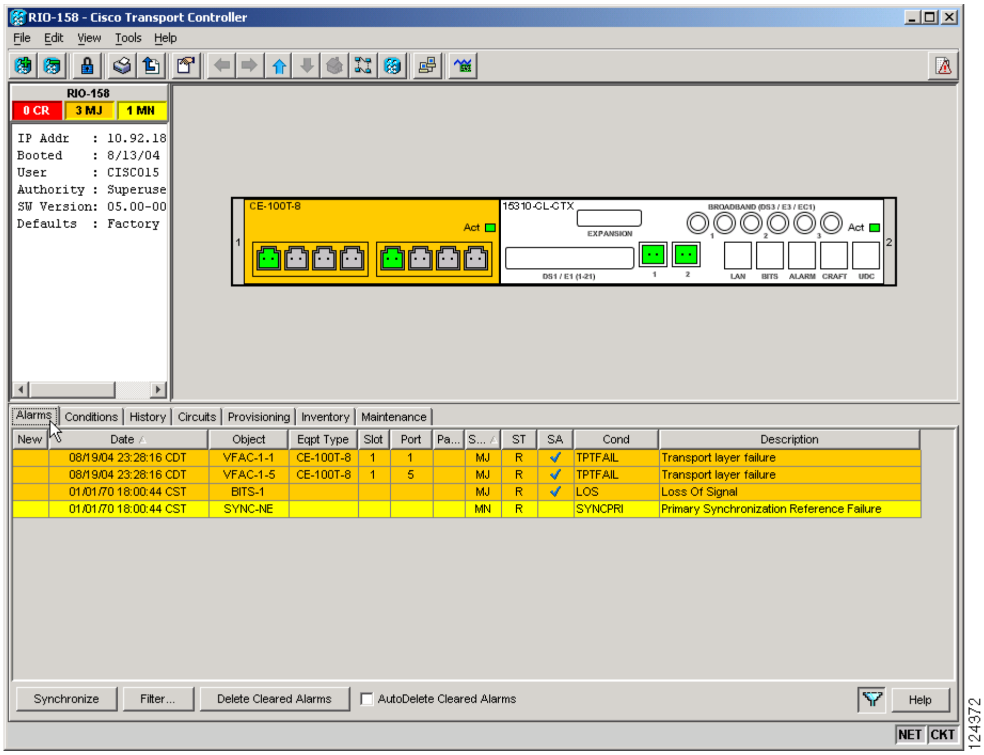
Step 11 Return to your originating procedure (NTP).

DLP-C72 View Alarms

Purpose	This task views current alarms on a card, node, or network.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 (Figure 17-23). The ONS 15310-CL window is shown, and the ONS 15310-MA Alarms window is very similar to it.

Figure 17-23 ONS 15310-CL Alarms in Node View



```
IP Addr   : 10.92.18
Booted    : 8/13/04
User      : CISCO15
Authority : Superuse
SW Version: 05.00-00
Defaults  : Factory
```

New	Date	Object	Eqpt Type	Slot	Port	Pa...	S...	ST	SA	Cond	Description
	08/19/04 23:28:16 CDT	VFAC-1-1	CE-100T-8	1	1		MJ	R	✓	TPTFAIL	Transport layer failure
	08/19/04 23:28:16 CDT	VFAC-1-5	CE-100T-8	1	5		MJ	R	✓	TPTFAIL	Transport layer failure
	01/01/70 18:00:44 CST	BITS-1					MJ	R	✓	LOS	Loss Of Signal
	01/01/70 18:00:44 CST	SYNC-NE					MN	R		SYNCPRI	Primary Synchronization Reference Failure

□ AutoDelete Cleared Alarms

Table 17-6 lists the columns in the Alarms window and their descriptions.

Table 17-6 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. Table 17-8 on page 17-89 lists these identifiers. For an STSmon or VTmon, this is the monitored STS or VT object.
Eqpt Type	If an alarm is raised on a card, the card type in this slot.
Shelf	For DWDM configurations, the shelf where the alarmed object is located. Visible in network view.
Slot	If an alarm is raised on a card, the slot where the alarm occurred (appears only in network and node view).
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.

Table 17-6 Alarm Column Descriptions (continued)

Column	Information Recorded
Path Width	Indicates how many STSs are contained in the alarmed path. This information complements the alarm object notation, which is explained in Table 17-8 on page 17-89.
Sev	Severity level: CR (Critical), MJ (Major), MN (minor), NA (Not Alarmed), NR (Not Reported).
ST	Status: R (raised), C (clear).
SA	When checked, indicates a service-affecting alarm.
Cond	The error message/alarm name; these names are alphabetically defined in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.
Description	Description of the alarm.

Table 17-7 lists the color codes for alarm and condition severities.

Table 17-7 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

In network view, CTC identifies STS and VT alarm objects using a TL1-type access identifier (AID). Table 17-8 lists these AIDs.

Table 17-8 STC and VT Alarm Object Identification

STS and VT Alarm Numbering	
MON Object (Optical)	**Syntax and Examples**
OC3/OC12 STS	Syntax: STS-<Slot>-<Ppm>-<Port>-<STS> Ranges: STS-{2}-{1-2}-{1}-{1-*n*[1]} Example: STS-2-1-1-6
OC3/OC12 VT	Syntax: VT1-<Slot>-<Ppm>-<Port>-<STS>-<VT Group>-<VT> Ranges: VT1-{2}-{1-2}-{1}-{1-*n*[1]}-{1-7}-{1-4} Example: VT1-2-1-1-6-1-1
EC1 STS	Syntax: STS-<Slot>-<Port>-<STS> Ranges: STS-{2}-{1-3}-{1-*n*[1]} Example: STS-2-1-6

Table 17-8 STC and VT Alarm Object Identification (continued)

STS and VT Alarm Numbering	
MON Object (Optical)	**Syntax and Examples**
EC1 VT	Syntax: VT1-<Slot>-<Port>-<STS>-<VT Group>-<VT> Ranges: VT1-{2}-{1-3}-{1-*n*[1]}-{1-7}-{1-4} Example: VT1-2-1-6-1-1
TERM Object (Electrical)	**Syntax and Examples**
T1 STS	Syntax: STS-<Slot>-<STS> Ranges: STS-{2}-{1-*n*[1]} Example: STS-2-6
T1 VT	Syntax: VT1-<Slot>-<STS>-VT Group>-<VT> Ranges: VT1-{2}-{1-*n*[1]}-{1-7}-{1-3} Example: VT1-2-6-1-1
T3 STS	Syntax: STS-<Slot>-<Port>-<STS> Ranges: STS-{2}-{1-3}-{1-*n*[1]} Example: STS-2-1-6
T3 VT	VT not supported

[1] Maximum STS number depends on the rate and size of the STS.

Step 2 If alarms are present, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* for information and troubleshooting procedures.

Step 3 Return to your originating procedure (NTP).

DLP-C73 View Alarm or Event History

Purpose	This task views past cleared and uncleared ONS 15310-CL or ONS 15310-MA 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-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 To view node alarm history, proceed to Step 2. To view network alarm history, proceed to Step 3. To view card alarm history, proceed to Step 4.

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 to view the alarm and condition history for the node.

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-C84 Enable Alarm Filtering" task on page 17-104 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 display the card-level 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 15310-CL and ONS 15310-MA 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 oldest events in that category are discarded.

Raised and cleared alarm messages (and events, if selected) appear.

Step 5 Return to your originating procedure (NTP).

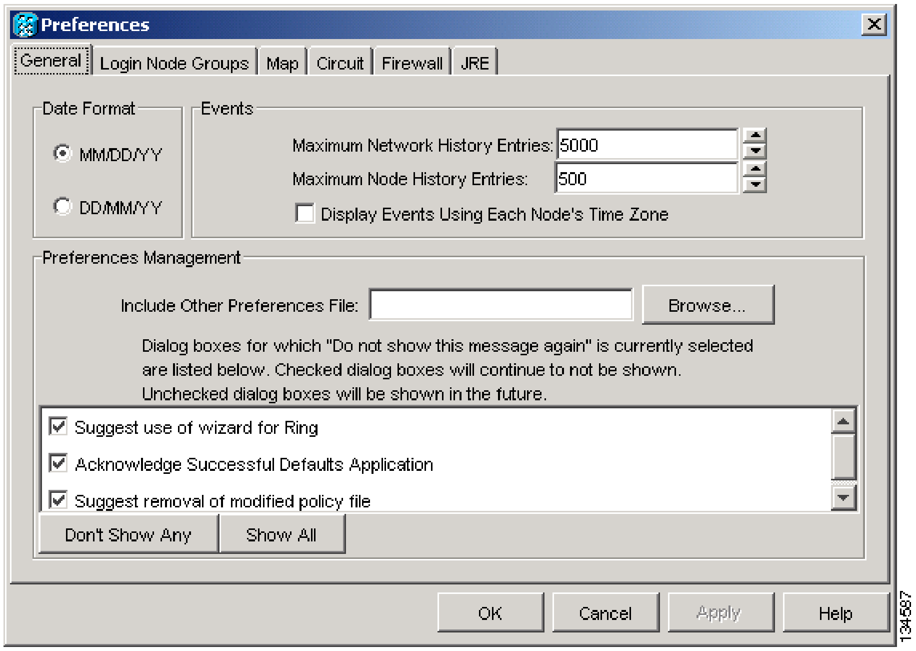
DLP-C74 Change the Maximum Number of Session Entries for Alarm History

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-C29 Log into CTC, page 17-44
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 17-24).

Figure 17-24 CTC Preferences Dialog Box



● MM/DD/YY

○ DD/MM/YY

Maximum Network History Entries: 5000

Maximum Node History Entries: 500

☐ Display Events Using Each Node's Time Zone

Include Other Preferences File:

Dialog boxes for which "Do not show this message again" is currently selected are listed below. Checked dialog boxes will continue to not be shown. Unchecked dialog boxes will be shown in the future.

☑ Suggest use of wizard for Ring

☑ Acknowledge Successful Defaults Application

☑ Suggest removal of modified policy file

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 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-C75 Display Alarms and Conditions Using Time Zone

Purpose	This task changes the time stamp for events to the time zone of the ONS 15310-CL or ONS 15310-MA 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-C29 Log into CTC, page 17-44
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 17-24).

Step 2 Check the **Display Events Using Each Node's Time Zone** check box.

Step 3 Click **Apply** and **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-C76 Synchronize Alarms

Purpose	This task is used to view ONS 15310-CL and ONS 15310-MA 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-C29 Log into CTC, page 17-44
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 messages arrive from the node.

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-C77 View Conditions

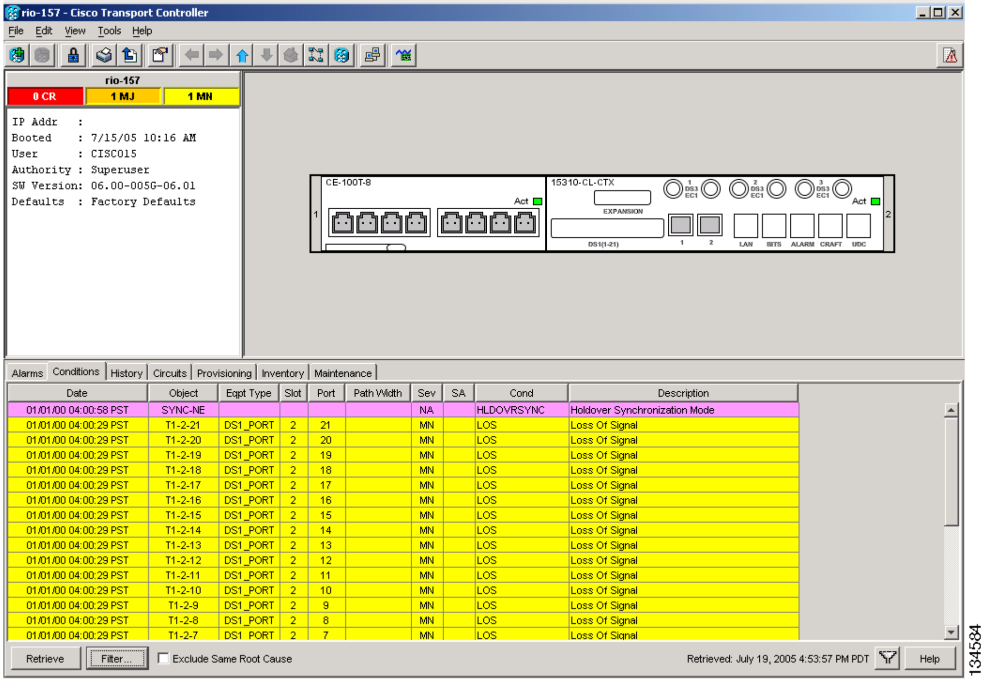
Purpose	This task is used to view conditions [events with a Not-Reported (NR) severity] at the card, node, or network level. Conditions give you a clear record of changes or events that do not result in alarms.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In the card, node, or network view, click the **Conditions** tab.

Step 2 Click **Retrieve** (Figure 17-25).

The Retrieve button requests the current set of fault conditions from the node, card, or network. The window is not updated when conditions change on the node. You must click Retrieve to see any changes.

Figure 17-25 ONS 15310-CL Node View Conditions Window


rio-157 - Cisco Transport Controller
File Edit View Tools Help
rio-157
0 CR
1 MJ
1 MN
CE-100T-8
Act
1
15310-CL-CTX
EXPANSION
DS1(1-21)
DS3 EC1
Act
2
LAN
BITS
ALARM
CRAFT
UDC
Alarms Conditions History Circuits Provisioning Inventory Maintenance
Retrieve
Filter...
Help
134584

```
IP Addr   :
Booted    : 7/15/05 10:16 AM
User      : CISCO15
Authority : Superuser
SW Version: 06.00-005G-06.01
Defaults  : Factory Defaults
```

Date	Object	Eqpt Type	Slot	Port	Path Width	Sev	SA	Cond	Description
01/01/00 04:00:58 PST	SYNC-NE					NA		HLDOVRSYNC	Holdover Synchronization Mode
01/01/00 04:00:29 PST	T1-2-21	DS1_PORT	2	21		MN		LOS	Loss Of Signal
01/01/00 04:00:29 PST	T1-2-20	DS1_PORT	2	20		MN		LOS	Loss Of Signal
01/01/00 04:00:29 PST	T1-2-19	DS1_PORT	2	19		MN		LOS	Loss Of Signal
01/01/00 04:00:29 PST	T1-2-18	DS1_PORT	2	18		MN		LOS	Loss Of Signal
01/01/00 04:00:29 PST	T1-2-17	DS1_PORT	2	17		MN		LOS	Loss Of Signal
01/01/00 04:00:29 PST	T1-2-16	DS1_PORT	2	16		MN		LOS	Loss Of Signal
01/01/00 04:00:29 PST	T1-2-15	DS1_PORT	2	15		MN		LOS	Loss Of Signal
01/01/00 04:00:29 PST	T1-2-14	DS1_PORT	2	14		MN		LOS	Loss Of Signal
01/01/00 04:00:29 PST	T1-2-13	DS1_PORT	2	13		MN		LOS	Loss Of Signal
01/01/00 04:00:29 PST	T1-2-12	DS1_PORT	2	12		MN		LOS	Loss Of Signal
01/01/00 04:00:29 PST	T1-2-11	DS1_PORT	2	11		MN		LOS	Loss Of Signal
01/01/00 04:00:29 PST	T1-2-10	DS1_PORT	2	10		MN		LOS	Loss Of Signal
01/01/00 04:00:29 PST	T1-2-9	DS1_PORT	2	9		MN		LOS	Loss Of Signal
01/01/00 04:00:29 PST	T1-2-8	DS1_PORT	2	8		MN		LOS	Loss Of Signal
01/01/00 04:00:29 PST	T1-2-7	DS1_PORT	2	7		MN		LOS	Loss Of Signal

□ Exclude Same Root Cause

Retrieved: July 19, 2005 4:53:57 PM PDT

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-C84 Enable Alarm Filtering" task on page 17-104 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-C86 Suppress Alarm Reporting" task on page 17-107.

Current conditions are shown with the severity chosen in the alarm profile, if used. (For more information about alarm profiles, see the "NTP-C60 Create, Download, and Assign Alarm Severity Profiles" procedure on page 9-6.)

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 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

Note When a port is placed in the Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS) service state but is not connected to a valid signal, it generates a loss of signal (LOS) alarm.

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-C78 Search for Circuits

Purpose	This task searches for ONS 15310-CL and ONS 15310-MA circuits at the network, node, or card level.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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)**, in 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-C79 Create a 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-C29 Log into CTC, page 17-44
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, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 4 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 6.

Step 5 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 6 Click **OK**.

The alarm severity profile appears in the Alarm Profiles window.

Step 7 Right-click anywhere in the profile column to display the profile editing shortcut menu. (Refer to Step 11 for further information about the Default profile.)

Step 8 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 9 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 10 Click **OK**.

A new alarm profile (named in Step 9) 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-474-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, refer to the "DLP-C82 Apply Alarm Profiles to Cards and Nodes" task on page 17-101.)

Step 11 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:

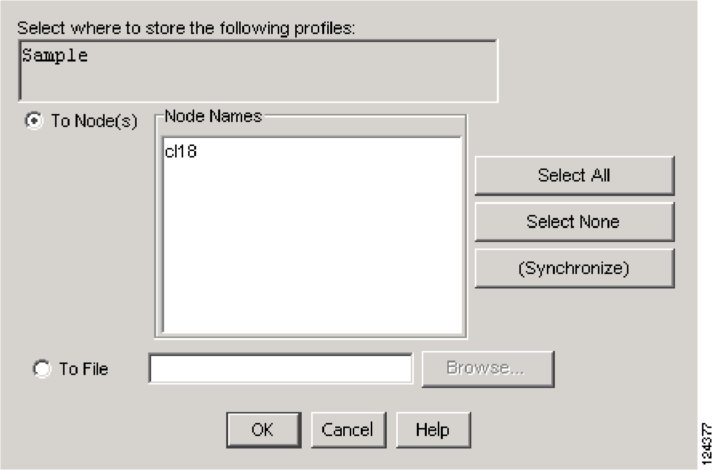
- All Critical (CR) or Major (MJ) default or user-defined severity settings are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.
- Default severities are used for all alarms and conditions until you create and apply a new profile.
- Changing a severity to inherited (I) or unset (U) does not change the severity of the alarm.

Step 12 After you have customized the new alarm profile, right-click the profile column to highlight it.

Step 13 Click **Store**.

Step 14 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 17-26).

Figure 17-26 Store Profile(s) Dialog Box



Select where to store the following profiles:

Sample

● To Node(s)

Node Names

cl18

○ To File

a. Choose the node(s) 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 15 As needed, perform any of the following actions:

- Click the **Hide Identical Rows** check box to configure the Alarm Profiles window to display rows with dissimilar severities.
- Click the **Hide Reference Values** check box to configure the Alarm Profiles window to display 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 16 Return to your originating procedure (NTP).

DLP-C80 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-C29 Log into CTC, page 17-44
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, 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 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 display 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-C81 Apply Alarm Profiles to Ports

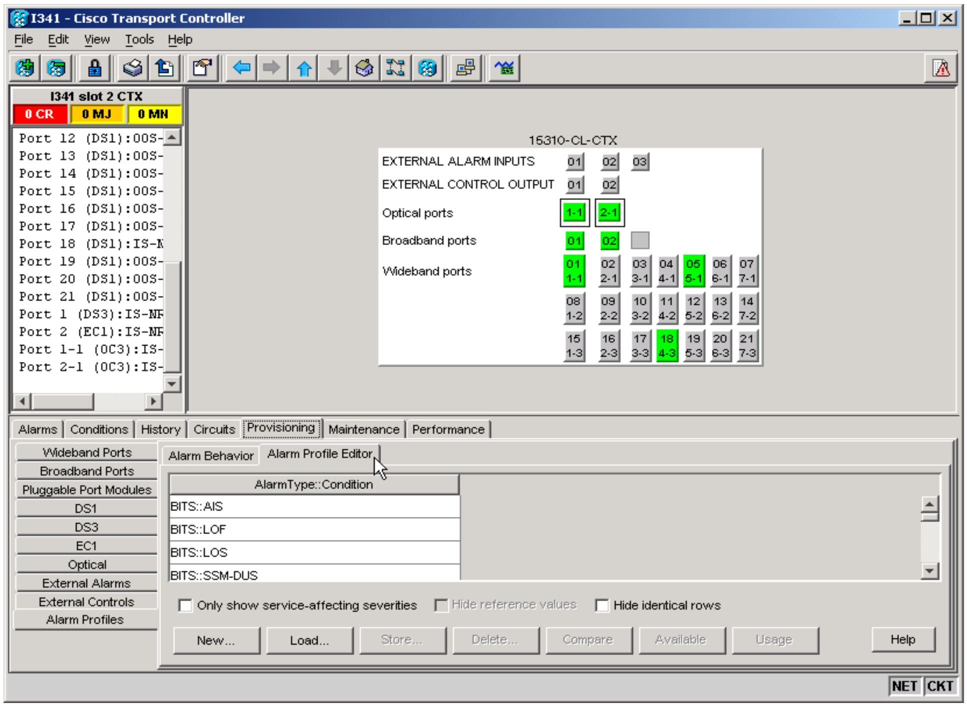
Purpose	This task applies a custom or default alarm severity profile to a port or ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-C79 Create a Cloned Alarm Severity Profile, page 17-96 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, double-click a card to open the card view.

Step 2 Click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

An ONS 15310-MA optical port profile is shown in Figure 17-27. CTC shows Parent Card Profile: Inherited.

Figure 17-27 ONS 15310-MA Card View Optical Port Alarm Profile



```
Port 12 (DS1):OOS-
Port 13 (DS1):OOS-
Port 14 (DS1):OOS-
Port 15 (DS1):OOS-
Port 16 (DS1):OOS-
Port 17 (DS1):OOS-
Port 18 (DS1):IS-N
Port 19 (DS1):OOS-
Port 20 (DS1):OOS-
Port 21 (DS1):OOS-
Port 1 (DS3):IS-NR
Port 2 (EC1):IS-NR
Port 1-1 (OC3):IS-
Port 2-1 (OC3):IS-
```

AlarmType::Condition
BITS::AIS
BITS::LOF
BITS::LOS
BITS::SSM-DUS

☐ Only show service-affecting severities ☐ Hide reference values ☐ Hide identical rows

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** menu 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**.

Step 5 To reapply a previous alarm profile after you have applied a new one, select the previous profile and click **Apply** again.

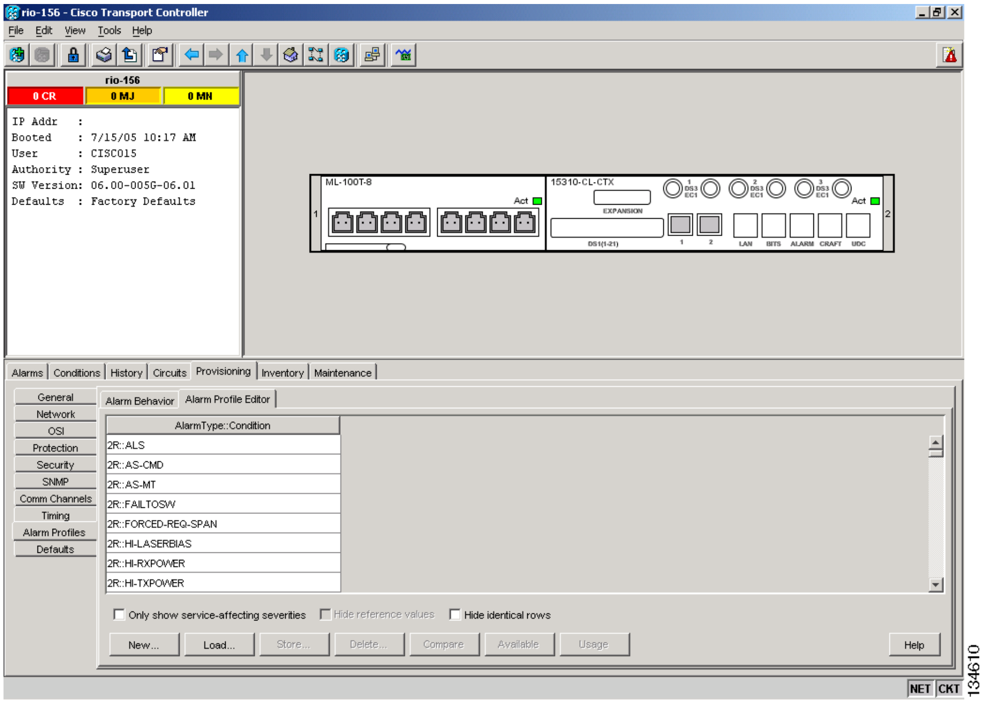
Step 6 Return to your originating procedure (NTP).

DLP-C82 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-C79 Create a Cloned Alarm Severity Profile, page 17-96 DLP-C29 Log into CTC, page 17-44
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 Profile Editor** tabs (Figure 17-28). In the figure, and ONS 15310-CL is shown.

Figure 17-28 Example Card View Alarm Profile of an ONS 15310-CL-CTX Card



```
IP Addr    :
Booted     : 7/15/05 10:17 AM
User       : CISCO15
Authority  : Superuser
SW Version: 06.00-005G-06.01
Defaults   : Factory Defaults
```

AlarmType::Condition
2R::ALS
2R::AS-CMD
2R::AS-MT
2R::FAILTOSW
2R::FORCED-REQ-SPAN
2R::HI-LASERBIAS
2R::HI-RXPOWER
2R::HI-TXPOWER

☐ Only show service-affecting severities ☐ Hide reference values ☐ Hide identical rows

Step 2 To apply profiles to a card:

- **a.** Click the Profile row 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** menu arrow at the bottom of the window (Figure 17-28).
- **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-C83 Delete Alarm Severity Profiles

Purpose	This task deletes a custom or default alarm severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs.

Step 3 To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

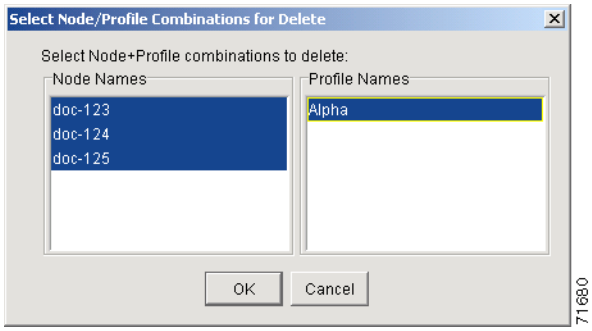
Step 4 To access the profile editor from a card view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 5 Click the profile you are deleting to select it.

Step 6 Click **Delete**.

The Select Node/Profile Combination for Delete dialog box appears (Figure 17-29).

Figure 17-29 Select Node/Profile Combination For Delete Dialog Box



Select Node/Profile Combinations for Delete

Select Node+Profile combinations to delete:

Node Names
doc-123
doc-124
doc-125

Profile Names
Alpha

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 11.

Step 7 Click the node name(s) 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 8 Click the profile name(s) you want to delete in the Profile Names list.

Step 9 Click **OK**.

Step 10 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 11 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 12 Return to your originating procedure (NTP).

DLP-C84 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-C29 Log into CTC, page 17-44
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.

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-C85 Modify Alarm and Condition Filtering Parameters

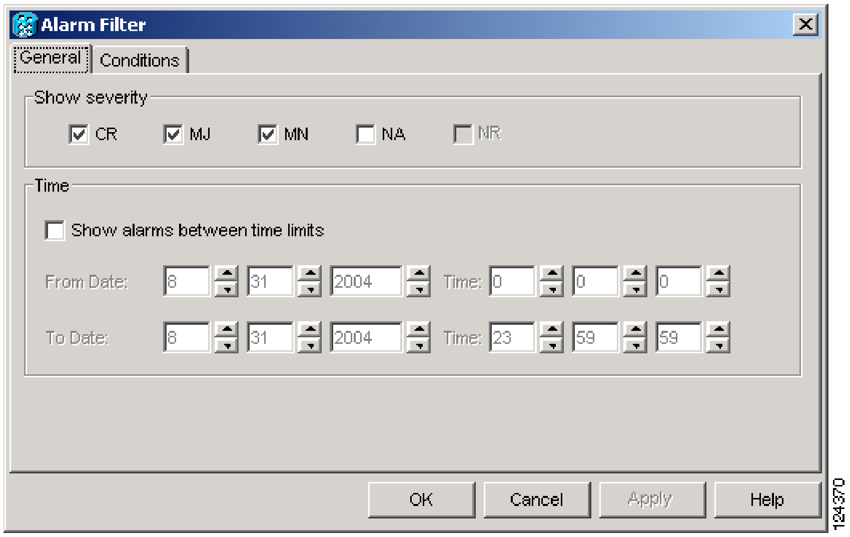
Purpose	This task changes alarm and condition reporting in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-C84 Enable Alarm Filtering, page 17-104 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 At the node, network, or card view, click the **Alarms** tab, **Conditions** tab, or **History** tab.

Step 2 Click the **Filter** command button at the lower-left of the bottom toolbar.

The filter dialog box appears, displaying the General tab. Figure 17-30 shows the Alarm Filter dialog box; the Conditions and History tabs have similar dialog boxes.

Figure 17-30 Alarm Filter Dialog Box General Tab



Alarm Filter

Show severity

☑ CR ☑ MJ ☑ MN □ NA □ NR

Time

□ Show alarms between time limits

From Date: 8 31 2004 Time: 0 0 0

To Date: 8 31 2004 Time: 23 59 59

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.

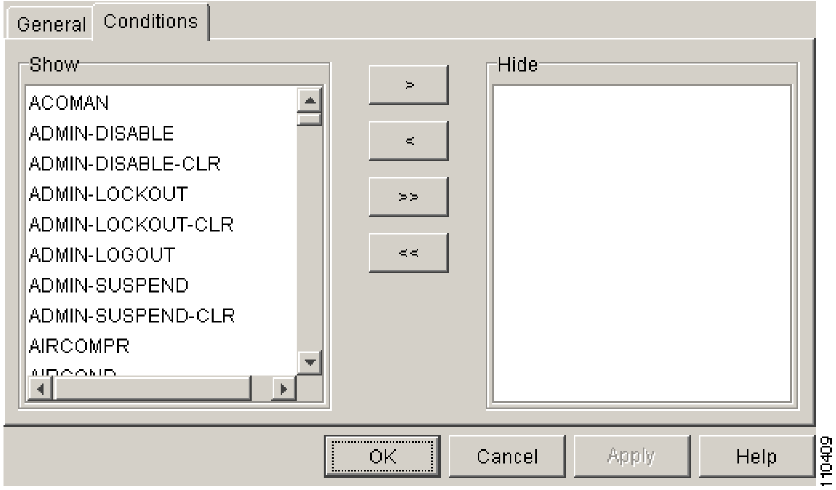
When alarm filtering is disabled, all alarms show.

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 17-31).

Figure 17-31 Alarm Filter Dialog Box Conditions Tab



ACOMAN
ADMIN-DISABLE
ADMIN-DISABLE-CLR
ADMIN-LOCKOUT
ADMIN-LOCKOUT-CLR
ADMIN-LOGOUT
ADMIN-SUSPEND
ADMIN-SUSPEND-CLR
AIRCOMPR

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-C84 Enable Alarm Filtering" task on page 17-104), and the parameters are not enforced when alarm filtering is disabled (see the "DLP-C88 Disable Alarm Filtering" task on page 17-109).

Step 7 Return to your originating procedure (NTP).

DLP-C86 Suppress Alarm Reporting

Purpose	This task suppresses the reporting of ONS 15310-CL/ONS 15310-MA alarms at the node, card, or port level.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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; this alarm will show System 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 (Figure 17-23 on page 17-88).

Alarms that directly apply to this card will change appearance as described in Step 2. For example, if you suppressed raised alarms for a CE 100T-8 card in Slot 2, 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 (i.e., the AS-CMD object will be “SLOT-2.”

Step 4 Click **Apply**.

Step 5 To suppress alarms for individual card ports double-click the card in node view.

Step 6 Click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

Step 7 Check the **Suppress Alarms** column check box for the port row where you want to suppress alarms (Figure 17-23 on page 17-88).

Step 8 Click **Apply**.

Alarms that apply directly to this port will change appearance as described in Step 2. (However, alarms raised on the 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 2 CE 100T-8 card, the alarm object will show "FAC-2-1."

Step 9 Return to your originating procedure (NTP).

DLP-C87 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-C86 Suppress Alarm Reporting, page 17-107 DLP-C29 Log into CTC, page 17-44
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 may have previously been cleared from the window using the Synchronize button.) The alarms suppressed by user command (AS-CMD) condition 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 may have previously been cleared from the window using the Synchronize button.) The AS-CMD condition with the slot object (for example, SLOT-2) will be cleared in all views.

Step 3 Uncheck the **Suppress Alarms** check box for the ports you no longer want to suppress.

Step 4 Click **Apply**.

Suppressed alarms will reappear in the Alarms window. (They may have previously been cleared from the window using the Synchronize button.) The AS-CMD condition with the port object (for example, FAC-2-1) will be cleared in all views.

Step 5 Return to your originating procedure (NTP).

DLP-C88 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-C84 Enable Alarm Filtering, page 17-104 DLP-C29 Log into CTC, page 17-44
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.

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-C89 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-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the 15310-CL-CTX card, the CTX2500 card, or the Ethernet card. The card view appears.

Step 2 Click the **Performance** tab.

- To refresh PM Counts for optical ports, click the **Optical** tab.
- To refresh PM Counts for ML-Series and CE-Series Ethernet cards, click the **Ether Ports > History** tabs or **POS Ports > History** tabs.

Step 3 From the Port drop-down list, choose the target port to highlight your selection.

Step 4 Click **Refresh**. The PM counts for the newly selected port appear.

Step 5 Return to your originating procedure (NTP).

DLP-C90 Refresh Electrical or Optical PM Counts at Fifteen-Minute Intervals

Purpose	This task changes the window view to display PM counts in 15-minute intervals.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the 15310-CL-CTX, CTX2500 or electrical card. The card view appears.

Note In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports.

Step 2 Click the **Performance** tab.

Step 3 Click the **DS1**, **DS3**, **EC1**, or **Optical** tabs.

Step 4 Click the **15 min** radio button.

Step 5 Click **Refresh**. Performance monitoring parameters appear in 15-minute intervals synchronized with the time of day.

Step 6 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 PM number represents the counter value for each specific performance monitoring parameter.

Step 7 View the Prev-*n* columns to find PM counts for the previous 15-minute intervals.

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 states. When the problem is corrected, the subsequent 15-minute interval appears with a white background.

Step 8 Return to your originating procedure (NTP).

DLP-C91 Refresh Electrical or Optical PM Counts at One-Day Intervals

Purpose	This task changes the window to display PM parameters in 1-day intervals.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the 15310-CL-CTX, CTX2500, or electrical card. The card view appears.

Note In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports.

Step 2 Click the **Performance** tab.

Step 3 Click the **DS1**, **DS3**, **EC1**, or **Optical** tabs

Step 4 Click the **1 day** radio button.

Step 5 Click **Refresh**. Performance monitoring appears in 1-day intervals synchronized with the time of day.

Step 6 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 TCA is raised. The PM number represents the counter value for each performance monitoring parameter.

Step 7 View the Prev-*n* columns to find PM counts for the previous 1-day intervals.

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 states. When the problem is corrected, the subsequent 1-day interval appears with a white background.

Step 8 Return to your originating procedure (NTP).

DLP-C92 Monitor 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-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the 15310-CL-CTX, CTX2500, electrical, or Ethernet card. The card view appears.

Note In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports. The ONS 15310-CL and ONS 15310-MA both support Ethernet cards.

Step 2 Click the **Performance** tab.

Step 3 Click the **DS1**, **DS3**, or **Optical** tabs.

Step 4 Click the **Near End** radio button.

Step 5 Click **Refresh**. All PM parameters for the selected card on the incoming signal appear. For PM parameter definitions refer to the "Performance Monitoring" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 6 View the Curr column to find PM counts for the current time interval.

Step 7 View the Prev-*n* columns to find PM counts for the previous time intervals.

Step 8 Return to your originating procedure (NTP).

DLP-C93 Monitor Far-End PM Counts

Purpose	Use this task to view far-end PM parameters for the selected card and port.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an 15310-CL-CTX, CTX2500, electrical, or Ethernet card. The card view appears.

Note In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports. The ONS 15310-CL and ONS 15310-MA both support Ethernet cards.

Step 2 Click the **Performance** tab.

Step 3 Click the **DS1**, **DS3**, or **Optical** tabs

Step 4 Click the **Far End** radio button.

Note Only cards that allow far-end performance monitoring have this button as an option.

Step 5 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 in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual.*

Step 6 View the Curr column to find PM counts for the current time interval.

Step 7 View the Prev-*n* columns to find PM counts for the previous time intervals.

Step 8 Return to your originating procedure (NTP).

DLP-C94 Reset Current PM Counts

Purpose	This task uses the Baseline button to clear the PM count displayed in the current time interval, 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-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click a 15310-CL-CTX, CTX2500, electrical, or Ethernet card. The card view appears.

Note In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports. The ONS 15310-CL and ONS 15310-MA both support Ethernet cards.

Step 2 Click the **Performance** tab.

- To reset current PM Counts for optical ports click the **Optical** tab.
- To reset current PM Counts for electrical ports click the **DS1, DS3,** or **EC1** tabs.

- To reset current PM counts for ML-Series and CE-Series Ethernet cards click the **Ether Ports > Statistics** tabs or **POS Ports > Statistics** tabs.

Step 3 Click **Baseline**.

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 in 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 Monitoring 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-C95 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-C29 Log into CTC, page 17-44
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 Unavailable Seconds (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 15310-CL-CTX, CTX2500, electrical, or Ethernet card. The card view appears.

Note In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports. The ONS 15310-CL and ONS 15310-MA both support Ethernet cards.

Step 2 Click the **Performance** tab.

- To clear selected PM Counts for optical ports, click the **Optical** tab.
- To clear selected PM Counts for electrical ports, click the **DS1, DS3,** or **EC1** tab.
- To clear selected PM counts for ML-Series and CE-Series Ethernet cards, click the **Ether Ports > Statistics** tabs or the **POS Ports > Statistics** tabs.

Step 3 Click **Clear**.

Step 4 On the Clear Statistics dialog box, choose one of 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 that the selected time interval, direction, and signal type counts are erased from the card and the window.

  Note This option is available only for electrical and optical ports.

- **All statistics for port** *x*: Clearing all of the 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 that all time intervals, directions, and signal type counts are erased from the card and the window.
- **All statistics for card**: Clearing all of the statistics for the card erases from the card and the window display all PM counts for all ports.

Step 5 Click **Ok**. In the confirmation dialog box, click **Yes** to clear the selected statistics.

Step 6 View the displayed columns to verify that the selected PM counts have been cleared.

Step 7 Return to your originating procedure (NTP).

DLP-C96 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-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an electrical, Ethernet, 15310-CL-CTX, or CTX2500 card. The card view appears.

Note In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports. The ONS 15310-CL and ONS 15310-MA both support Ethernet cards.

Step 2 Click the **Performance** tab.

- To set the auto-refresh interval for optical ports click the **Optical** tab.
- To set the auto-refresh interval for electrical ports click the **DS1, DS3,** or **EC1** tabs.
- To set the auto-refresh interval for ML-Series and CE-Series Ethernet cards click the **Ether Ports > Statistics** tabs or **POS Ports > Statistics** tabs.

Step 3 Click the Auto-refresh drop-down list and 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 displayed PM counts are not updated unless you click the Refresh button.

Step 5 Return to your originating procedure (NTP).

DLP-C97 Monitor PM Counts for Selected Signal Types

Purpose	This task enables you to monitor near-end or far-end PM counts for specific signals on a selected card and port.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click a 15310-CL-CTX, CTX2500, electrical, or Ethernet card. The card view appears.

Note In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports. The ONS 15310-CL and ONS 15310-MA both support Ethernet cards.

Step 2 Click the **Performance** tab.

Step 3 Click the **DS1, DS3, EC1,** or **Optical** tabs.

Note Different port and signal-type drop-down lists appear depending on the port type and the circuit type. The appropriate types (DS1, DS3, VT path, STS path, OC-N section, and OC-N line) appear based on the card.

Step 4 Click the **Port/Line** drop-down list and highlight the desired port/line. (Options vary depending on the port.)

Step 5 Click the **signal type** drop-down list and highlight the desired signal. (Options vary depending on the port.)

Step 6 Click **Refresh**. All PM counts recorded by the near-end or far-end node appear for the specified outgoing signal type on the selected card and port. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 7 View the Curr column to find PM counts for the current time interval.

Step 8 View the Prev-*n* columns to find PM counts for the previous time intervals.

Step 9 Return to your originating procedure (NTP).

DLP-C98 Enable Pointer Justification Count Performance Monitoring

Purpose	This task enables pointer justification counts, which provide a way to align the phase variations in STS and VT payloads and to monitor the clock synchronization between nodes. A consistent, large pointer justification count indicates clock synchronization problems between nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the 15310-CL-CTX or CTX2500 card. The card view appears.

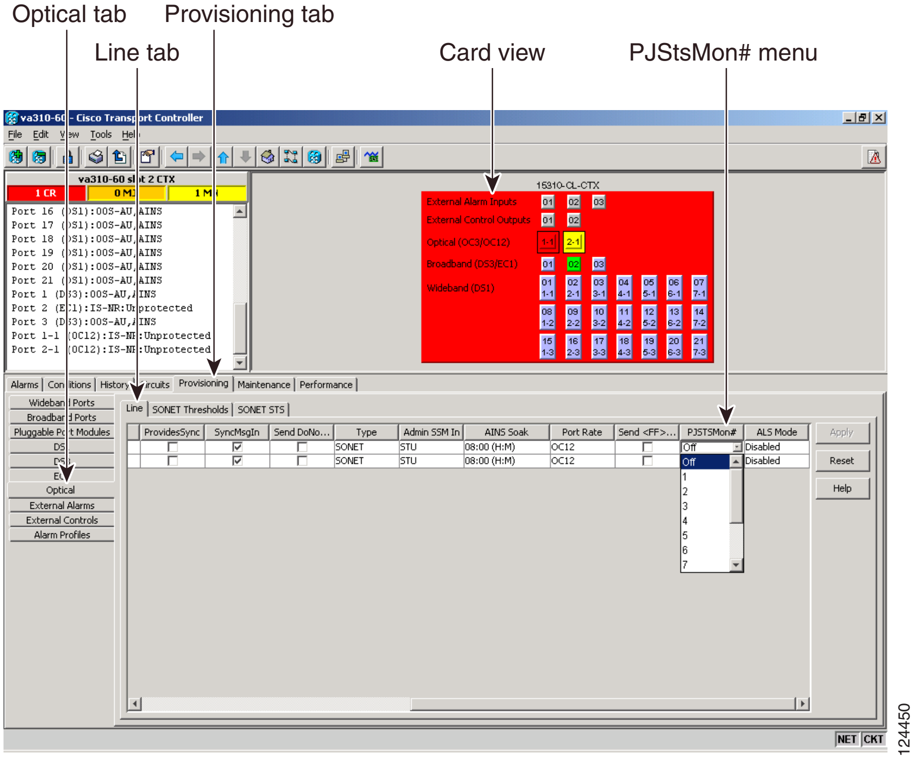
Step 2 Click the **Provisioning > Optical > Line** tabs.

Step 3 Click the **PJStsMon#** menu and make a selection based on the following rules:

- The default value Off means pointer justification monitoring is disabled.
- The values 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 17-32 shows the PJStsMon# drop-down list on the Provisioning window.

Figure 17-32 Line Tab for Enabling Pointer Justification Count Parameters



```
Port 16 (DS1):OOS-AU,AINS
Port 17 (DS1):OOS-AU,AINS
Port 18 (DS1):OOS-AU,AINS
Port 19 (DS1):OOS-AU,AINS
Port 20 (DS1):OOS-AU,AINS
Port 21 (DS1):OOS-AU,AINS
Port 1 (DS3):OOS-AU,AINS
Port 2 (EC1):IS-NR:Unprotected
Port 3 (DS3):OOS-AU,AINS
Port 1-1 (OC12):IS-NR:Unprotected
Port 2-1 (OC12):IS-NR:Unprotected
```

	ProvidesSync	SyncMsgIn	Send DoNo...	Type	Admin SSM In	AINS Soak	Port Rate	Send <FF>...	PJSTSMon#	ALS Mode
	□	☑	□	SONET	STU	08:00 (H:M)	OC12	□	Off	Disabled
	□	☑	□	SONET	STU	08:00 (H:M)	OC12	□	Off 1 2 3 4 5 6 7	Disabled

Step 4 In the Service State field, confirm that the port is in the In-Service and Normal (IS-NR) service state.

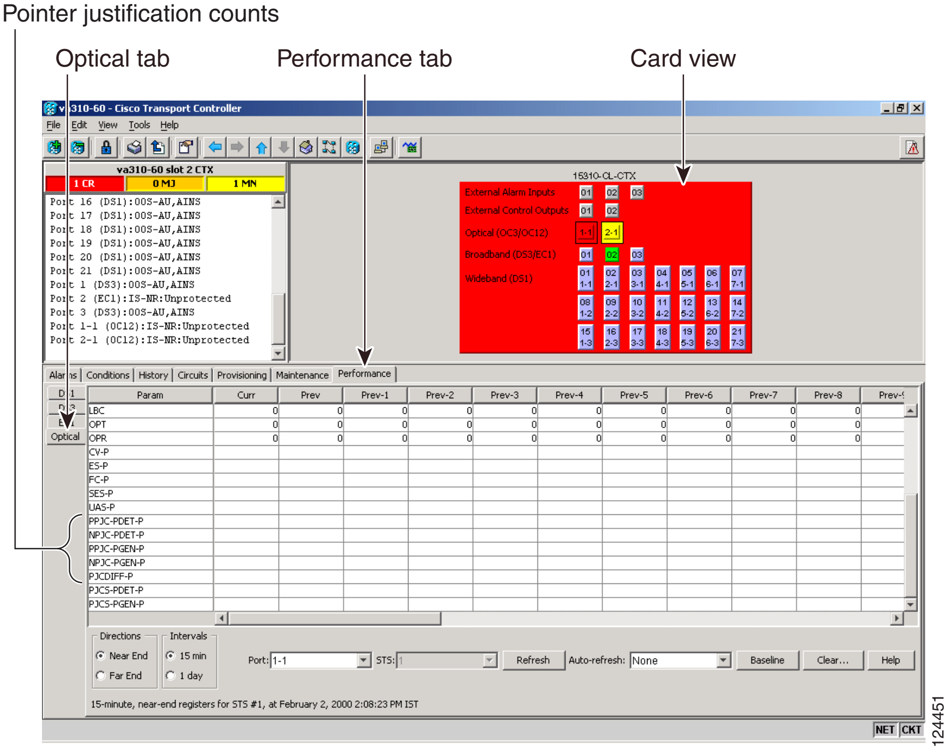
Step 5 If the port is IS-NR, click **Apply** and go to Step 7.

Step 6 If the port is in the Out-of-Service and Disabled (OOS,DSLBD); Out-of-Service and Maintenance (OOS,MT); or In-Service and Automatic In-Service (IS,AINS), select **IS** in the Admin State field and click **Apply**.

Step 7 Click the **Performance** tab to view PM parameters. Figure 17-33 shows pointer justification counts. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for more PM information, details, and definitions.

Note In CTC, the count fields for PPJC and NPJC PM parameters appear white and blank unless they are enabled on the Provisioning > Optical > Line tabs.

Figure 17-33 Viewing Pointer Justification Counts



```
Port 16 (DS1):OOS-AU,AINS
Port 17 (DS1):OOS-AU,AINS
Port 18 (DS1):OOS-AU,AINS
Port 19 (DS1):OOS-AU,AINS
Port 20 (DS1):OOS-AU,AINS
Port 21 (DS1):OOS-AU,AINS
Port 1 (DS3):OOS-AU,AINS
Port 2 (EC1):IS-NR:Unprotected
Port 3 (DS3):OOS-AU,AINS
Port 1-1 (OC12):IS-NR:Unprotected
Port 2-1 (OC12):IS-NR:Unprotected
```

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9
LBC	0	0	0	0	0	0	0	0	0	0	
OPT	0	0	0	0	0	0	0	0	0	0	
OPR	0	0	0	0	0	0	0	0	0	0	
CV-P											
ES-P											
FC-P											
SES-P											
UAS-P											
PPJC-PDET-P											
NPJC-PDET-P											
PPJC-PGEN-P											
NPJC-PGEN-P											
PJCDIFF-P											
PJCS-PDET-P											
PJCS-PGEN-P											

Directions: ● Near End ○ Far End
Intervals: ● 15 min ○ 1 day
Port: 1-1 STS: 1 Refresh Auto-refresh: None Baseline Clear... Help

15-minute, near-end registers for STS #1, at February 2, 2000 2:08:23 PM IST

Step 8 Return to your originating procedure (NTP).

DLP-C99 Enable Intermediate-Path Performance Monitoring

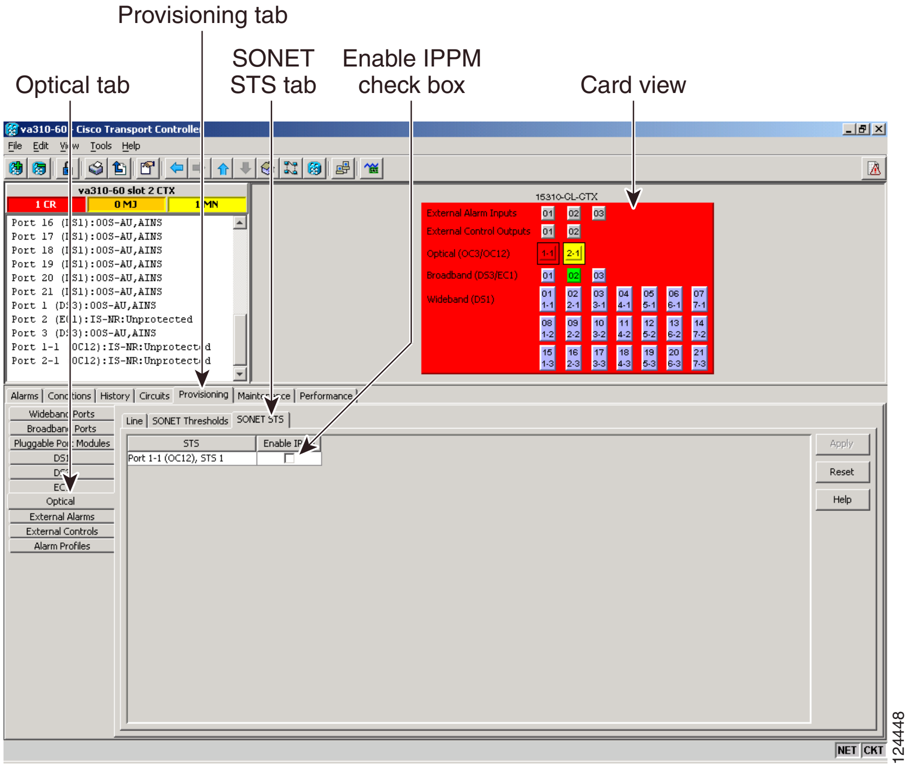
Purpose	This task enables intermediate-path performance monitoring (IPPM), which allows you to monitor large amounts of STS traffic through intermediate nodes. This task also enables IIPM VT in the ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As 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. For more information about IPPM parameters, refer to the “Performance Monitoring” chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 1 In node view, double-click the 15310-CL-CTX or CTX2500 card. The card view appears.

Step 2 Click the **Provisioning > Optical > SONET STS** tabs. Figure 17-34 shows the SONET STS tab in the Provisioning window.

Figure 17-34 SONET STS Tab for Enabling IPPM



```
Port 16 (DS1):OOS-AU,AINS
Port 17 (DS1):OOS-AU,AINS
Port 18 (DS1):OOS-AU,AINS
Port 19 (DS1):OOS-AU,AINS
Port 20 (DS1):OOS-AU,AINS
Port 21 (DS1):OOS-AU,AINS
Port 1 (DS3):OOS-AU,AINS
Port 2 (EC1):IS-NR:Unprotected
Port 3 (DS3):OOS-AU,AINS
Port 1-1 (OC12):IS-NR:Unprotected
Port 2-1 (OC12):IS-NR:Unprotected
```

STS	Enable IPPM
Port 1-1 (OC12), STS 1	□

Step 3 Check the check box in the Enable IPPM column for the STS you want to monitor.

Step 4 Click **Apply**.

Step 5 Click the **Performance** tab to view PM parameters. For IPPM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 6 Return to your originating procedure (NTP).

CHAPTER 18

DLPs C100 to C199

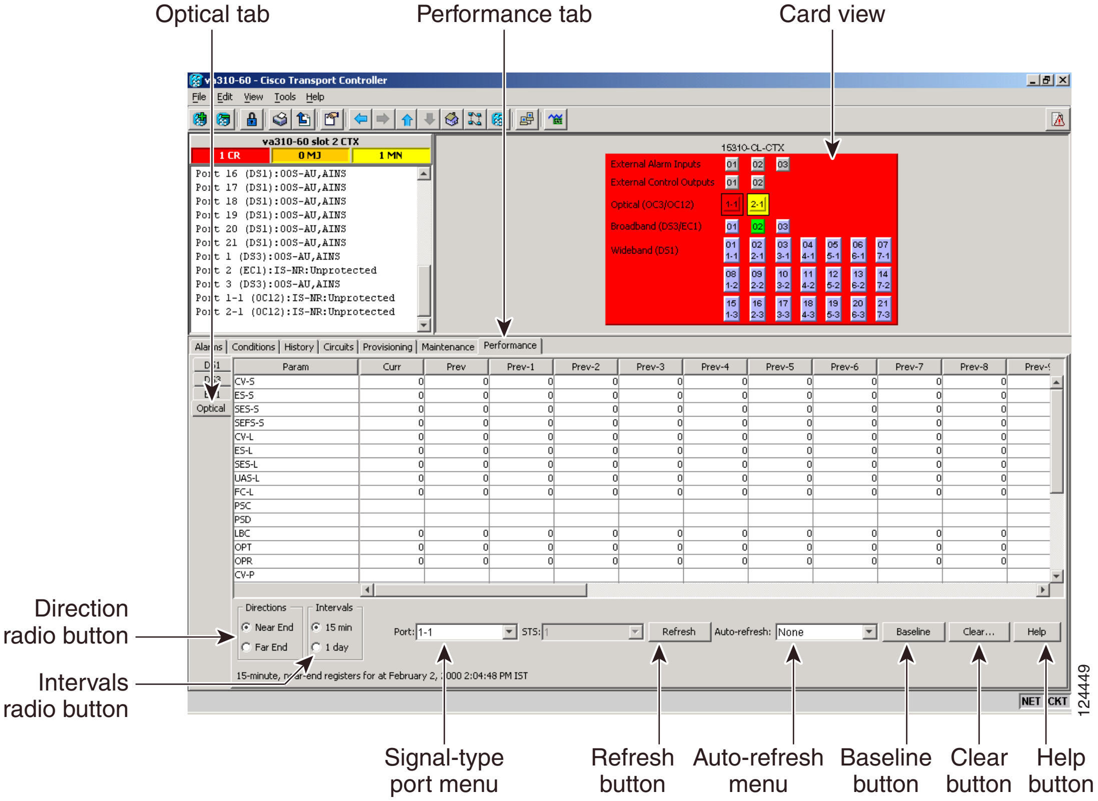
DLP-C100 View Optical OC-N PM Parameters

Purpose	This task enables you to view PM counts on an optical (OC-N) port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the 15310-CL-CTX or CTX2500 card. The card view appears.

Step 2 Click the **Performance > Optical** tabs (Figure 18-1).

Figure 18-1 Viewing Optical Performance Monitoring Information


Optical tab
Performance tab
Card view
Direction radio button
Intervals radio button
Signal-type port menu
Refresh button
Auto-refresh menu
Baseline button
Clear button
Help button
124449
va310-60 - Cisco Transport Controller
File Edit View Tools Help
15310-CL-CTX
External Alarm Inputs 01 02 03
External Control Outputs 01 02
Optical (OC3/OC12) 1-1 2-1
Broadband (DS3/EC1) 01 02 03
Wideband (DS1) 01 1-1 02 2-1 03 3-1 04 4-1 05 5-1 06 6-1 07 7-1 08 1-2 09 2-2 10 3-2 11 4-2 12 5-2 13 6-2 14 7-2 15 1-3 16 2-3 17 3-3 18 4-3 19 5-3 20 6-3 21 7-3
Alarms Conditions History Circuits Provisioning Maintenance Performance
DS1 DS3 EC1 Optical
Refresh Baseline Clear... Help
NET CKT

va310-60 slot 2 CTX

1 CR | 0 MJ | 1 MN

```
Port 16 (DS1):OOS-AU,AINS
Port 17 (DS1):OOS-AU,AINS
Port 18 (DS1):OOS-AU,AINS
Port 19 (DS1):OOS-AU,AINS
Port 20 (DS1):OOS-AU,AINS
Port 21 (DS1):OOS-AU,AINS
Port 1 (DS3):OOS-AU,AINS
Port 2 (EC1):IS-NR:Unprotected
Port 3 (DS3):OOS-AU,AINS
Port 1-1 (OC12):IS-NR:Unprotected
Port 2-1 (OC12):IS-NR:Unprotected
```

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9
CV-S	0	0	0	0	0	0	0	0	0	0	
ES-S	0	0	0	0	0	0	0	0	0	0	
SES-S	0	0	0	0	0	0	0	0	0	0	
SEFS-S	0	0	0	0	0	0	0	0	0	0	
CV-L	0	0	0	0	0	0	0	0	0	0	
ES-L	0	0	0	0	0	0	0	0	0	0	
SES-L	0	0	0	0	0	0	0	0	0	0	
UAS-L	0	0	0	0	0	0	0	0	0	0	
FC-L	0	0	0	0	0	0	0	0	0	0	
PSC											
PSD											
LBC	0	0	0	0	0	0	0	0	0	0	
OPT	0	0	0	0	0	0	0	0	0	0	
OPR	0	0	0	0	0	0	0	0	0	0	
CV-P											

Directions: ● Near End ○ Far End

Intervals: ● 15 min ○ 1 day

Port: 1-1 STS: 1 Auto-refresh: None

15-minute, near-end registers for at February 2, 2000 2:04:48 PM IST

Step 3 The PM parameter names appear on the left side of the window in the Param column. The PM values appear on the right side of the window in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 4 Return to your originating procedure (NTP).

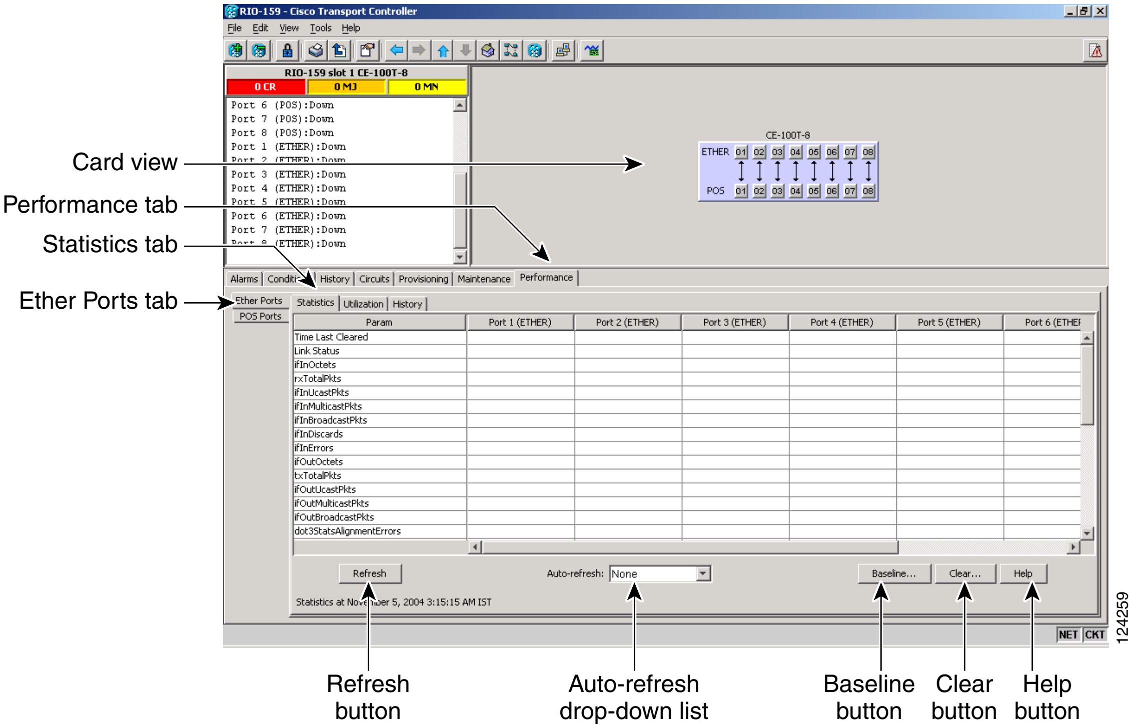
DLP-C101 View Ether Ports and POS Ports Statistics PM Parameters

Purpose	This task enables you to view current statistical PM counts on a CE-Series or ML-Series Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click a CE-Series or ML-Series Ethernet card. The card view appears.

Step 2 Click the **Performance > Ether Ports > Statistics** tabs or the **Performance > POS Ports > Statistics** tabs (Figure 18-2).

Figure 18-2 Statistics Window on the CE, ML Card View Performance Tab



RIO-159 - Cisco Transport Controller
File Edit View Tools Help
RIO-159 slot 1 CE-100T-8
0 CR
0 MJ
0 MN
CE-100T-8
ETHER 01 02 03 04 05 06 07 08
POS 01 02 03 04 05 06 07 08
Card view
Performance tab
Statistics tab
Ether Ports tab
Alarms | Conditions | History | Circuits | Provisioning | Maintenance | Performance
Ether Ports
POS Ports
Statistics | Utilization | History
Refresh
Auto-refresh: None
Baseline...
Clear...
Help
NET CKT
124259
Refresh button
Auto-refresh drop-down list
Baseline button
Clear button
Help button

```
Port 6 (POS):Down
Port 7 (POS):Down
Port 8 (POS):Down
Port 1 (ETHER):Down
Port 2 (ETHER):Down
Port 3 (ETHER):Down
Port 4 (ETHER):Down
Port 5 (ETHER):Down
Port 6 (ETHER):Down
Port 7 (ETHER):Down
Port 8 (ETHER):Down
```

Param	Port 1 (ETHER)	Port 2 (ETHER)	Port 3 (ETHER)	Port 4 (ETHER)	Port 5 (ETHER)	Port 6 (ETHEI
Time Last Cleared						
Link Status						
ifInOctets						
rxTotalPkts						
ifInUcastPkts						
ifInMulticastPkts						
ifInBroadcastPkts						
ifInDiscards						
ifInErrors						
ifOutOctets						
txTotalPkts						
ifOutUcastPkts						
ifOutMulticastPkts						
ifOutBroadcastPkts						
dot3StatsAlignmentErrors						

Statistics at November 5, 2004 3:15:15 AM IST

Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

The PM parameter names appear on the left side of the window in the Param column. The parameter numbers appear on the right side of the window in the Port # columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 4 View the Port # columns to see the current PM statistics for each port.

Step 5 Return to your originating procedure (NTP).

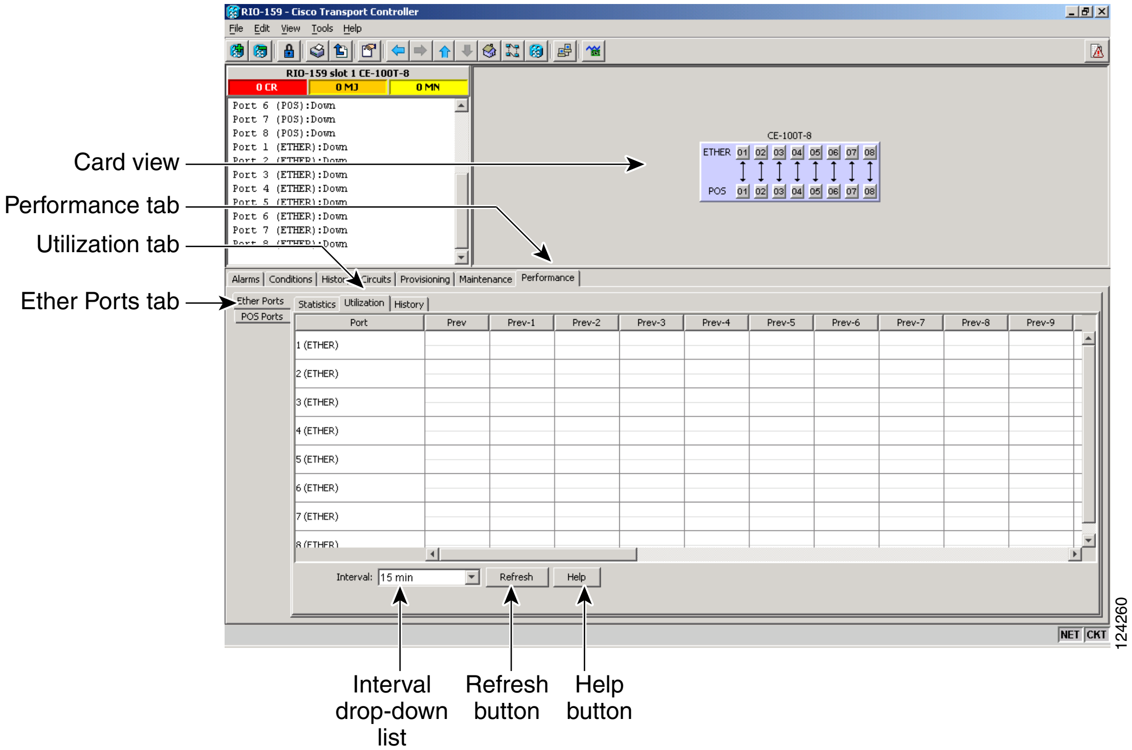
DLP-C102 View Ether Ports and POS Ports Utilization PM Parameters

Purpose	This task enables you to view line utilization PM counts on a CE-Series or an ML-Series Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click a CE-Series or ML-Series Ethernet card. The card view appears.

Step 2 Click the **Performance > Ether Ports > Utilization** tabs or the **Performance > POS Ports > Utilization** tabs (Figure 18-3).

Figure 18-3 Utilization Window on the Card View Performance Tab for CE-Series and ML-Series Cards



```
Port 6 (POS):Down
Port 7 (POS):Down
Port 8 (POS):Down
Port 1 (ETHER):Down
Port 2 (ETHER):Down
Port 3 (ETHER):Down
Port 4 (ETHER):Down
Port 5 (ETHER):Down
Port 6 (ETHER):Down
Port 7 (ETHER):Down
Port 8 (ETHER):Down
```

Port	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9
1 (ETHER)										
2 (ETHER)										
3 (ETHER)										
4 (ETHER)										
5 (ETHER)										
6 (ETHER)										
7 (ETHER)										
8 (ETHER)										

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 View the Prev-*n* columns to find Tx and Rx bandwidth utilization values for the previous time intervals.

Step 6 Return to your originating procedure (NTP).

DLP-C103 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-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click a CE-Series or ML-Series Ethernet card. The card view appears.

Step 2 Click the **Performance > Ether Ports** tabs or the **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 displays the specified PM counts in one-minute time intervals.
- **15 min**: This option displays the specified PM counts in fifteen-minute time intervals.
- **1 hour**: This option displays the specified PM counts in one-hour time intervals.
- **1 day**: This option displays the specified PM counts in one-day (24-hour) time intervals.

Step 5 Click **Refresh**. The PM counts refresh with values based on the chosen time interval.

Step 6 Return to your originating procedure (NTP).

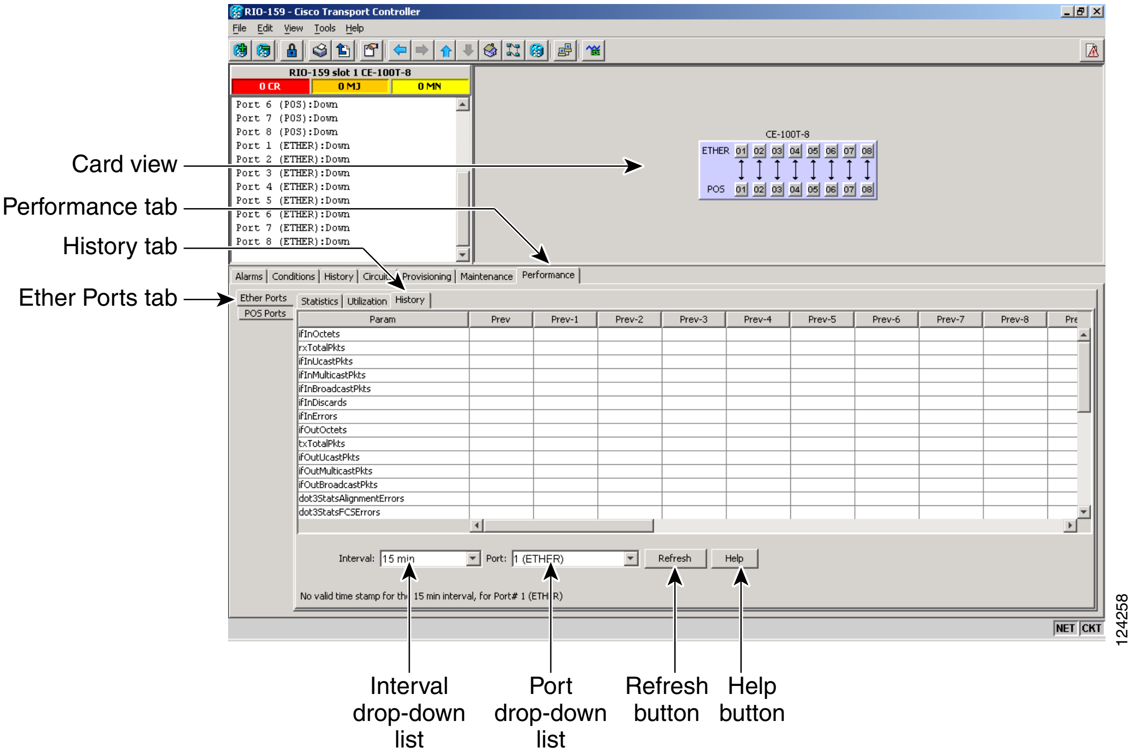
DLP-C104 View Ether Ports and POS Ports History PM Parameters

Purpose	This task enables you to view historical PM counts at selected time intervals on a CE-Series or an ML-Series Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click a CE-Series or an ML-Series Ethernet card. The card view appears.

Step 2 Click the **Performance > Ether Ports > History** tabs or the **Performance > POS Ports > History** tabs (Figure 18-4).

Figure 18-4 History Window on the Card View Performance Tab



RIO-159 slot 1 CE-100T-8

0 CR | 0 MJ | 0 MN

```
Port 6 (POS):Down
Port 7 (POS):Down
Port 8 (POS):Down
Port 1 (ETHER):Down
Port 2 (ETHER):Down
Port 3 (ETHER):Down
Port 4 (ETHER):Down
Port 5 (ETHER):Down
Port 6 (ETHER):Down
Port 7 (ETHER):Down
Port 8 (ETHER):Down
```

Param	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Pre
ifInOctets										
rxTotalPkts										
ifInUcastPkts										
ifInMulticastPkts										
ifInBroadcastPkts										
ifInDiscards										
ifInErrors										
ifOutOctets										
txTotalPkts										
ifOutUcastPkts										
ifOutMulticastPkts										
ifOutBroadcastPkts										
dot3StatsAlignmentErrors										
dot3StatsFCSErrors										

Interval: 15 min Port: 1 (ETHER)

No valid time stamp for the 15 min interval, for Port# 1 (ETHER)

RIO-159 - Cisco Transport Controller
File Edit View Tools Help
CE-100T-8
ETHER 01 02 03 04 05 06 07 08
POS 01 02 03 04 05 06 07 08
Alarms | Conditions | History | Circuits | Provisioning | Maintenance | Performance
Ether Ports
POS Ports
Statistics | Utilization | History
Refresh
Help
NET CKT
Card view
Performance tab
History tab
Ether Ports tab
Interval drop-down list
Port drop-down list
Refresh button
Help button
124258

Step 3 Click **Refresh**. Performance monitoring statistics appear for each port on the card.

The PM parameter names appear on the left side of the window in the Param column. The parameter numbers appear on the right side of the window in the Port # columns. For PM parameter definitions refer to the "Performance Monitoring" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 4 View the Port # columns to see the current PM statistics for each port.

Step 5 Return to your originating procedure (NTP)

DLP-C105 Create Ethernet RMON Alarm Thresholds

Purpose	This task sets up RMON to allow network management systems to monitor Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The CE-100T-8 uses the ONG RMON. The ONG RMON contains the statistics, history, alarms, and events MIB groups from the standard RMON MIB.

Note ONG RMON is recommended for the ML-100T-8 card. The standard Cisco IOS RMON is also available.

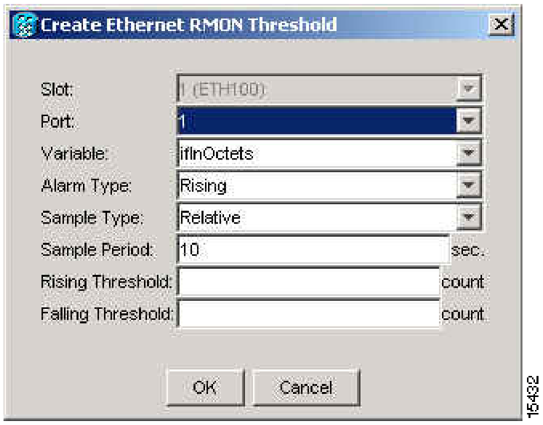
Step 1 Double-click the Ethernet card where you want to create the RMON alarm thresholds.

Step 2 In card view, click the **Provisioning > Ether Ports > RMON Thresholds** tabs or the **Provisioning > POS Ports > RMON Thresholds** for CE-Series and ML-Series Ethernet cards.

Step 3 Click **Create**.

The Create Threshold dialog box appears (Figure 18-5).

Figure 18-5 Creating RMON Thresholds



Create Ethernet RMON Threshold

Slot: 1 (ETH100)
Port: 1
Variable: ifInOctets
Alarm Type: Rising
Sample Type: Relative
Sample Period: 10 sec.
Rising Threshold: count
Falling Threshold: count

Step 4 From the Slot drop-down list, choose the appropriate Ethernet card.

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.

In the POS Ports Create Threshold window, the variables that appear in the Variable drop-down list depend on the framing mode used by the cards. The two framing modes for the POS port on the CE-Series and ML-Series cards are HDLC (High-Level Data Link Control) and GFP-F (frame-mapped generic framing procedure).

Table 18-1 provides a list of the Ether ports threshold variables available in this field.

Table 18-1 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	Number of multicast frames received error free

Table 18-1 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
ifInBroadcastPkts	The number of packets, delivered by this sublayer to a higher (sub)layer, which were addressed to a broadcast address at this sublayer
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
ifOutUcastPkts	Total number of unicast packets requested to transmit to a single address
ifOutMulticastPkts	Number of multicast frames transmitted error free
ifOutBroadcastPkts	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sublayer, including those that were discarded or not sent
txTotalPkts	Total number of transmit packets
rxTotalPkts	Total number of receive packets
dot3statsAlignmentErrors	Number of frames with an alignment error, that is, frames with a length that is not an integral number of octets and where the frame cannot pass the frame check sequence (FCS) test
dot3StatsFCSErrors	Number of frames with framecheck errors, that is, where there is an integral number of octets, but an incorrect FCS
dot3StatsSingleCollisionFrames	Number of successfully transmitted frames that had exactly one collision
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
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
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address; this does not include multicast packets

Table 18-1 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
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
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
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

Table 18-2 provides a list of the POS ports threshold variables for HDLC mode.

Table 18-2 POS Threshold Variables for HDLC Mode (MIBs)

Parameter	Definition
iflnOctets	The total number of octets received on the interface, including framing octets
txTotalPkts	The total number of transmit packets
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	The total number of transmitted octets, including framing packets
rxTotalPkts	The total number of receive packets
ifOutOversizePkts	Number of packets larger than 1518 bytes sent out into SONET; packets larger than 1600 bytes do not get transmitted.
mediaIndStatsRxFramesBadCRC	A count of the received Fibre Channel frames with errored cyclic redundancy checks (CRCs).
hdlcRxAborts	Number of received packets aborted before input

Table 18-2 POS Threshold Variables for HDLC Mode (MIBs) (continued)

Parameter	Definition
ifInPayloadCRCErrors	The number of receive data frames with payload CRC errors
ifOutPayloadCRCErrors	The number of transmit data frames with payload CRC errors

Table 18-3 provides a list of the POS ports threshold variables for GFP-F mode.

Table 18-3 POS Threshold Variables for GFP-F Mode (MIBs)

Variable	Definition
iflnOctets	The total number of octets received on the interface, including framing octets
txTotalPkts	The total number of transmit packets
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	The total number of transmitted octets, including framing packets
rxTotalPkts	The total number of receive packets
ifOutOversizePkts	Number of packets larger than 1518 bytes sent out into SONET; packets larger than 1600 bytes do not get transmitted.
gfpStatsRxSBitErrors	Receive frames with Single Bit Errors (cHEC, tHEC, eHEC)
gfpStatsRxMBitErrors	Receive frames with Multi Bit Errors (cHEC, tHEC, eHEC)
gfpStatsRxTypeInvalid	Receive frames with invalid type (PTI, EXI, UPI)
gfpStatsRxCRCErrors	Receive data frames with Payload CRC errors
gfpStatsRxCIDInvalid	Receive frames with Invalid CID
gfpStatsCSFRaised	Number of receive (Rx) client management frames with Client Signal Fail indication
ifInPayloadCRCErrors	The number of receive data frames with payload CRC errors
ifOutPayloadCRCErrors	The number of transmit data frames with payload CRC 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 **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 Enter an appropriate number of seconds for the Sample Period.

Step 10 Enter the appropriate number of occurrences for the Rising Threshold.

Note 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.

Note 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 seconds subsides and creates only 799 collisions in 15 seconds, 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-second 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-C106 Delete Ethernet RMON Alarm Thresholds

Purpose	This task deletes RMON threshold crossing alarms for Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-C68 Create or Delete Ethernet RMON Thresholds, page 8-5 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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 or the **Provisioning > POS Ports > 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 that threshold.

Step 6 Return to your originating procedure (NTP).

DLP-C107 View Circuit Information

Purpose	This task provides information about ONS 15310-CL and ONS 15310-MA circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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.

Step 2 Click the **Circuits** tab. The Circuits tab has the following information:

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.

- 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), STS-V (STS virtual concatenated [VCAT] circuit), or VT-V (VT VCAT circuit).
- Size—Circuit size. VT circuits are 1.5. ONS 15310-CL STS circuits are 1, 3c, 6c, 9c, or 12c. ONS 15310-MA STS circuits are 1, 3c, 6c, 9c, 12c, 24c, and 48c. VCAT circuits are VT1.5-*n*v or STS-1-*n*v, where *n* is the number of members.
- Protection—The type of circuit protection. See Table 18-4 for a list of protection types.

Table 18-4 Circuit Protection Types

Protection Type	Description
1+1	The circuit is protected by a 1+1 protection group.
N/A	A circuit with connections on the same node is not protected.
Protected	The circuit is protected by diverse SONET topologies, for example, a path protection configuration and a 1+1 protection group.
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.

Table 18-4 Circuit Protection Types (continued)

Protection Type	Description
Unprot (red)	A circuit created as a fully protected circuit is no longer protected due to a system change, such as removal of a 1+1 protection group.
Path protection	The circuit is protected by a path protection configuration.

- Dir—The circuit direction, either two-way or one-way.
- Status—The circuit status. Table 18-5 lists the circuit statuses that may appear.

Table 18-5 ONS 15310-CL and ONS 15310-MA 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 circuit source to destination.
DELETING	CTC is deleting a circuit.
PARTIAL	A CTC-created circuit is missing a cross-connect or network span or a complete path from source to destinations does not exist. 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 may flow on a protect path. Network spans are in one of two states: up or down. On CTC circuit and network maps, up spans appear as green lines, and down spans appear 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 that 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 does not appear on the network map. Subsequently, circuits routed on a network span that goes down appear as DISCOVERED during the current CTC session, but 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 or circuit span (network link), and a complete path from source to destinations does not exist.
CONVERSION_PENDING	An existing circuit in a topology upgrade is set to this status. The circuit returns to the DISCOVERED status when the topology upgrade is complete.

Table 18-5 ONS 15310-CL and ONS 15310-MA Circuit Status (continued)

Status	Definition/Activity
PENDING_MERGE	Any new circuits created to represent an alternate path in a topology upgrade are set to this status to indicate that they are temporary circuits. These circuits can be deleted if a topology upgrade fails.
DROP_PENDING	A circuit is set to this status when a new circuit drop is being added.

- Source—The circuit source in the format: *node/slot/port "port name"/STS/VT*. (Port name appears in quotes.) Node and slot 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 uses a pluggable port module (PPM), the port format is *PPM-port number*, for example, p2-1. If the port is a DS-1, DS-3, or EC-1 port, port type is indicated, for example, pDS1. If the circuit size is a concatenated size (3c, 6c, 9c, 12c), STSs used in the circuit are indicated by an ellipsis, for example, S7..9, (STSs 7, 8, and 9) or S10..12 (STSs 10, 11, and 12).
- Destination—The circuit destination in same format as the circuit source.
- # of Spans—The number of inter-node 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.
- State—The circuit service state, which 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-C109 Filter the Display of Circuits

Purpose	This task filters the display of circuits in the ONS network, node, or card view Circuits window based on circuit name, size, type, direction, and other attributes.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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).
- Status—Choose a circuit status to filter the circuits. For more information about circuit statuses, see Table 18-5 on page 18-13.
- 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 18-4 on page 18-12.
- 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), or **VT Aggregation Point** (displays only VT aggregation points).
- Size—Click the appropriate check boxes to filter circuits based on size: VT circuits are 1.5. ONS 15310-CL STS circuits are 1, 3c, 6c, 9c, or 12c. ONS 15310-MA STS circuits are 1, 3c, 6c, 9c, 12c, 24c, and 48c. VCAT circuits are VT1.5-*n*v or STS-1-*n*v, where *n* is the number of members.

  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.

Step 4 To set the filter for ring, node, link, and source and drop type, click the **Advanced** tab and complete the following. 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-C110 View Circuits on a Span

Purpose	This task displays circuits routed on an ONS 15310-CL or ONS 15310-MA span.
Tools/Equipment	None
Prerequisite Procedures	Circuits must be created on the span; see Chapter 6, "Create Circuits and VT Tunnels" DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From the View menu in node view, choose **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 you want to view and choose **Circuits** to view path protection, 1+1, or unprotected circuits on the span.

In the Circuits on Span dialog box, you can view the following information for circuits provisioned on the span:

- STS—Displays STSs used by the circuits.
- VT—Displays VTs used by the circuits (VT circuits).
- Path Protection—(Path protection span only) If checked, path protection circuits are on the span.
- Circuit—Displays the circuit name.
- 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-C166 Initiate a Path Protection Force Switch on a Span" task on page 18-60 for instructions. If you want to edit a circuit on the span, double-click the circuit. See the "DLP-C112 Edit a Circuit Name" task on page 18-18 or the "DLP-C114 Edit Path Protection Circuit Path Selectors" task on page 18-20 for instructions.

Step 3 Return to your originating procedure (NTP).

DLP-C111 Change a Circuit Service State

Purpose	This task changes the service state of a circuit. For more information about circuit states, refer to the "Circuits and Tunnels" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node or network view, click the **Circuits** tab.

Step 2 Click the circuit with the service state that you want to change.

Step 3 From the Tools menu, choose **Circuits > Set Circuit State**.

Step 4 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 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 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**—(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. OOS-MA,OOG applies only 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.

Note You can also change the administrative state by clicking the **Edit** button on the Circuits tab, then clicking the **State** tab on the Edit Circuits window.

For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual.*

Step 5 If you want to apply the administrative state to the circuit source and destination ports, check the **Apply to drop ports** check box.

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.

Step 6 Click **Apply**.

Step 7 If a confirmation dialog box appears, click **Yes** to continue. If the Circuit State Transitions 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, 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-C50 Change the Service State for a Port" task on page 17-67.

Step 8 Return to your originating procedure (NTP).

DLP-C112 Edit a Circuit Name

Purpose	This task edits a circuit name, including VCAT circuit member names.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node or network view, click the **Circuits** tab.

Step 2 Click the circuit you want to rename, then click **Edit**.

Step 3 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 4.

a. Click the **Members** tab.

b. Click the VCAT member that you want to edit, then click **Edit Member**. The Edit Member window opens.

Step 4 In the General tab, click the **Name** field and edit or rename the circuit. Names can be up to 48 alphanumeric and/or special characters.

Note If you will create a monitor circuit on this circuit, do not make the name longer than 44 characters because monitor circuits add "_MON" (four characters) to the circuit name.

Step 5 Click **Apply**.

Step 6 From the File menu, choose **Close**.

Step 7 If you changed the name of a VCAT circuit member, repeat Step 6 for the Edit Circuit window.

Step 8 In the Circuits window, verify that the circuit was correctly renamed.

Step 9 Return to your originating procedure (NTP).

DLP-C113 Change Active and Standby Span Color

Purpose	This task changes the color of active (working) and standby (protect) circuit spans 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-C29 Log into CTC, page 17-44
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 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, continue with Step 4.
- To change the color of the standby (protect) span, continue with Step 5.
- To return active and standby spans to their default colors, continue with Step 6.

Step 4 As needed, change the color of the active span:

a. In the Span Colors area, click the colored square next to 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, continue with 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 next to 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 Return the active and standby spans to their default colors:

a. From the Edit menu, choose **Preferences**.

b. In the Preferences dialog box, click the **Circuits** tab.

c. Click the **Reset to Defaults** button.

d. 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-C114 Edit Path Protection Circuit Path Selectors

Purpose	This task changes the path protection signal fail and signal degrade thresholds, the reversion and reversion time, and the PDI-P settings for one or more path protection circuits.
Tools/Equipment	None
Prerequisite Procedures	NTP-C31 Provision Path Protection Nodes, page 5-10 DLP-C29 Log into CTC, page 17-44
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 path protection circuits 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 you want to change.

Step 4 From the Tools menu, choose **Circuits > Set Path Selector Attributes**.

Note Alternatively, for single circuits you can click the **Edit** button, then click the **Path Protection Selectors** tab on the Edit Circuits window.

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 this 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 VT Circuits Only area, set the following thresholds:
  - SF Ber Level—Sets the path protection signal failure BER threshold.
  - SD Ber Level—Sets the path protection signal degrade BER threshold.
- In the STS Circuits Only area, set the following thresholds:
  - SF Ber Level—Sets the path protection signal failure BER threshold.

- SD Ber Level—Sets the path protection signal degrade BER threshold.
- Switch on PDI-P—When checked, traffic switches if an STS payload defect indication is received.

Step 6 Click **OK** and verify that the changed values are correct.

Step 7 Return to your originating procedure (NTP).

DLP-C115 Delete Circuits

Purpose	This task deletes circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 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 "NTP-C102 Back Up the Database" procedure on page 15-2 to preserve the existing database and circuits.

Step 2 Verify that traffic is no longer carried on the circuit and that the circuit can be safely deleted.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-C88 Disable Alarm Filtering" task on page 17-109 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms are present, investigate and resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

Step 4 From the View menu, choose **Go to Network View**.

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:

- **Set drop ports to OOS**—Puts the circuit source and destination ports to OOS-MA,DSBLD if the circuit is the same size as the port or is the only circuit using the port. 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.
- **Notify when completed**—If checked, the CTC Alerts confirmation dialog box indicates when all circuit source/destination ports are in OOS-MA,DSBLD and the circuit is deleted. During this time, you cannot perform other CTC functions. If you are deleting many circuits, waiting for confirmation can take a few minutes. 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 checkbox. For more information, see the "DLP-C36 Configure the CTC Alerts Dialog for Automatic Popup" task on page 17-51. If the CTC Alerts dialog 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 next step.

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-C102 Back Up the Database" procedure on page 15-2.

Step 12 Return to your originating procedure (NTP).

DLP-C116 Add a Member to a VCAT Circuit

Purpose	This task adds a member to non-LCAS and LCAS circuits on CE-100T-8 or ML-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 fiber) specified during the VCAT circuit creation procedure.
Tools/Equipment	CE-100T-8 or ML-100T-8 card
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 VCAT 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

Caution Adding a member to non-LCAS VCAT circuits can be service affecting.

Caution Adding a member to 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 use a Cisco ONS 15454 ML-Series card as a source or destination.

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 an 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.

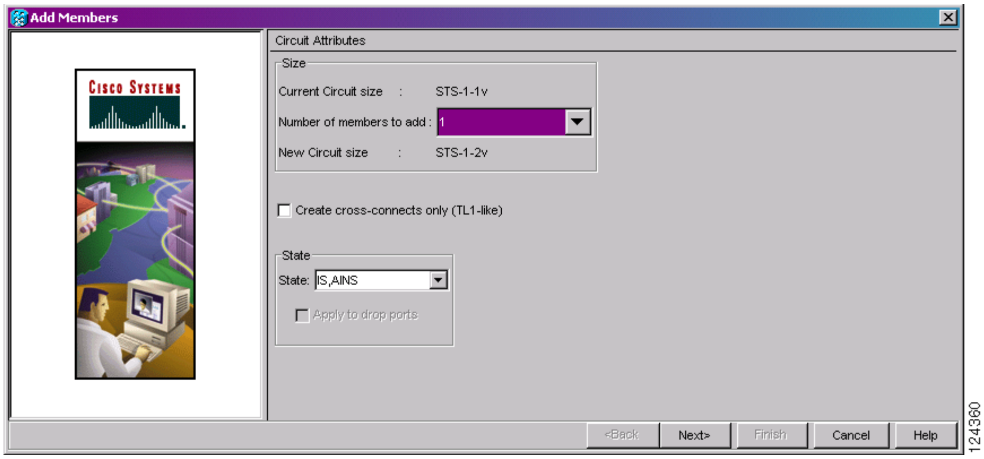
Step 5 Click **Add Member**. The Add Member button is enabled if the VCAT circuit has sufficient bandwidth for an added member.

Step 6 Define the number of members and member attributes (Figure 18-6):

- 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 15310-CL and Cisco ONS 15310-MA 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 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 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. IS,AINS is the default state.
- OOS,MT—Puts the member 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. See the "DLP-C180 Change a VCAT Member Service State" task on page 18-73.
- OOS,OOG—(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.

Figure 18-6 Adding a VCAT Member



Add Members

Circuit Attributes

Size

Current Circuit size : STS-1-1v

Number of members to add : 1

New Circuit size : STS-1-2v

□ Create cross-connects only (TL1-like)

State

State: IS,AINS

□ Apply to drop ports

Step 7 Click **Next**.

Step 8 To route the members 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 from the drop-down list to identify the member.
- Name—Enter 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—(Future use) Routes the member on a BLSR protection channel.

Note Although ONS 15310-CLs do not support BLSR, you can route an LCAT VCAT circuit over a BLSR network of ONS 15600s, ONS 15454s, or ONS 15327s.

  - 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—(Future use) Routes the member on a BLSR protection channel.

Note Although ONS 15310-CL and ONS 15310-MAs do not support BLSR, you can route an LCAT VCAT circuit over a BLSR network of ONS 15600, ONS 15454, or ONS 15327 nodes.

  - 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 or unprotected portions of the member route from the source to the destination.
- Add one span for all 1+1 portions of the route from the source to the destination.
- For members routed on path protection dual ring interconnect topologies, provision the working and protect paths.

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 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* for the procedure to clear the alarm. If it does not, continue with b.

b. Complete the "DLP-C180 Change a VCAT Member Service State" task on page 18-73 to put the member in the IS service state.

Step 15 Return to your originating procedure (NTP).

DLP-C117 Delete a Member from a VCAT Circuit

Purpose	This task removes a member from a non-LCAS or LCAS VCAT circuit on CE-100T-8 or ML-100T-8 cards. This task reduces the size of the VCAT circuit. You cannot delete members from VCAT circuits that use ONS 15454 ML-Series cards as a circuit source or destination.
Tools/Equipment	CE-100T-8 or ML-100T-8 card
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 VCAT circuits must exist on the network. See Chapter 6, "Create Circuits and VT Tunnels" for circuit creation procedures. As necessary, complete the "DLP-C180 Change a VCAT Member Service State" task on page 18-73 to change a LCAS member state to OOS-MA,OOG.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Deleting a member from a non-LCAS circuit can be service-affecting.

Caution Deleting LCAS members in the IS-NR or OOS-AU,AINS service state can be service affecting. Cisco recommends putting the LCAS 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.

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**.

You cannot delete members from VCAT circuits that use ONS 15454 ML-Series cards as a circuit source or destination.

Step 6 In the confirmation dialog box, click **Yes**.

Step 7 Return to your originating procedure (NTP).

DLP-C118 Change Tunnel Type

Purpose	This task converts a traditional DCC tunnel to an IP-encapsulated tunnel or an IP-encapsulated tunnel to a traditional DCC tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-C67 Create a DCC Tunnel, page 17-84 or DLP-C69 Create an IP-Encapsulated Tunnel, page 17-86 DLP-C29 Log into CTC, page 17-44
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%).
- 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-C119 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. DLP-C29 Log into CTC, page 17-44
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.
- 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-C120 Delete Overhead Circuits

Purpose	This task deletes overhead circuits. Overhead circuits include DCC tunnels, IP-encapsulated tunnels, and user data channels.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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-C50 Change the Service State for a Port" task on page 17-67.

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: 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-C121 Provision Path Trace on Circuit Source and Destination Ports

Purpose	This task creates a path trace on STS circuit source ports and destination ports.
Tools/Equipment	Cards capable of transmitting and receiving path trace must be installed at the circuit source and destination. See Table 18-6 on page 18-29 for a list of cards.
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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.

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. Table 18-6 shows the ONS 15310-CL and ONS 15310-MA cards and/or ports that support J1 and/or J2 path trace.

Table 18-6 ONS 15310-CL and ONS 15310-MA Cards/Ports Capable of J1/J2 Path Trace

Trace Function	J1 or J2	Cards/Ports
Transmit and receive	J1	ONS 15310-CL DS-1 and DS-3 ports
		ML-100T-8
	J1 and J2	CE-100T-8
	J2	ONS 15310-MA OC-N and DS1 ports
Receive	J1	ONS 15310-CL EC-1, OC-3, and OC-12 ports ONS 15310-MA OC-N, EC-1, DS1, and DS3 ports

Step 3 If neither port is transmit/receive, you will not be able to complete this task. If one port is transmit/receive and the other is a receive-only port, 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 double-click it (or 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. In 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.

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. In 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 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 the baseline. An alarm is raised when a string that differs from the baseline is received.
- Manual—The string entered in the Current Expected String 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 the Path Trace Mode field to Auto, skip this step.

c. Check the **Disable AIS and RDI if TIM-P is detected** check box if you want to suppress the alarm indication signal (AIS) and RDI when the STS Path Trace Identifier Mismatch Path (TIM-P) alarm appears. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* for descriptions of alarms and conditions.

d. (Check box visibility depends on card selection.) Check the **Disable AIS on C2 Mis-Match** check box if you want to suppress the Alarm Indication Signal when a C2 mis-match occurs.

e. Click **Apply**, then click **Close**.

Note It is not necessary to set the format (16 bytes for VT circuits or 64 bytes for STS circuits) 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 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 Path Trace Mode 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 the **Disable AIS and RDI if TIM-P is detected** check box if you want to suppress the alarm indication signal (AIS) and RDI when the STS Path Trace Identifier Mismatch Path (TIM-P) alarm appears. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* for descriptions of alarms and conditions.

e. (Check box visibility depends on card selection.) Check the **Disable AIS on C2 Mis-Match** check box if you want to suppress the Alarm Indication Signal when a C2 mis-match occurs.

f. Click **Apply**.

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 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 **Reset** 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**.

When you display the detailed circuit window, path trace is indicated by 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-C122 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 18-6 on page 18-29.
Prerequisite Procedures	DLP-C121 Provision Path Trace on Circuit Source and Destination Ports, page 18-29 DLP-C29 Log into CTC, page 17-44
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 In node view, 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, check 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.

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 end as the baseline string. An alarm is raised when a string that differs from the baseline is received. For OC-N ports, Auto is recommended, since Manual mode requires you to trace the circuit on 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 window to determine whether the port is in the circuit source or destination path, then set the New Expected String field 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-C123 Change the Node Name, Date, Time, and Contact Information

Purpose	This task changes basic information such as node name, date, time, and contact information.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 > 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 Saving Time

See the "NTP-C20 Set Up Name, Date, Time, and Contact Information" procedure on page 4-4 for detailed field descriptions.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-C124 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-C29 Log into CTC, page 17-44
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:

- <b> Begins boldface font
- </b> Ends boldface font
- <center> Aligns type in the center of the window
- </center> Ends the center alignment
- <font=n, where n = point size> Changes the font to the new size
- </font> Ends the font size command
- <p> Creates a line break
- <sub> Begins subscript
- </sub> Ends subscript
- <sup> Begins superscript
- </sup> Ends superscript
- <u> Begins underline
- </u> Ends underline

Step 3 If you want to preview your changed statement and format, click the **Preview** subtab.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-C125 Change IP Settings

Purpose	This task explains how to change the IP address, subnet mask, default router, dynamic host configuration protocol (DHCP) access, firewall access, and SOCKS proxy server settings for the ONS 15310-CL and Cisco ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C39 Provision IP Settings, page 17-53
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note If you assign one ONS 15310 node an IP address that is in use on another node, both nodes might retain the duplicated IP addresses even after you attempt to change them. Duplicated IP addresses raises the DUP-IPADDR alarm. Refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* to troubleshoot the DUP-IPADDR alarm.

Step 1 In node view, click the **Provisioning** > **Network** > **General** tabs.

Step 2 Change any of the following:

- IP Address
- Suppress CTC IP Display
- Default Router
- Forward DHCP Request To
- Net/Subnet Mask Length
- CTX CORBA (IIOP) Listener Port
- Gateway Settings

See the "DLP-C39 Provision IP Settings" task on page 17-53 for detailed field descriptions.

Step 3 Click **Apply**.

If you changed any of the network fields that will cause the node to reboot, the Change Network Configuration confirmation dialog box appears. If you changed a gateway setting, a confirmation appropriate to the gateway field appears. If you only changed the IP address fields, no confirmation dialog box appears.

Step 4 If a confirmation dialog box appears, click **Yes**.

If you changed the IP address, subnet mask length, or CTX CORBA (IIOP) listener port, the 15310-CL-CTX card (in the ONS 15310-CL) or CTX2500 card (in the ONS 15310-MA) will reboot.

Step 5 Return to your originating procedure (NTP).

DLP-C126 Modify a Static Route

Purpose	This task modifies a static route on an ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C40 Create a Static Route, page 17-55
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 that you want to edit.

Step 3 Click **Edit**.

Step 4 In the Edit Selected Static Route dialog box, enter the following:

- Mask
- Next Hop
- Cost

See the "DLP-C40 Create a Static Route" task on page 17-55 for detailed field descriptions.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-C127 Delete a Static Route

Purpose	This task deletes a static route on an ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C40 Create a Static Route, page 17-55
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-C128 Disable Open Shortest Path First Protocol

Purpose	This task disables the Open Shortest Path First (OSPF) routing protocol for an ONS 15310-CL or ONS 15310-MA local area network (LAN).
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C41 Set Up or Change Open Shortest Path First Protocol, page 17-56
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**.

Note Disabling OSPF can cause an 15310-CL-CTX or CTX2500 reboot, which causes a temporary loss of connectivity to the node but does not affect traffic.

Step 4 Return to your originating procedure (NTP).

DLP-C129 Delete a Proxy Tunnel

Purpose	This task removes a proxy tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 Continue with your originating procedure (NTP).

DLP-C130 Delete a Firewall Tunnel

Purpose	This task removes a firewall tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, 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-C131 Change the Network View Background Color

Purpose	This task changes the network view background color and the domain view background color (the area shown when you open a domain).
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
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 local computer. The change does not affect other CTC users on different computers.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Right-click the network view or domain map area and choose **Set Background Color** from the shortcut menu.

Step 3 In the Choose Color dialog box, click a background color.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-C132 Change to the Default Network View Background Map

Purpose	This task changes the background map to the default map of the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
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 local computer. The change does not affect other CTC users on different computers.

Step 1 From the View menu, choose **Go to Network View**.

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

Step 3 Under Defaults Selector, choose **CTC** and then **Network**.

Step 4 Click the **Default Value** field and choose a default map from the drop-down list. The 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 15310-CL or ONS 15310-MA icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until all the node 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 15310-CL or ONS 15310-MA icons appear at the magnification you want.

Step 10 Return to your originating procedure (NTP).

DLP-C133 Apply a Custom Network View Background Map

Purpose	This task changes the background image or map on the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
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 local computer. The change does not affect other CTC users on different computers.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Right-click the network or domain map and choose **Set Background Image**.

Step 3 Navigate to the graphic file you want to use as a background.

Step 4 Select the file and click **Open**. The graphic file appears as the CTC background image.

Step 5 As needed, complete the following to view and move the node icons:

- If the node icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until all of the node icons are visible.
- If you want to reposition the node icons, drag and drop them one at a time to a new location on the map.
- It you want to change the magnification of the icons, right-click the network view and choose **Zoom In** or **Zoom Out**. Repeat until the node icons appear at the magnification you want.

Step 6 Return to your originating procedure (NTP).

DLP-C134 Create Domain Icons

Purpose	This task creates a domain icon to group ONS 15310-CL or ONS 15310-MA icons in CTC network view. By default, domains are visible on all CTC sessions that log into the network.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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-C137 Edit Network Element Defaults" procedure on page 15-18 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-C135 Manage Domain Icons

Purpose	This task manages CTC network view domain icons. By default, domains are visible on all CTC sessions that log into the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C134 Create Domain Icons, page 18-40
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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-C137 Edit Network Element Defaults" procedure on page 15-18 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 18-7 and complete the appropriate steps.

Table 18-7 Managing Domains

Domain action	Steps
Move a domain	Drag and drop the node 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.

Table 18-7 Managing Domains (continued)

Domain action	Steps
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 choose **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-C136 Enable Dialog Box Do-Not-Display Option

Purpose	This task enables or disables the "Do not display" dialog box preference for subsequent sessions.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
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 on a dialog box, the dialog box does not appear for any other users who perform that operation on the network unless the command is overridden using the following task.

Step 1 From the Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **General** tab.

The Preferences Management area lists all dialog boxes where "Do not show this dialog again" was checked.

Step 3 Choose one of the following:

- **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-C137 Modify a 1+1 Protection Group

Purpose	This task modifies a 1+1 protection group for any optical port.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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, double click the 1+1 protection group you want to modify or click **Edit**.

Step 3 In the Edit Protection Group dialog box, 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 check 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 menu. Uncheck if you do not want traffic to revert.
- Reversion Time—If the Revertive check box is checked, 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 "NTP-C141 Create Optical Protection Groups for the ONS 15310-CL" procedure on page 4-12 or "NTP-C142 Create Protection Groups for the ONS 15310-MA" procedure on page 4-13 for field descriptions.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-C138 Delete a Protection Group

Purpose	This task deletes a protection group.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note 1:1 electrical protection groups are created automatically in the ONS 15310-MA and can only be deleted after the protect card of a 1:1 protection group is deleted.

Step 1 In node view, click the **Provisioning** > **Protection** tabs.

Step 2 In the Protection Groups list, click the protection group you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Yes** in the Delete Protection Group dialog box to confirm deletion.

Step 5 Return to your originating procedure (NTP).

DLP-C139 Change the Node Timing Source

Purpose	This task changes the SONET timing source for the ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution The following task can be service affecting; perform it during a scheduled maintenance window.

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 In the General Timing area, 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
- Reversion Time

See the "DLP-C45 Set Up External or Line Timing" task on page 17-61 for field descriptions.

Step 3 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 Mechanical Interface Cards (MICs). If you attach equipment to the 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

Step 4 In the BITS Facilities area, you can change the following information:

Note The BITS Facilities section sets the parameters for your BITS1 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.

- In/Out State
- Coding
- Framing
- Sync Messaging
- AIS Threshold
- Admin SSM
- LBO

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

DLP-C140 Verify Timing in a Reduced Ring

Purpose	Use this task to verify timing in the ring where you removed a node.
Tools/Equipment	None
Prerequisite Procedures	NTP-C98 Remove a Path Protection Node, page 14-4
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 Identify the type of timing (Line, External, Mixed) in the Timing Mode field.

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. Look for another node on the ring that can be used as a BITS source and set the Timing Mode for that node to **External**. Choose that node as the primary timing source for all other nodes in the ring. See the "DLP-C139 Change the Node Timing Source" task on page 18-44.

b. If no node in the reduced ring can be used as a BITS source, choose one node to be your internal timing source. Set the Timing Mode for that node to **External**, set the BITS 1 and 2 State field to **OOS**, and set the NE Reference to **Internal Clock**. Then, choose line timing for all other nodes in the ring. This forces the first node to be the primary timing source. See the "DLP-C139 Change the Node Timing Source" task on page 18-44.

Note Internal 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-C23 Set Up Timing" procedure on page 4-11.

Step 6 Return to your originating procedure (NTP).

DLP-C141 Change the 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-C29 Log into CTC, page 17-44
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 Before Lockout—Displays 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 unlock a user manually 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). If you checked Manual Unlock by Superuser, Lockout Duration is disabled.

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 he or she can reuse a password.
- New Password must Differ from the Old Password—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 his or her password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, SUPERUSER. The range is 20 to 95 days.
- Warning—Sets the number 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.
- 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 45 to 90 days.

Step 7 Click **Apply**.

Step 8 Return to your originating procedure (NTP).

DLP-C142 Change the 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-C29 Log into CTC, page 17-44
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 Before Lockout—Displays 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). If you checked Manual Unlock by Superuser, Lockout Duration is disabled.

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 he or she can reuse a password.

- New Password must Differ from the Old Password—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 his or her password the first time they log into the 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, PROVISIONER, SUPERUSER. The range is 20 to 95 days.
- Warning—Sets the number days the user will be warned to change his or her 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.
- 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 45 to 90 days.

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-C143 Change Node Access and PM Clearing Privilege

Purpose	This task provisions the physical access points and shell programs used to connect to the ONS 15310-CL or ONS 15310-MA and sets the user security level that can clear node performance monitoring data.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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.
  - **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.

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. Non-Secure mode allows access to the shell using telnet.
- 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 shell 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 allows telnet access through ports 2361, 3082 and 3083; Secure allows SSH access through port 4083.

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 (allows access using IIOP and HTTP), and Secure (allows access using SSLIOP and HTTPS).

In the TCC CORBA (IIOP/SSLIOP) Listener Port area, choose a listener port option:

- **Default - TCC Fixed**—Uses Port 57790 (non-secure IIOP port) and Port 57791 (secure SSLIOP port) 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 or Port 57791 is open. 57790 is the non-secure IIOP port, 57791 is the secure SSLIOP port.
- **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-C144 Change User Password and Security Settings on a Single Node

Purpose	This task changes settings for an existing user at one node.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C37 Create a New User on a Single Node, page 17-51
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.

Step 3 Click **Change**.

Step 4 In the Change User dialog box, you can:

- Change a user password
- Modify the user security level
- Lock out or disable the user

See the "DLP-C37 Create a New User on a Single Node" task on page 17-51 for field descriptions.

Step 5 Click **OK**.

Note User settings that you changed during this task will not appear until that user logs off and logs back in.

Step 6 Return to your originating procedure (NTP).

DLP-C145 Change User Password and Security Settings on Multiple Nodes

Purpose	This task changes settings for an existing user on multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C38 Create a New User on Multiple Nodes, page 17-52
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. Click 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 password
- Modify the user security level
- Lock out or disable the user

See the "DLP-C38 Create a New User on Multiple Nodes" task on page 17-52 for field descriptions.

Step 5 Click **OK**. A Change Results confirmation dialog box appears.

Step 6 Click **OK** to acknowledge the changes.

Step 7 Return to your originating procedure (NTP).

DLP-C146 Delete a User on a Single Node

Purpose	This task deletes an existing user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note CTC will allow you to delete other Superuser IDs if one Superuser ID remains. For example, you can delete the CISCO15 user if you have created another Superuser ID. Use this option with caution.

Note Users who are logged in when you delete them will not be logged out. The delete user action will take effect after the user logs out. To log out a user who is currently logged in, complete the "DLP-C148 Log Out a User on a Single Node" task on page 18-52.

Step 1 In node view, click the **Provisioning** > **Security > Users** tabs.

Step 2 Choose the user you want to delete.

Step 3 In the Delete User dialog box, complete the following:

a. To log the user out before the deleting the user, check **Logout before delete**.

b. Click **OK**.

Step 4 In the User Deletion Results dialog box, click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-C147 Delete a User on Multiple Nodes

Purpose	This task deletes an existing user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note CTC will allow you to delete other Superuser IDs if one Superuser ID remains. For example, you can delete the CISCO15 user if you have created another Superuser ID. Use this option with caution.

Note Users who are logged in when you delete them will not be logged out. The delete user action will take effect after the user logs out. To log out a user who is currently logged in, complete the "DLP-C149 Log Out a User on Multiple Nodes" task on page 18-53.

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning** > **Security > Users** tabs. Click the name of the user you want to delete.

Step 3 Click **Delete**.

Step 4 In the Delete User dialog box, complete the following:

a. To log the user out before the deleting the user, check **Logout before delete**.

b. Click **OK**.

Step 5 In the User Deletion Results dialog box, click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-C148 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-C29 Log into CTC, page 17-44
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 you want to log out and click **Logout**.

Step 3 In the Logout User dialog box, check **Lockout before Logout** if you want to prevent the user from logging in after logout. User lockout parameters provisioned in the Policy tab determine when the user can log back in. A user is locked out for the amount of time specified in the Lockout Duration field unless a Superurser manually unlocks the lockout. See the "DLP-C141 Change the Security Policy on a Single Node" task on page 18-46 for more information.

Step 4 Click **OK**.

Step 5 Click **Yes** to confirm the logout.

Step 6 Return to your originating procedure (NTP).

DLP-C149 Log Out a User on Multiple Nodes

Purpose	This task logs out a user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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** > **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 prevent the user from logging in after logout. User lockout parameters provisioned in the Policy tab determine when the user can log back in. A user is locked out for the amount of time specified in the Lockout Duration field unless a Superurser manually unlocks the lockout. See the "DLP-C141 Change the Security Policy on a Single Node" task on page 18-46 for more information.

Step 7 Click **OK**.

Step 8 Click **Yes** to confirm the logout.

Step 9 Return to your originating procedure (NTP).

DLP-C150 Modify SNMP Trap Destination

Purpose	This task modifies the SNMP trap destinations on an ONS 15310-CL or ONS 15310-MA including community name, default UDP port, and SNMP trap version.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 Click the trap that you want to modify in the Trap Destinations dialog box.

For a description of SNMP traps, refer to the "SNMP" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 3 In the Selected Destination area, you can modify the following:

- Community
- UDP port
- Trap version (SNMPv1 or SNMPv2)

Note The community name is a form of authentication and access control. The community name assigned to the ONS 15310-CL or ONS 15310-MA is case-sensitive and must match the community name of the NMS.

Note The default UDP port for SNMP is 162.

Note Refer to your NMS documentation to determine which trap version to use.

Step 4 If you want to allow the ONS 15310-CL or ONS 15310-MA SNMP agent to accept SNMP SET requests on certain MIBs, check the **Allow SNMP Sets** check box. If the box is not checked, SET requests are rejected.

Step 5 If you want to set up the SNMP proxy feature to allow network management, message reporting, and performance statistic retrieval across firewalls, check the **Allow SNMP Proxy** check box.

Step 6 Click **Apply**. SNMP settings are now configured.

Step 7 To view SNMP information for each node, click the node IP address in the Trap Destinations area of the Trap Destinations screen.

Step 8 Return to your originating procedure (NTP).

DLP-C151 Delete SNMP Trap Destinations

Purpose	This task deletes SNMP trap destinations on an ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 list, 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-C152 Change a Section DCC Termination

Purpose	This task modifies a SONET data communications channel (SDCC). You can also enable or disable OSPF and enable or disable the foreign node setting.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	Provisioning or higher

Step 1 In node view, 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, Open Shortest Path First 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-C153 Change a Line DCC Termination

Purpose	This task modifies a line data communications channel (LDCC). You can also enable or disable OSPF and enable or disable the foreign node setting.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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, Open Shortest Path First 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-C154 Delete a Section DCC Termination

Purpose	This task deletes a SONET Section DCC termination on the ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Comm Channels > SDCC** tabs.

Step 2 Click the SDCC termination that you want to delete 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-C155 Delete a Line DCC Termination

Purpose	This task deletes a SONET Line DCC termination on the ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 In node view, click the **Provisioning > Comm Channels > LDCC** tabs.

Step 2 Click the LDCC termination that you want to delete and click **Delete**. The Delete LDCC Termination dialog box appears.

Step 3 Click **Yes** in the confirmation dialog box.

Step 4 Return to your originating procedure (NTP).

DLP-C156 Delete a Provisionable Patchcord

Purpose	This task deletes a provisionable patchcord.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 > PPCs** tabs. If you are in network view, click **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-C163 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-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	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 graphically displayed on the span with 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. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, AIS-P, SF, and SD. Make sure the Filter button is not selected.

If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 9, “Manage Alarms,” or, if necessary, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

Step 5 Return to your originating procedure (NTP).

DLP-C164 Manually Route a Path Protection Circuit in 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-C29 Log into CTC, page 17-44 NTP-C96 Convert an Unprotected Point-to-Point or Linear ADM to a Path Protection Configuration Automatically, page 13-6
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 Uprotected 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-C165 Automatically Route a Path Protection Circuit in 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-C29 Log into CTC, page 17-44 NTP-C96 Convert an Unprotected Point-to-Point or Linear ADM to a Path Protection Configuration Automatically, page 13-6
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, check **Route Automatically.**

Check **Review Route Before Creation** if you want to review and edit the circuit route before the circuit is created.

Step 2 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 3 If you selected Review Route Before Creation, complete the following substeps. If not, continue with Step 4.

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 4 Click **Finish**.

Step 5 Return to your originating procedure (NTP).

DLP-C166 Initiate a Path Protection Force Switch on a Span

Purpose	This task switches all circuits on a path protection span to another span.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Traffic is not protected during Force path protection switches.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Right-click the span where you want to Force switch path protection traffic. Choose **Circuits** from the shortcut menu.

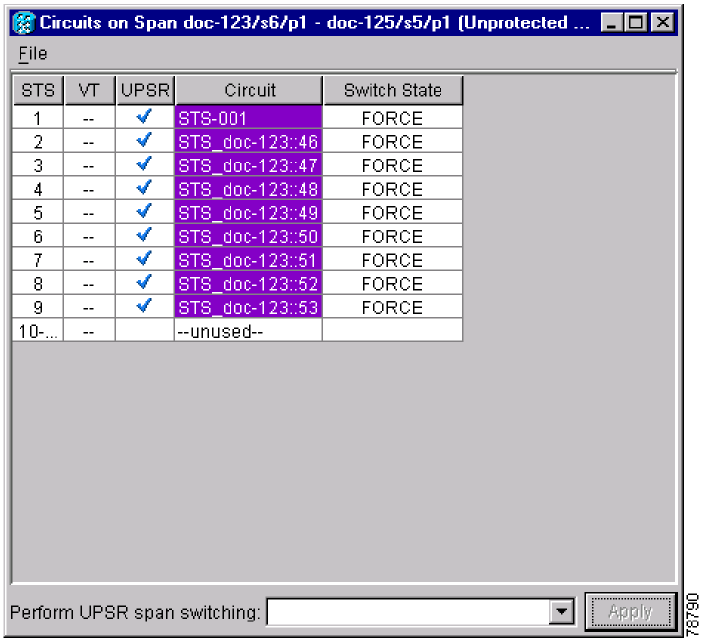
Step 3 In the Circuits on Span dialog box, choose **FORCE SWITCH AWAY**. Click **Apply**.

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 18-7 shows an example.

Figure 18-7 Circuits on Span Dialog Box with a Force Switch



Circuits on Span doc-123/s6/p1 - doc-125/s5/p1 (Unprotected ...

STS	VT	UPSR	Circuit	Switch State
1	--	✓	STS-001	FORCE
2	--	✓	STS_doc-123::46	FORCE
3	--	✓	STS_doc-123::47	FORCE
4	--	✓	STS_doc-123::48	FORCE
5	--	✓	STS_doc-123::49	FORCE
6	--	✓	STS_doc-123::50	FORCE
7	--	✓	STS_doc-123::51	FORCE
8	--	✓	STS_doc-123::52	FORCE
9	--	✓	STS_doc-123::53	FORCE
10-...	--		--unused--	

Perform UPSR span switching:

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; it is informational only.

Step 6 Return to your originating procedure (NTP).

DLP-C167 Clear a Path Protection Force Switch

Purpose	This task clears a path protection Force switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 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 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).

DLP-C168 Verify Pass-Through Circuits

Purpose	This task verifies that circuits passing through a node that will be removed enter and exit the node on the same STS and/or VT.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 target node 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 a circuit mapping on the west port s5/p1-1/S1 (Slot 5, Port 1-1, STS 1), verify that the mapping is STS 1 on the east port. If the circuit appears different STSs and/or VTs on the east and west ports, write down the name of the circuit.

Step 4 Repeat Steps 1 through 3 for each circuit displayed in the Circuits tab.

Delete and recreate each circuit recorded in Step 3 that entered/exited the node on different STSs. To delete the circuit, complete the "DLP-C115 Delete Circuits" task on page 18-21. To create circuits, complete the appropriate procedures in Chapter 6, "Create Circuits and VT Tunnels."

Step 5 Return to your originating procedure (NTP).

DLP-C169 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)

Purpose	This task reinitializes the ONS 15310-CL or the ONS 15310-MA using the CTC reinitialization tool on a Windows computer. Reinitialization uploads a new software package to the 15310-CL-CTX (on the ONS 15310-CL) or CTX2500 (ONS 15310-MA) card, clears the node database, and restores the factory default parameters.
Tools/Equipment	ONS 15310-CL System Software CD, Version 8.5.x ONS 15310-MA System Software CD, Version 8.5.x Java Runtime Environment (JRE) 5.0 must be installed on the computer to log into the node at the completion of the reinitialization. The reinitializtion tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 5.0.
Prerequisite Procedures	NTP-C102 Back Up the Database, page 15-2 NTP-C13 Set Up Computer for CTC, page 3-2 One of the following: • NTP-C14 Set Up CTC Computer for Local Craft Connection to the Node, page 3-3 • NTP-C15 Set Up a CTC Computer for a Corporate LAN Connection to the Node, page 3-5
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.

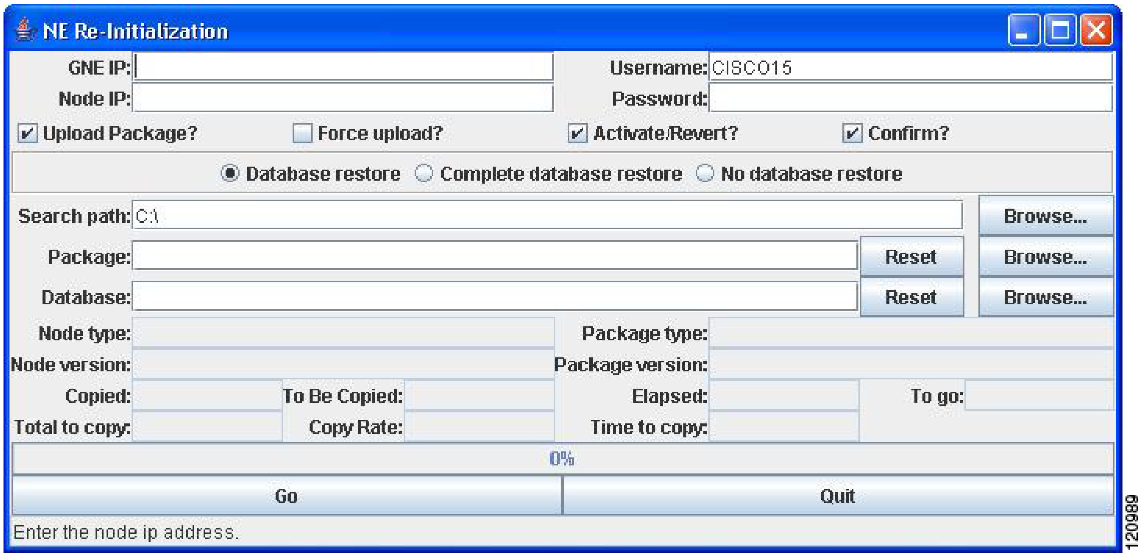
Step 1 Insert the ONS 15310-CL System Software CD, Version 8.5.x into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.

Step 2 From the Windows Start menu, choose **Run.** In the Run dialog box, click **Browse** and navigate to the CISCO15310 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 18-8).

Figure 18-8 Reinitialization Tool in Windows



NE Re-Initialization

GNE IP:

Username: CISCO15

Node IP:

Password:

☑ Upload Package? □ Force upload? ☑ Activate/Revert? ☑ Confirm?

● Database restore ○ Complete database restore ○ No database restore

Search path: C:\

Package:

Database:

Node type:

Package type:

Node version:

Package version:

Copied:

To Be Copied:

Elapsed:

To go:

Total to copy:

Copy Rate:

Time to copy:

0%

Enter the node ip address.

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 tab.
- 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 CISCO15310 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 15310-CL-CTX card, “Complete” appears in the status bar and the 15310-CL-CTX (CL) or CTX2500 (MA) card will reboot. Wait a few minutes for the reboot to complete.

Step 8 After the reboot is complete, log into the node using “DLP-C29 Log into CTC” task on page 17-44.

Step 9 Manually set the node name and network configuration to site-specific values. See the “NTP-C20 Set Up Name, Date, Time, and Contact Information” procedure on page 4-4 and the “NTP-C20 Set Up Name, Date, Time, and Contact Information” procedure on page 4-4 for information on setting the node name, IP address, subnet mask and gateway, and IIOP port.

Step 10 Return to your originating procedure (NTP).

DLP-C170 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)

Purpose	This task reinitializes the ONS 15310-CL or ONS 15310-MA using the CTC reinitialization tool on a UNIX computer. Reinitialization uploads a new software package to the 15310-CL-CTX or CTX2500 card, clears the node database, and restores the factory default parameters.
Tools/Equipment	ONS 15310-CL System Software CD, Version 8.5.x or ONS 15310-MA System Software CD, Version 8.5.x JRE 5.0 must be installed on the computer to log into the node at the completion of the reinitialization. The reinitializtion tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 5.0.
Prerequisite Procedures	NTP-C102 Back Up the Database, page 15-2 NTP-C13 Set Up Computer for CTC, page 3-2 One of the following: • NTP-C14 Set Up CTC Computer for Local Craft Connection to the Node, page 3-3 • NTP-C15 Set Up a CTC Computer for a Corporate LAN Connection to the Node, page 3-5
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 To find the recovery tool file, go to the CISCO15310 directory on the CD (usually /cdrom/cdrom0/CISCO15310).

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 18-8 on page 18-64).

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 tab.
- 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 CISCO15310 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 15310-CL-CTX or CTX2500 card, “Complete” appears in the status bar and the 15310-CL-CTX or CTX2500 card will reboot. Wait a few minutes for the reboot to complete.

Step 7 After the reboot is complete, log into the node using DLP-C29 Log into CTC, page 17-44.

Step 8 Manually set the node name and network configuration to site-specific values. See the "NTP-C20 Set Up Name, Date, Time, and Contact Information" procedure on page 4-4 and "NTP-C20 Set Up Name, Date, Time, and Contact Information" procedure on page 4-4 for information on setting the node name, IP address, subnet mask and gateway, and IIOP port.

Step 9 Return to your originating procedure (NTP).

DLP-C171 Apply a Lock-on

Purpose	This task prevents traffic from being switched from one port to another.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Note For a 1+1 optical protection group, only the working port can be placed in the lock on state.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group where you want to apply a lock on.

Step 3 If you determine that the protect port is in standby mode and you want to apply the lock on to the protect port, make the protect port active:

a. In the Selected Group list, click the protect port.

b. In the Switch Commands area, click **Force**.

Step 4 In the Selected Group list, click the active port where you want to lock traffic.

Step 5 In the Inhibit Switching area, click **Lock On**.

Step 6 Click **Yes** in the confirmation dialog box.

The lock-on has been applied and traffic cannot be switched to the working port. To clear the lock on, see the "DLP-C173 Clear a Lock-on or Lockout" task on page 18-68.

Step 7 Return to your originating procedure (NTP).

DLP-C172 Apply a Lockout

Purpose	This task switches traffic from one port to another using a lockout, which is a switching mechanism that overrides other manual switching connections (Force or Manual).
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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.

Note For a 1+1 optical protection group, only the protect port can be locked out.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group that contains the port you want to lock out.

Step 3 In the Selected Group list, click the port where you want to lock out traffic.

Step 4 In the Inhibit Switching area, click **Lock Out**.

Step 5 Click **Yes** in the confirmation dialog box.

The Lock Out has been applied and traffic is switched to the opposite port. To clear the lockout, see the "DLP-C173 Clear a Lock-on or Lockout" task on page 18-68.

Note Provisioning a lockout raises a LOCKOUT-REQ or an FE-LOCKOUTOFPR condition in CTC. Clearing the lockout switch request clears these conditions.

Step 6 Return to your originating procedure (NTP).

DLP-C173 Clear a Lock-on or Lockout

Purpose	This task clears a lock on or lockout.
Tools/Equipment	None
Prerequisite Procedures	DLP-C171 Apply a Lock-on, page 18-67 or DLP-C172 Apply a Lockout, page 18-68
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 list, click the protection group that contains the port you want to clear.

Step 3 In the Selected Group list, click the port 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-C174 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	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam or view directly with optical instruments.** Statement 1051

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-C175 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	As needed
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 through 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-C176 Clean the Fiber Adapters

Purpose	This task cleans the fiber adapters.
Tools/Equipment	CLETOP stick swab
Prerequisite Procedures	None
Required/As Needed	As needed
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-C177 Manual or Force Switch the Node Timing Reference

Purpose	This task commands the node to switch to the timing reference that you have selected if the synchronization status message (SSM) quality of the reference is not less than the quality of the reference that the node is currently running.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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. The Timing Source window appears.

Step 2 Click the Reference drop-down list for the desired Clock, and choose the desired reference.

Step 3 Click the Operation drop-down list for the desired Clock, and choose one of the following options:

- **Manual**—This operation commands the NE to switch to the reference you have selected, if the SSM quality of the reference is not less than the quality of the reference that the node is currently running.
- **Force**—This operation commands the NE to switch to the reference you have selected, regardless of the SSM quality, if the reference is valid.

Step 4 Click **Apply**.

Step 5 Click **Yes** in the confirmation dialog box.

- If the selected timing reference is invalid, a warning dialog appears. Click **OK**; the NE remains on the original timing reference without performing the switch.
- If the selected timing reference is an acceptable valid reference, the NE switches to the selected timing reference.

Step 6 Return to your originating procedure (NTP).

DLP-C178 Clear a Manual or Force Switched 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-C29 Log into CTC, page 17-44
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. The Timing Source window appears.

Step 2 Find the Clock reference that is currently set to Manual or Force in the Operation drop-down list.

Step 3 Click the Operation drop-down list for the clock and choose **Clear**.

Step 4 Click **Apply**.

Step 5 Click **Yes** in the confirmation dialog box.

- If the normal timing reference is invalid or has failed, a warning dialog appears. Click **OK**; the NE remains on the previous timing reference without performing the switch.
- If the normal timing reference is an acceptable valid reference, the NE reverts to the normal timing reference as defined by the system configuration.

Step 6 Return to your originating procedure (NTP).

DLP-C179 Initiate an Optical Protection Switch

Purpose	This procedure initiates a Manual or Force switch on an optical port.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 that you want to switch.

Step 3 In the Selected Group area, select the card and port that 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 (SD) bit error rate (BER) threshold. A Force switch will switch traffic even if the path has SD or signal fail (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-C180 Change a VCAT Member Service State

Purpose	This task changes a VCAT member service state on the Edit Circuit window.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
	VCAT 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 CTC only permits you to change the state of a non-LCAS member 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-MA,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.

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-C181 Install the LAN Cable for CTC Interface

Purpose	This task installs the LAN cable to provide a 10/100 Mbps Ethernet interface for CTC/TL1 provisioning.
Tools/Equipment	CAT-5 RJ-45 cable
Prerequisite Procedures	NTP-C2 Install the Shelf Assembly, page 1-4
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the LAN cable into the LAN port on the front of the ONS 15310-CL (Figure 17-9 on page 17-12).

Step 2 Connect the other end to the PC you want to use to access CTC.

Table 18-8 shows the LAN cable pin assignments.

Table 18-8 LAN Cable Pin Assignments

RJ-45 Pin Number	Function
1	TX +
2	TX –
3	RX +
4	NC
5	NC
6	RX –
7	NC
8	NC

Step 3 Return to your originating procedure (NTP).

DLP-C182 Turn On and Verify AC Office Power

Purpose	This task verifies the chassis LED activity and verifies power on the AC ONS 15310-CL chassis.
Tools/Equipment	Voltmeter
Prerequisite Procedures	DLP-C5 Connect the Office Ground to the ONS 15310-CL, page 17-5
	DLP-C6 Connect AC Office Power to the ONS 15310-CL, page 17-6
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug the power cord into an AC wall socket or UPS power supply outlet.

Step 2 Verify the chassis LED activity (Figure 17-9 on page 17-12):

a. The FAIL LED blinks red for 20 to 30 seconds, then turns off.

b. The ALARM LED is off.

c. The PWR LED is green.

d. The SYNC LED is green.

Step 3 If the ONS 15310-CL does not power up, check the voltage at the power source using a voltmeter. The voltage should be 100-240VAC +/–10 percent.

Step 4 Return to your originating procedure (NTP).

DLP-C183 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-C29 Log into CTC, page 17-44
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 start a roll.

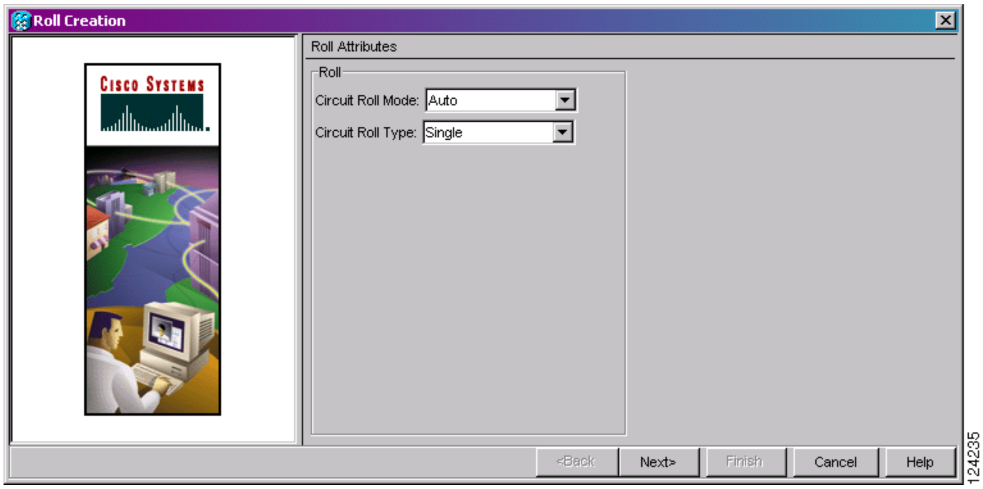
Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

Step 5 In the Roll Attributes area, complete the following (Figure 18-9):

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 18-9 Selecting Single Roll Attributes



Roll Creation

Roll Attributes

Roll

Circuit Roll Mode: Auto

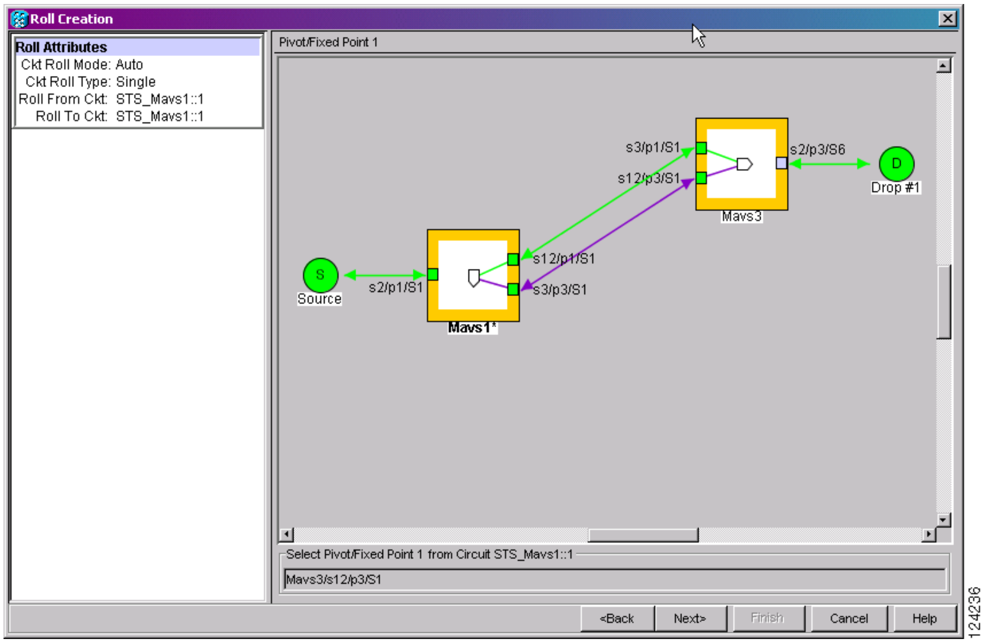
Circuit Roll Type: Single

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 18-10).

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 18-10 Selecting a Path



Roll Creation

Roll Attributes
Ckt Roll Mode: Auto
Ckt Roll Type: Single
Roll From Ckt: STS_Mavs1::1
Roll To Ckt: STS_Mavs1::1

Pivot/Fixed Point 1

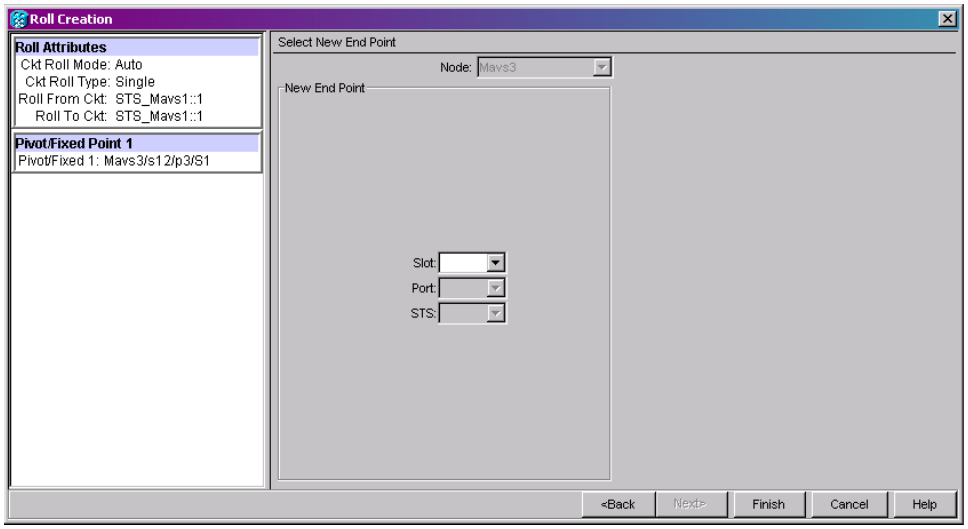
Select Pivot/Fixed Point 1 from Circuit STS_Mavs1::1

Mavs3/s12/p3/S1

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 18-11).

Figure 18-11 Selecting a New Endpoint



Roll Creation

Roll Attributes

Ckt Roll Mode: Auto
Ckt Roll Type: Single
Roll From Ckt: STS_Mavs1::1
Roll To Ckt: STS_Mavs1::1

Pivot/Fixed Point 1

Pivot/Fixed 1: Mavs3/s12/p3/S1

Select New End Point

Node: Mavs3

New End Point

Slot:
Port:
STS:

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 18-12). For the pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with Step 12.

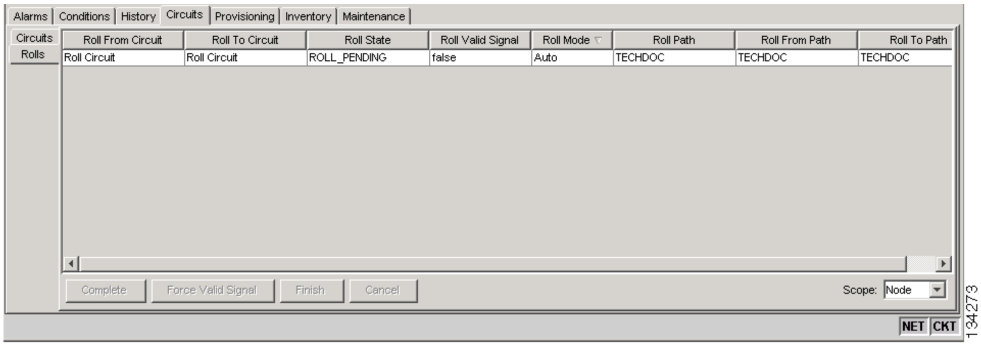
- If the Roll Valid Signal status is true, a valid signal was found on the new port.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. To cancel the roll, see the "DLP-C189 Cancel a Roll" task on page 18-88.
- 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.

- 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 18-12 Viewing the Rolls Tab



Roll From Circuit	Roll To Circuit	Roll State	Roll Valid Signal	Roll Mode	Roll Path	Roll From Path	Roll To Path
Roll Circuit	Roll Circuit	ROLL_PENDING	false	Auto	TECHDOC	TECHDOC	TECHDOC

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-C184 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-C29 Log into CTC, page 17-44 DLP-C52 Provision Section DCC Terminations, page 17-68 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 complete 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**.

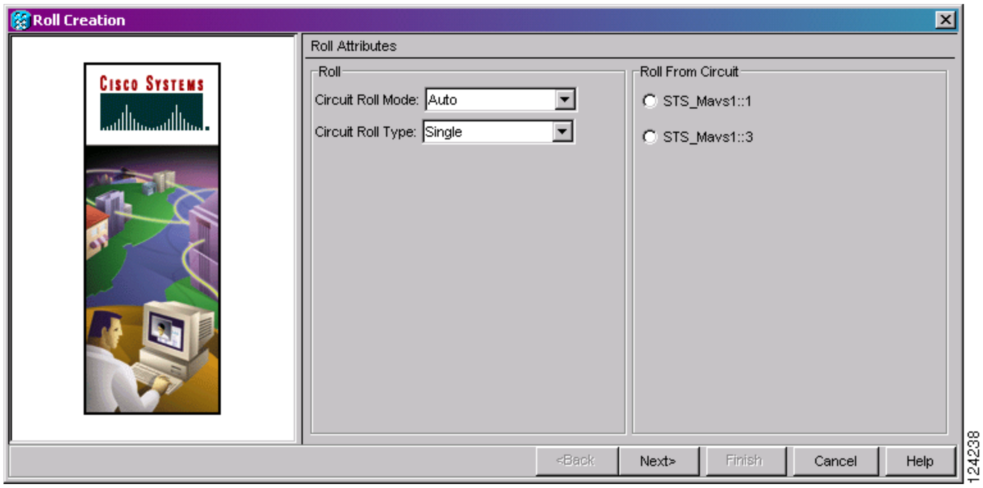
Step 5 In the Roll Attributes area, complete the following (Figure 18-13):

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 18-13 Selecting Roll Attributes for a Single Roll onto a Second Circuit



Roll Creation

Roll Attributes

Roll

Circuit Roll Mode: Auto

Circuit Roll Type: Single

Roll From Circuit

○ STS_Mavs1::1

○ STS_Mavs1::3

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 18-10 on page 18-76).

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.
- 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. To cancel the roll, see the "DLP-C189 Cancel a Roll" task on page 18-88.
- 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 once the roll is completed.

Step 12 If you selected Manual in Step 5, click the roll on the Rolls tab and click **Complete** to route the traffic to the new port. 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-C185 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-C29 Log into CTC, page 17-44
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 has the connections that you want to roll. The circuit must have a DISCOVERED status for you to start a roll.

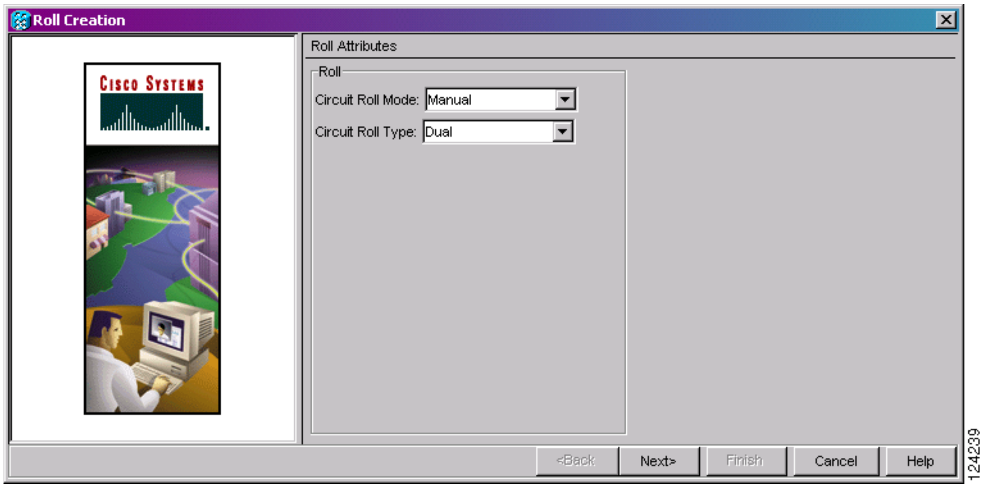
Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

Step 5 In the Roll Attributes area, complete the following (Figure 18-14):

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 18-14 Selecting Dual Roll Attributes



Roll Creation

Roll Attributes

Roll

Circuit Roll Mode: Manual

Circuit Roll Type: Dual

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 18-10 on page 18-76).

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.

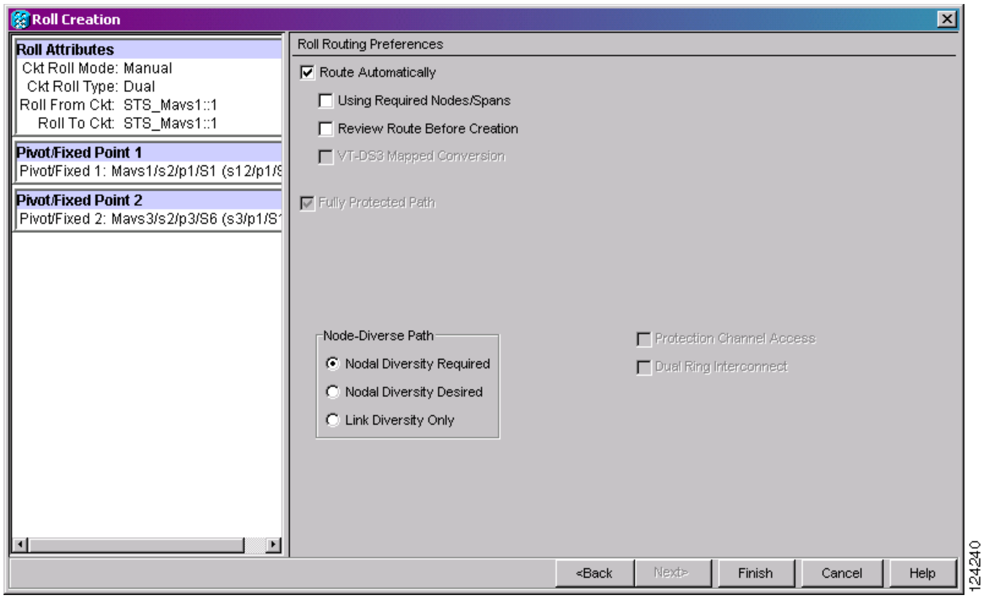
The path that is not selected is the Roll From path. The Roll From path is deleted after the roll is completed. The path identifier appears in the text box below the graphic image.

Step 11 Click **Next**.

Step 12 In the Circuit Routing Preferences area, check **Route Automatically** to allow CTC to find the route (Figure 18-15). 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 18-15 Setting Roll Routing Preferences



Roll Creation

Roll Attributes
Ckt Roll Mode: Manual
Ckt Roll Type: Dual
Roll From Ckt: STS_Mavs1::1
Roll To Ckt: STS_Mavs1::1

Pivot/Fixed Point 1
Pivot/Fixed 1: Mavs1/s2/p1/S1 (s12/p1/S

Pivot/Fixed Point 2
Pivot/Fixed 2: Mavs3/s2/p3/S6 (s3/p1/S1

Roll Routing Preferences

☑ Route Automatically
□ Using Required Nodes/Spans
□ Review Route Before Creation
□ VT-DS3 Mapped Conversion

☑ Fully Protected Path

Node-Diverse Path
● Nodal Diversity Required
○ Nodal Diversity Desired
○ Link Diversity Only

□ Protection Channel Access
□ Dual Ring Interconnect

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 port mentioned in this statement. If the termination port is the DS-1 port, 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 DS-1 port 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 tabs. On the DS-1 port, Send AIS-V for Ds1 AIS only works for 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.
- 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 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*. To cancel the roll, see the "DLP-C189 Cancel a Roll" task on page 18-88.
- 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 once the roll is completed.

Step 19 If you selected Manual in Step 5, click both rolls on the Rolls tab and click **Complete** to route the traffic to the new port. 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-C186 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-C29 Log into CTC, page 17-44
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 start a roll.

Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

Step 5 In the Roll Attributes area, complete the following (Figure 18-14 on page 18-81):

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 18-10 on page 18-76).

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 18-15 on page 18-82).
- 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-C64 Provision an OC-N Circuit Route" task on page 17-81.

Caution The following is only seen with DUAL roll mode when both ends of the circuit use the port mentioned in this statement. If the termination port is the DS-1 port, 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 DS-1 port 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 tabs. On the DS-1 port, Send AIS-V for Ds1 AIS only works for 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.
- 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. To cancel the roll, see the "DLP-C189 Cancel a Roll" task on page 18-88.
- 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 once the roll is completed.

Step 19 If you selected Manual in Step 5, click each roll and click **Complete** to route the traffic to the new port. 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-C187 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-C29 Log into CTC, page 17-44
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 complete 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 18-10 on page 18-76).

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 18-15 on page 18-82).
- 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 port mentioned in this statement. If the termination port is the DS-1 port, 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 DS-1 port 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 tabs. On the DS-1 port, Send AIS-V for Ds1 AIS only works for VT circuits.

Step 12 Click **Finish**. In the Circuits tab, the Roll From and Roll To circuits change from the DISCOVERED status to ROLL RENDING.

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.
- 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. To cancel the roll, see the "DLP-C189 Cancel a Roll" task on page 18-88.
- 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 once the roll is completed.

Step 14 If you selected Manual in Step 5, click both rolls on the Rolls tab and click **Complete** to route the traffic to the new port. 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-C188 Delete a Roll

Purpose	This task deletes a roll. Use caution when selecting this option, traffic may be affected. Delete a roll only if it cannot be completed or cancelled in normal ways. Circuits may have a PARTIAL status when this option is selected. See Table 18-5 on page 18-13 for a description of circuit statuses.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 NTP-C129 Bridge and Roll Traffic, page 7-10
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-C189 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, cancel 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-C29 Log into CTC, page 17-44 NTP-C129 Bridge and Roll Traffic, page 7-10
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 once 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 the 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-C190 Provision CE-100T-8 Card Ethernet Ports

Purpose	This task provisions the CE-100T-8 card Ethernet ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The user can provision SONET CCAT or VCAT circuits for the CE-100T-8 card before or after provisioning the card's Ethernet ports or POS ports. See the "NTP-C47 Create an Automatically Routed Optical Circuit" procedure on page 6-34 or the "NTP-C51 Create an Automatically Routed VCAT Circuit" procedure on page 6-46, as needed.

Step 1 In the node view, double-click the CE-100T-8 card graphic to open the card.

Step 2 Click the **Provisioning** > **Ether Ports** tabs.

Step 3 For each CE-100T-8 port, provision the following parameters:

- Port Name—If you want to label the port, enter the port name.
- Admin State—Choose **IS** to put the port in service. Putting an Ethernet port into IS-NR also puts the mapped POS port in IS-NR.
- 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** 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 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 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 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 card attempts to negotiate symmetrical flow control with the attached device.
- 802.1Q VLAN CoS—For a CoS-tagged frame, the CE-100T-8 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 card can also map any of the 256 priorities specified in IP 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. In card view, click the **Performance > POS Ports > Statistics** tabs.

b. Click **Refresh**.

Note Reprovisioning an Ethernet port on the CE-100T-8 card does not reset the Ethernet statistics for that port.

Step 6 Return to your originating procedure (NTP).

DLP-C191 Provision CE-100T-8 Card POS Ports

Purpose	This task provisions CE-100T-8 card POS ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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-100T-8 card before or after provisioning the card's Ethernet ports or POS ports. See the "NTP-C47 Create an Automatically Routed Optical Circuit" procedure on page 6-34 or the "NTP-C51 Create an Automatically Routed VCAT Circuit" procedure on page 6-46, as needed.

Step 1 In the node view, double-click the CE-100T-8 card graphic to open the card.

Step 2 Click the **Provisioning** > **POS Ports** tabs.

Step 3 For each CE-100T-8 port, provision the following parameters:

- Port Name—If you want to label the port, enter the port name.
- Admin State—Choose **IS** to put the port in the IS-NR service state. Putting a POS port in IS-NR also puts the mapped Ethernet port in IS-NR.
- 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** 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 on the interoperabilty of ONS Ethernet cards, including information on encapsulation, framing, and CRC, refer to the "POS on ONS Ethernet Cards" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Note The CE-100T-8 card 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. In card view, click the **Performance > POS Ports > Statistics** tabs.

b. Click **Refresh**.

Step 6 Return to your originating procedure (NTP).

DLP-C192 Provision a Multirate Pluggable Port Module

Purpose	This task provisions a multirate (OC-3/OC-12/OC-48) PPM in CTC. If a multirate PPM was preprovisioned, skip this procedure and go directly to the "DLP-C193 Provision the Optical Line Rate" task on page 18-92.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Multirate PPMs for the ONS 15310-CL support OC-3 and OC-12 line rates. Multirate PPMs for the ONS 15310-MA support OC-3, OC-12, and OC-48 line rates.

Step 1 In node view, double-click the 15310-CL-CTX card (ONS 15310-CL) or the CTX2500 card (ONS 15310-MA).

Step 2 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 3 In the Pluggable Port Modules area, click **Create**. The Create PPM dialog box appears.

Step 4 In the Create PPM dialog box, complete the following:

- PPM—Click the slot number where the SFP is installed from the drop-down list.
- PPM Type—Click the number of ports supported by your 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 in the Pluggable Port Modules area. The row on the Pluggable Port Modules area turns white and the Actual Equipment Type column lists the equipment name.

Step 6 Verify that the PPM appears in the list in the Pluggable Port Modules area. If it does not, repeat Steps 3 through 5.

Step 7 Repeat the task to provision a second PPM.

Step 8 Click **OK**.

Step 9 Continue with the "DLP-C193 Provision the Optical Line Rate" task on page 18-92 to provision the multirate PPM for OC-3 or OC-12.

Step 10 Return to your originating procedure (NTP).

DLP-C193 Provision the Optical Line Rate

Purpose	This task provisions the line rate on the ONS 15310-CL (OC-3 or OC-12) or ONS 15310-MA (OC-3, OC-12, or OC-48) on a multirate PPM. Single-rate PPMs do not need to be provisioned.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C192 Provision a Multirate Pluggable Port Module, page 18-92

Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If you plug in a single-rate SFP, the PPM will autoprovision and no further steps are necessary. If you plug in a multirate SFP, you need to provision the PPM and then provision the rate on the PPM tab by following this task. This is the node default behavior, but it can be changed by NE default settings. Refer to the "NTP-C137 Edit Network Element Defaults" procedure on page 15-18.

Step 1 In node view, for the ONS 15310-CL, double-click the 15310-CL-CTX card; for the ONS 15310-MA, double-click the CTX2500 card.

Step 2 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 3 In the Pluggable Ports area, click **Create**. The Create Port dialog box appears.

Step 4 In the Create Port dialog box, complete the following:

- Port—Select 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 with one port displays as 1-1 and the second PPM with one port displays as 2-1. The PPM number can be 1 to 4, but the port number is always 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. For the 15310-CL-CTX card, OC-3 (155 Mbps) and OC-12 (622 Mbps) rates are supported. For the CTX2500 in the 15310-MA, OC-3, OC-12, and OC-48 rates are supported.

Step 5 Click **OK**.

Step 6 Repeat Steps 3 through 5 to configure the port rates as needed.

Step 7 Click **OK**.

Step 8 Return to your originating procedure (NTP).

DLP-C194 Change the Optical Line Rate

Purpose	This task changes the port rate on a multirate PPM. Multirate PPMs for the ONS 15310-CL support OC-3 and OC-12 line rates. Multirate PPMs for the ONS 15310-MA support OC-3, OC-12, and OC-48 line rates.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
	DLP-C192 Provision a Multirate Pluggable Port Module, page 18-92
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the 15310-CL-CTX card or CTX2500 card.

Step 2 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 3 Click the port with the port rate that you want to change in the Pluggable Ports area. 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-C195 Delete Pluggable Port Modules

Purpose	This task deletes PPM provisioning for SFPs on the ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C192 Provision a Multirate Pluggable Port Module, page 18-92
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that you can delete the PPM. 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:

- NTP-C143 Modify or Delete Card Protection Settings, page 11-5
- NTP-C82 Change Node Timing, page 11-6
- NTP-C85 Modify or Delete Communications Channel Terminations and Provisionable Patchcords, page 11-8
- NTP-C71 Modify and Delete Circuits, page 7-3
- NTP-C72 Modify and Delete Overhead Circuits and Server Trails, page 7-4
- DLP-C50 Change the Service State for a Port, page 17-67

Step 2 In node view, for the ONS 15310-CL, double-click the 15310-CL-CTX card; for the ONS 15310-MA, double-click the CTX2500 card.

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 area. 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 area and the Pluggable Ports area.

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 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, complete the "DLP-C17 Remove SFP Connectors" task on page 17-23.

Step 7 Return to your originating procedure (NTP).

DLP-C196 Configure the Node for RADIUS Authentication

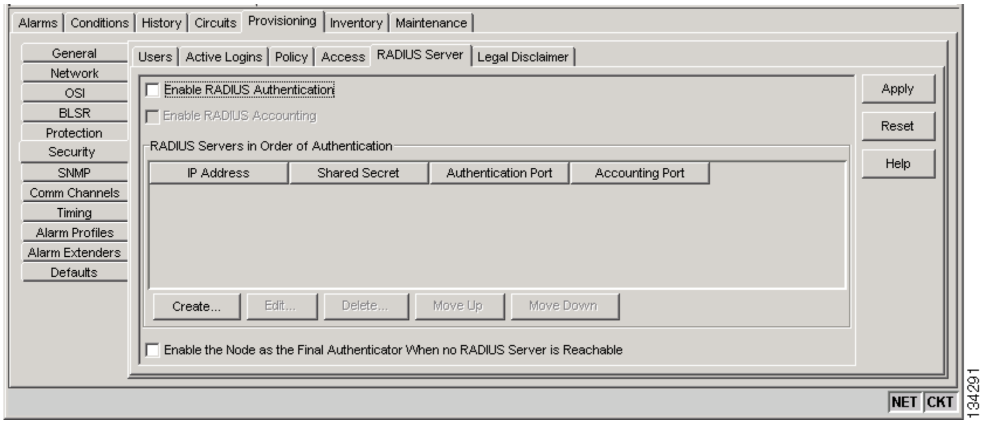
Purpose	This task allows you to configure a node for Remote Authentication Dial In User Service (RADIUS) authentication. RADIUS validates remote users who are attempting to connect to the network.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44 Before configuring the node 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.

Step 1 In node view, click the **Provisioning > Security > RADIUS Server** tabs (Figure 18-16).

Figure 18-16 RADIUS Server Tab



☐ Enable RADIUS Authentication

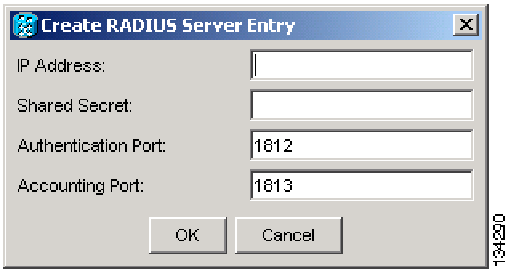
☐ Enable RADIUS Accounting

RADIUS Servers in Order of Authentication

☐ Enable the Node as the Final Authenticator When no RADIUS Server is Reachable

Step 2 Click **Create** to add a RADIUS server to the list of authenticators. The Create RADIUS Server Entry window appears (Figure 18-17).

Figure 18-17 Create RADIUS Server Entry Window



IP Address:

Shared Secret:

Authentication Port: 1812

Accounting Port: 1813

Step 3 Enter the RADIUS server IP address in the IP 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.

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-C197 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-C29 Log into CTC, page 17-44
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, SSH, or SFTP)
- 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).

CHAPTER 19

DLPs C200 to C299

DLP-C200 Provision OSI Routing Mode

Purpose	This task provisions the Open System Interconnection (OSI) routing mode. Complete this task when the ONS 15310-CL or ONS 15310-MA 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	DLP-C29 Log into CTC, page 17-44
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 or IS Level 1. This decision must be carefully considered. For additional information about OSI provisioning, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA 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 The ONS 15310 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 In node view, click the **Provisioning** > **OSI** > **Main Setup** tabs.

Step 2 Choose a routing mode:

- End System—The ONS 15310 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 15310 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.

Step 3 If needed, change the L1 LSP Buffer Size. This adjusts the Level 1 link state protocol data unit (PDU) buffer size. The default is 512. It should not be changed.

Step 4 Return to your originating procedure (NTP).

DLP-C201 Provision or Modify TARP Operating Parameters

Purpose	This task provisions or modifies the Target Identifier Address Resolution Protocol (TARP) operating parameters including TARP PDU propagation, timers, and loop detection buffer (LDB).
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
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 This parameter is not used when the Node Routing Area (Provisioning > OSI > Main Setup tab) is set to End System.

- 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 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.

- 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.

Note 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 15310 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 Timers T1, T2, and T4 are not used if TARP PDUs Origination is not enabled.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-C202 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-C29 Log into CTC, page 17-44
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-C203 Remove a Static TID to NSAP Entry from the TARP Data Cache

Purpose	This task removes a static TID to NSAP entry from the Tarp Data Cache (TDC).
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
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-C204 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 15310-CL or ONS 15310-MA must communicate across routers or non-SONET NEs that lack TARP capability.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
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-C205 Provision OSI Routers

Purpose	This task enables the OSI virtual router and edits its primary manual area address.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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.

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 **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-C206 Provision Additional Manual Area Addresses

Purpose	This task provisions the OSI manual area addresses. Three additional manual areas can be created for each virtual router.
Tools/Equipment	None
Prerequisite Procedures	DLP-C205 Provision OSI Routers, page 19-6 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 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 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 **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-C207 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-C29 Log into CTC, page 17-44
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-C52 Provision Section DCC Terminations" task on page 17-68 and the "DLP-C53 Provision Line DCC Terminations" task on page 17-70.

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 15310-CL or ONS 15310-MA 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-C208 Create an IP-Over-CLNS Tunnel

Purpose	This task creates an IP-over-CLNS tunnel to allow ONS 15310-CL or ONS 15310-MA nodes to communicate across equipment and networks that use the OSI protocol stack.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 15310-CL or ONS 15310-MA. The other end point is generally provisioned on non-ONS equipment including routers and other vendor NEs. Before you begin, verify that you have the capability to create an IP-over-CLNS 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 CLNS 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.

- Node Address—Enter the IP address of the IP-over-CLNS tunnel destination.
- Subnet Mask—Enter the IP address subnet mask of the IP-over-CLNS destination.
- OSPF Cost—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.

Step 6 Return to your originating procedure (NTP).

DLP-C209 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-C29 Log into CTC, page 17-44
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-C211 Edit the OSI Router Configuration

Purpose	This task edits 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-C29 Log into CTC, page 17-44
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 Choose 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-C212 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-C29 Log into CTC, page 17-44
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 > 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.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-C213 Edit an IP-Over-CLNS Tunnel

Purpose	This task edits the parameters of an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite procedures	DLP-C208 Create an IP-Over-CLNS Tunnel, page 19-8 DLP-C29 Log into CTC, page 17-44
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 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—Edit the 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-C214 Delete an IP-Over-CLNS Tunnel

Purpose	This task allows you to delete an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
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 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-C215 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-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In 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 network service access point (NSAP) of the IS.
- MAC Address—For destination NEs that are accessed by LAN subnets, the NE's MAC 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-C216 View ES-IS Routing Information Base

Purpose	This task allows you to view the End-System-to-Intermediate-System (ES-IS) protocol 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-C29 Log into CTC, page 17-44
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.
- MAC Address—For destination NEs that are accessed by LAN subnets, the NE's MAC 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-C217 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-C29 Log into CTC, page 17-44
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 NSAP or Network Element Title (NET) of the originating NE.
- Type—Indicates how the TDC 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 TDC is not enabled on the Provisioning > OSI > TARP tab.

a. Click the **TID to NSAP** button.

b. In the TID to NSAP dialog box, enter the TID that you want to map to an NSAP.

c. Click **OK**, then click **OK** in 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-C218 Soft-Reset a 15310-CL-CTX or CTX2500 Card Using CTC

Purpose	This task resets a 15310-CL-CTX (ONS 15310-CL) or CTX2500 (ONS 15310-MA) card using a soft reset. A soft reset reboots the card and reloads the operating system and the application software. If there are two CTX2500 cards installed on the ONS 15310 MA the standby CTX2500 will become active after issuing an active CTX soft-reset.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Caution Soft-resetting the 15310-CL-CTX or CTX2500 cards causes a traffic hit only if a provisioning change or firmware update has occurred. Otherwise, the soft reset is errorless.

Caution Do not soft reset more than one ONS 15310-MA card at a time. Instead, issue a soft reset command for a single card, then wait until CTC shows the card is back up. You can then issue a soft reset on another card if needed. Completing soft resets in sequence helps to avoid unexpected traffic hits.

Note Before you reset the 15310-CL-CTX or CTX2500 card, you should wait at least 60 seconds after the last provisioning change to avoid losing any changes to the database.

Note The 15310-CL-CTX and CTX2500 cards do not support a real time clock with battery backup. Hence, during a card reset, the time is reset to default and the date starts at 1970 till you set the time/date again.

Note A software reset causes a standard Telcordia protection switch of less than 50 ms.

Step 1 In node view, right-click the 15310-CL-CTX card or the CTX2500 card to reveal a drop-down list.

Step 2 Click **Soft-Reset Card**.

Note For an ONS 15310-MA, if there is any condition that prevents an errorless soft-reset, the "Force Soft-Reset" message appears. You can choose to abort the soft-reset or proceed with the forced soft-reset.

Step 3 Click **Yes** when the "Are You Sure?" dialog box appears.

Step 4 Return to your originating procedure (NTP).

DLP-C219 Hard-Reset the 15310-CL-CTX or CTX2500 Card Using CTC

Purpose	This task resets the 15310-CL-CTX card (ONS 15310-CL) or CTX2500 card (ONS 15310-MA) using a hard reset. A hard reset temporarily removes power from the card and clears all buffer memory.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Caution Typically a hard reset causes a standard Telcordia protection switch of less than 50 ms. However, in the following scenarios, hard-resetting the 15310-CL-CTX or CTX2500 cards causes a traffic loss until the 15310-CL-CTX or CTX2500 card fully resets:

If a 1+1 protection group is provisioned between optical ports located on the same 15310-CL-CTX or CTX2500 card.

If both paths of a path protection configuration traverse through optical ports on the same 15310-CL-CTX or CTX2500.

Note Before you reset the 15310-CL-CTX or CTX2500 card, you should wait at least 60 seconds after the last provisioning change to avoid losing any changes to the database.

Note The 15310-CL-CTX and CTX2500 cards do not support a real time clock with battery backup. Hence, during a card reset, the time is reset to default and the date starts at 1970 till you set the time/date again.

Step 1 In node view, click the **Inventory** tab. Locate the 15310-CL-CTX or CTX2500 card in the inventory pane.

Step 2 Click the **Admin State** drop-down list and select **OOS-MT**. 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 OOS-MA,MT. The card faceplate appears blue in CTC.

Step 5 Right-click the card to reveal a shortcut 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-C220 Soft-Reset an Ethernet or Electrical Card Using CTC

Purpose	This task resets the ML-100T-8, CE-100T-8, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card using a soft reset. A soft reset reboots the card and reloads the operating system and the application software.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Caution Do not soft reset more than one ONS 15310-MA card at a time. Instead, issue a soft reset command for a single card, then wait until CTC shows the card is back up. You can then issue a soft reset on another card if needed. Completing soft resets in sequence helps to avoid unexpected traffic hits.

Caution Soft-resetting an Ethernet card causes a traffic hit. However, soft-resetting a traffic card 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 shortcut 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-C221 Hard-Reset an Ethernet or Electrical Card Using CTC

Purpose	This task resets the ML-100T-8, CE-100T-8, DS1-28/DS3-EC1-3, or DS1-28/DS3-EC1-3 card using a hard reset. A hard reset temporarily removes power from the card and clears all buffer memory before it is physically reseated.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Caution Hard-resetting a traffic card causes a traffic hit.

Note The hard-reset option is enabled only when the card is placed 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 list and select **OOS-MT**. 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 OOS-MA,MT. The card faceplate appears blue in CTC and the SRV LED turns amber.

Step 5 Right-click the card to reveal a shortcut 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-C222 Print CTC Data

Purpose	This task prints CTC card, node, or network data in graphical or tabular form on a Windows-provisioned printer.
Tools/Equipment	Printer connected to the CTC computer by a direct or network connection
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Click the CTC 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 (default login), and card view windows.

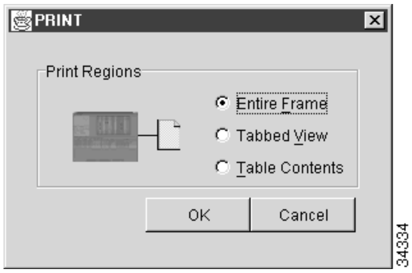
Step 2 From the File menu, choose **Print**.

Step 3 In the Print dialog box, click a a printing option (Figure 19-1).

- 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.The Table Contents option prints all the data contained in a table with the same 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 determine whether the printout applies to the network, node, or card view. Look at the tabs to determine which view you are printing. Network, node, and card views are identical except that network view does not contain an Inventory tab; node view and card view contain a Performance tab.

Figure 19-1 Selecting CTC Data For Print



Print Regions

● Entire Frame
○ Tabbed View
○ Table Contents

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-C223 Export CTC Data

Purpose	This task exports CTC table data as delineated text to view or edit the data in text editor, word processing, spreadsheet, database management, or web browser applications. You can also export data from the Edit Circuits window.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Click the CTC 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**.

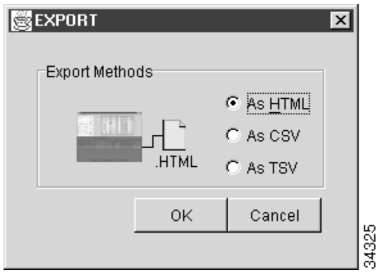
Note Depending upon your configuration, you might or might not see all of the listed tabs when you click Edit.

Step 3 From the File menu, choose **Export**.

Step 4 In the Export dialog box (Figure 19-2), click a data format:

- **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 tab.
- **As TSV**—Saves the CTC table as tab-separated values (TSV).

Figure 19-2 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 display the CTC data, or you can double-click the file name and choose an application such as Notepad.

Text editor and word processor applications display 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 display 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 applies to all tabular data except the following:

- Circuits (Edit option, General, and Monitor tabs)
- Provisioning > General tab
- Provisioning > Network > General tab
- Provisioning > Orderwire tab
- Provisioning > Security > Policy, Data Comm, Access, and Legal Disclaimer tabs
- Provisioning > SNMP tab
- Provisioning > Timing > General and BITS Facilities tabs
- Provisioning > OSI > Main Setup tab
- Provisioning > OSI > TARP > Config tab
- Maintenance > Database tab
- Maintenance > Diagnostic tab
- Maintenance > Protection tab
- Maintenance > Timing > Source tab

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 the 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-C224 Change Optics Thresholds Settings for Optical Ports

Purpose	This task changes the optics threshold settings on optical ports. Optical ports on the ONS 15310-CL and ONS 15310-MA are provided through Small Form-factor Pluggables (SFPs) installed on the 15310-CL-CTX card (ONS 15310-CL) and the CTX2500 card (ONS 15310-MA).
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the 15310-CL-CTX card or the CTX2500 card.

Step 2 Click the **Provisioning > Optical > Optics Thresholds** tabs.

Note If you want to modify a threshold setting, it might be necessary to click 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 19-1 by clicking in the field that you want to modify. In some fields, you can choose an option from a drop-down list; in others you can type a value.

Note You must set the normalized optical power received (OPR) value whenever you replace or insert an SFP. After you click Set for the port you are observing, the LBC (%), OPR (%), and OPT (%) values under the Performance > Optical tabs should be close to 100 percent. Only Cisco-approved SFPs should be used. See Chapter 1, "Install the Cisco ONS 15310-CL" or Chapter 2, "Install the Cisco ONS 15310-MA" for more information about installing SFPs and fiber-optic cable.

Table 19-1 Optics Thresholds Settings

Parameter	Description	Options
Port	(Display only) Port number.	• 1-1 • 2-1
LBC-LOW	Laser bias current–minimum.	Default (15 min/1 day): 50 percent
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

Table 19-1 Optics Thresholds Settings (continued)

Parameter	Description	Options
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 type of alert that occurs when a threshold is crossed. To change the type of threshold, choose one and click **Refresh**.	• TCA (threshold crossing 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 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-C225 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 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 Node Address—Enter the IP address of your network management system (NMS).
- Community—Enter the SNMP community name. (For more information about SNMP, refer to the "SNMP" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.)

Note The community name is a form of authentication and access control. The community name assigned to the ONS 15310 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.

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 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 8 Click **Apply**.

Step 9 Return to your originating procedure (NTP).

DLP-C226 Set Up SNMP for an ENE

Purpose	This procedure provisions the SNMP parameters for an ONS 15310-CL or ONS 15310-MA configured to be an ENE if you use SNMP proxy on the GNE.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 Node Address—Enter the IP address of your NMS.

- Community—Enter the SNMP community name. (For more information about SNMP, refer to the "SNMP" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.)

  Note The community name is a form of authentication and access control. The community name assigned to the ONS 15310 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.

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 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 8 Click **Apply**.

Step 9 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 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 A > RELAY B > RELAY C > NMS. For example:

- If there is are 0 intermediate relays, the order is ENE > RELAY A (GNE) > NMS
- If there is 1 intermediate relay, the order is ENE > RELAY A (NE 1) > RELAY B (GNE) > NMS
- If there is are 0 intermediate relays, the order is ENE > RELAY A (NE 1) > RELAY B (NE 2) > RELAY C (GNE) > NMS

Step 10 Click **Apply**.

Step 11 Repeat Step 2 through Step 10 for all NEs between the GNE and ENE.

Step 12 Return to your originating procedure (NTP).

DLP-C227 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-C29 Log into CTC, page 17-44
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 15310-CL or ONS 15310-MA 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 15310.

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 15310.

Step 4 On this 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 15310 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-C228 Provision Orderwire

Purpose	This task provisions orderwire.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 nodes, you can use either local or express orderwire channels. If regenerators exist, use the express orderwire channel.
- 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 nodes that reside 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-C229 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-C29 Log into CTC, page 17-44
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 link icons, 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 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:

a. Right-click the link on the network map.

b. Choose **Collapse [*link class*] Link** from the shortcut menu, where “link class” is DCC, GCC, OTS, PPC, or server trail. 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 19-3 shows the network view with unconsolidated DCC and PPC links.

Figure 19-3 Unconsolidated Links in the Network View

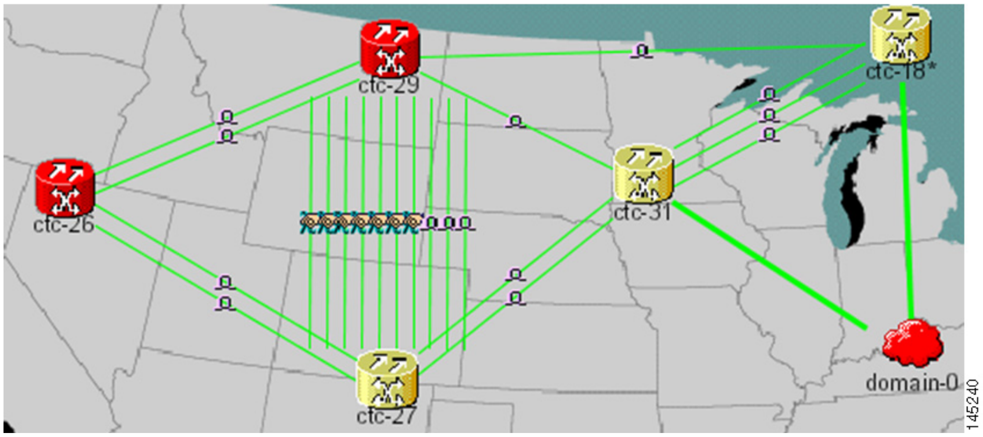


Figure 19-4 shows a network view with globally consolidated links.

Figure 19-4 Consolidated Links in the Network View

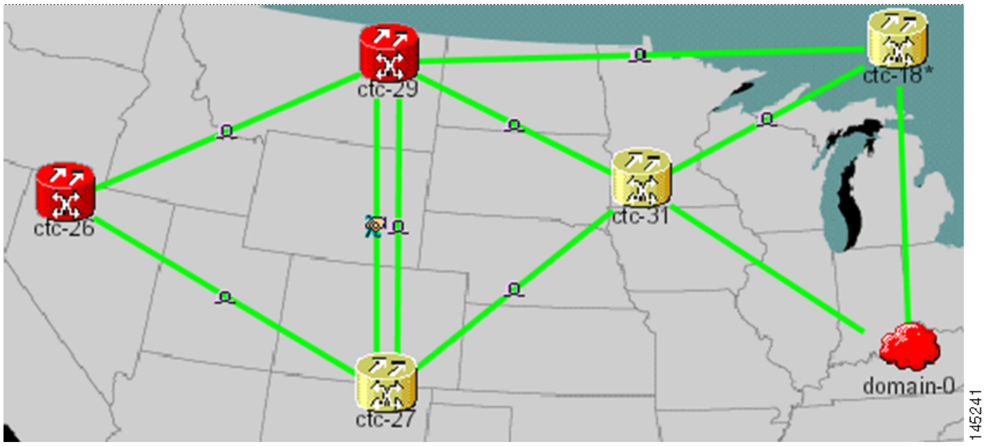
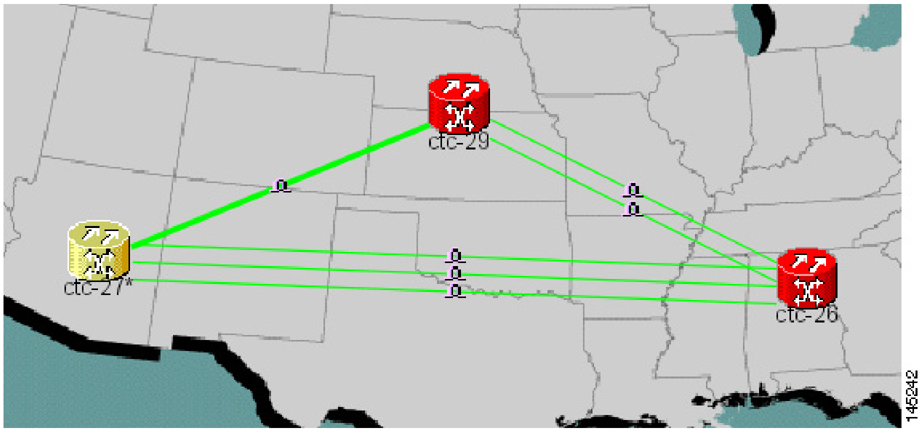


Figure 19-5 shows a network view with local DCC link consolidation between two nodes.

Figure 19-5 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 Links** from the shortcut menu.

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 19-2).

Table 19-2 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-C231 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-C232 Delete a Server Trail

Purpose	This task deletes a server trail.
Tools/Equipment	None
Prerequisite Procedures	NTP-C140 Create a Server Trail, page 6-56 DLP-C29 Log into CTC, page 17-44
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. 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-C233 Change Line and Threshold Settings for DS-1 Ports

Purpose	This task changes line and threshold settings for DS-1 ports on the 15310-CL-CTX card and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Refer to the “Network Element Defaults” appendix in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for DS-1 port default settings.

Step 1 In node view, double-click the 15310-CL-CTX card, DS1-28/DS3-EC1-3 card, or DS1-84/DS3-EC1-3 card where you want to change line or threshold settings.

Step 2 Click the **Provisioning > DS-1** tabs.

Step 3 Depending on the setting you need to modify, click the **Line**, **Line Thresholds**, **Elect Path Thresholds**, **or SONET Thresholds** subtabs.

Note If you want to modify a threshold setting, it might be necessary to click 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 that 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 4 and 5 for each subtab that has parameters you want to provision.

For definitions of line settings, see Table 19-3. For definitions of line threshold settings, see Table 19-4 on page 19-36. For definitions of the electrical path threshold settings, see Table 19-5 on page 19-36. For definitions of SONET threshold settings, see Table 19-6 on page 19-37.

Table 19-3 describes the values on the Provisioning > DS-1> Line tab for the DS-1 ports.

Table 19-3 Line Options for DS-1 Ports

Parameter	Description	Options
Port #	Port number.	• 1 to 21 (15310-CL-CTX, ONS 15310-CL only) • 1 to 28 (DS1-28/DS3-EC1-3; ONS 15310-MA only) • 1 to 84 (DS1-84/DS3-EC1-3; ONS 15310-MA only)
Port Name	Port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default See the "DLP-C56 Assign a Name to a Port" task on page 17-75.

Table 19-3 Line Options for DS-1 Ports (continued)

Parameter	Description	Options
Admin State	Sets the port service state unless network conditions prevent the change.	• IS—(In Service) Puts the port in service. The port service state changes to In Service and Normal (IS-NR). • IS,AINS—(In Service and Automatic In-Service) Puts the port in automatic in-service. The port service state changes to Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS). • OOS,DSBLD—(Out-of-Service and Disabled) Removes the port from service and disables it. The port service state changes to Out-of-Service and Management, Disabled (OOS-MA,DSBLD). • OOS,MT—(Out-of-Service and Maintenance) Removes the port from service for maintenance. The port service state changes to Out-of-Service and Management, Maintenance (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	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 (default) • 1E-5

Table 19-3 Line Options for DS-1 Ports (continued)

Parameter	Description	Options
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 (default) • 1E-8 • 1E-9
Line Type	Defines the line framing type.	• D4 • ESF—Extended Super Frame • Unframed • AUTO PROVISION FMT
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 backplane connection to the next termination point.	• 0 - 131 (default) • 132 - 262 • 263 - 393 • 394 - 524 • 525 - 655
AINS Soak	Automatic in-service soak.	• Duration of valid input signal in hh.mm after which the port is set in service by the software. • 0 to 48 hours, 15-minute increments
Provides Sync	(Display only) If checked, the card is provisioned as a NE timing reference.	• Yes (checked) • No (unchecked)
SyncMsgIn	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.	• Yes (checked, default) • No (unchecked)
Send DoNotUse	When checked, sends a do not use (DUS) message on the S1 byte.	• Yes (checked) • No (unchecked, default)
Enable Retiming	Retiming is an option that, when enabled, removes accumulated jitter and wander from synchronous transport network payload signals.	• Yes (checked) • No (unchecked, default)

Table 19-4 describes the values on the Provisioning > DS-1> Line Thresholds tab for the DS-1 ports.

Table 19-4 Line Thresholds Options for DS-1 Ports

Parameter	Description
Port	Port number • 1 to 21 (15310-CL-CTX, ONS 15310-CL only) • 1 to 28 (DS1-28/DS3-EC1-3; ONS 15310-MA only) • 1 to 84 ((DS1-84/DS3-EC1-3; ONS 15310-MA only)
CV	Coding violations. Available for Near End only.
ES	Errored seconds. Available for Near End and Far End.
SES	Severely errored seconds. Available for Near End only.
LOSS	Number of one-second intervals containing one or more loss of signal (LOS) defects. Available for Near End only.

Table 19-5 describes the values on the Provisioning > DS-1> Elect Path Thresholds tab for the DS-1 ports.

Table 19-5 Electrical Path Threshold Options for DS-1 Ports

Parameter	Description
Port	Port number • 1 to 21 (15310-CL-CTX, ONS 15310-CL only) • 1 to 28 (DS1-28/DS3-EC1-3; ONS 15310-MA only) • 1 to 84 ((DS1-84/DS3-EC1-3; ONS 15310-MA only)
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 and Far End.
CSS	Controlled Slip Seconds. Available for Far End only.
ESA	Errored Seconds-A. Available for Far End only.
ESB	Errored Seconds-B.Available for Far End only.
SEFS	Severely errored framing seconds. Available for Far End only.

Table 19-6 describes the values on the Provisioning > DS-1> SONET Thresholds tab for the DS-1 ports.

Table 19-6 SONET Thresholds Options for DS-1 Ports

Parameter	Description
Port #	DS-1 ports partitioned for synchronous transport signal (STS) • 1 to 21 (15310-CL-CTX, ONS 15310-CL only) • 1 to 28 (DS1-28/DS3-EC1-3; ONS 15310-MA only) • 1 to 84 ((DS1-84/DS3-EC1-3; ONS 15310-MA only)
CV	Coding violations. Available for Near End and Far End.
ES	Errored seconds. Available for Near End and Far End.
FC	Failure count. Available for Near End and Far End.
SES	Severely errored seconds. Available for Near End and Far End.
UAS	Unavailable seconds. Available for Near End and Far End.

Note The threshold value displays after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-C234 Grant Superuser Privileges to Provisioning Users

Purpose	This task enables a provisioning user to retrieve audit logs, clear PM privileges, restore databases, and activate and revert software loads.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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 After you have activated a software load, 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-C235 Change the OSI Routing Mode

Purpose	This task changes the OSI routing mode.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
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 or IS Level 1. This decision must be carefully considered. For additional information about OSI provisioning, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA 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 In node view, click the **Provisioning** > **OSI** > **Main Setup** tabs.

Step 2 The following routing modes are available for the ONS 15310-CL and ONS 15310-MA:

Note Changing a routing mode should be carefully considered. Additional information about protocols are provided in the "Management Network Connectivity" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

- End System—The ONS 15310 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 15310 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.

Step 3 Although Cisco does not recommend changing the LSP (Link State Protocol Data Unit) buffer sizes, you can change the L1 LSP Buffer Size field to change the Level 1 link state PDU buffer size.

Step 4 Return to your originating procedure (NTP).

DLP-C236 Change Line and Threshold Settings for DS-3 Ports

Purpose	This task changes the line and threshold settings for DS-3 ports on the 15310-CL-CTX card and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Refer to the "Network Element Defaults" appendix in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for DS-3 port default settings.

Step 1 In node view, double-click the 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card where you want to change line or threshold settings.

Step 2 Click the **Provisioning > DS-3** tabs.

Step 3 Depending on the setting you need to modify, click the **Line**, **Line Thresholds**, **Elect Path Thresholds**, or **SONET Thresholds** subtab.

Note If you want to modify a threshold setting, it might be necessary to click 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 tabs by clicking in the field that 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 4 and 5 for each subtab that has parameters you want to provision.

For definitions of the line settings, see Table 19-7. For definitions of the line threshold settings, see Table 19-8 on page 19-41. For definitions of the electrical path threshold settings, see Table 19-9 on page 19-41. For definitions of the SONET threshold settings, see Table 19-10 on page 19-42.

Table 19-7 describes the values on the Provisioning > Line tab for the DS-3 ports.

Table 19-7 Line Options for DS-3 Ports

Parameter	Description	Options
Port #	Port number.	• 1 to 3
Port Name	Port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default. See the "DLP-C56 Assign a Name to a Port" task on page 17-75.
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	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 (default) • 1E-5

Table 19-7 Line Options for DS-3 Ports (continued)

Parameter	Description	Options
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 (default) • 1E-8 • 1E-9
Line Type	Defines the line framing type.	• UNFRAMED • M13 (multiplexed DS1 to DS-3 framing) • C Bit (parity framing)
Line Coding	Defines the DS-3 transmission coding type.	• B3ZS (Bipolar 3 Zero Substitution)
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450
AINS Soak	Automatic in-service soak.	• Duration of valid input signal in hh.mm after which the port is set in service by the software. • 0 to 48 hours, 15-minute increments.

Table 19-8 describes the values on the Provisioning > Line Thresholds tab for the DS-3 ports.

Table 19-8 Line Thresholds Options for DS-3 Ports

Parameter	Description
Port	Port number (display only). • 1 to 3
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.
LOSS	Number of one-second intervals containing one or more loss of signal (LOS) defects. Available for Near End and Far End.

Table 19-9 describes the values on the Provisioning > Elect Path Thresholds tab for the DS-3 ports.

Table 19-9 Electrical Path Threshold Options for DS-3 Ports

Parameter	Description
Port	(Display only) Port number. • 1 to 3
CV	Coding violations. Available for Near End (DS3 Pbit and DS3CPbit); and Far End (DS3 CPbit only).

Table 19-9 Electrical Path Threshold Options for DS-3 Ports (continued)

Parameter	Description
ES	Errored seconds. Available for Near End (DS3 Pbit and DS3CPbit); and Far End (DS3 CPbit only).
SAS	Severely errored seconds. Available for Near End, DS3 Pbit only.
SES	Severely errored seconds. Available for Near End (DS3 Pbit and DS3CPbit); and Far End (DS3 CPbit only).
UAS	Unavailable seconds. Available for Near End (DS3 Pbit and DS3CPbit); and Far End (DS3CPbit only).
AISS	Alarm indication signal seconds. Available for Near End, DS3 Pbit only.

Table 19-10 describes the values on the Provisioning > SONET Thresholds tab for the DS-3 ports.

Table 19-10 SONET Thresholds Options for DS-3 Ports

Parameter	Description
Port	Port number • 1 to 3
CV	Coding violations. Available for Near End and Far End.
ES	Errored seconds. Available for Near End and Far End.
FC	Failure count. Available for Near End and Far End.
SES	Severely errored seconds. Available for Near End and Far End.
UAS	Unavailable seconds. Available for Near End and Far End.

Note The threshold value displays after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-C237 Change Line and Threshold Settings for the EC-1 Ports

Purpose	This task changes the line and threshold settings for EC-1 ports on the 15310-CL-CTX card and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Refer to the "Network Element Defaults" appendix in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for DS-3 port default settings.

Step 1 In node view, double-click the 15310-CL-CTX card, DS1-28/DS3-EC1-3 card, or DS1-84/DS3-EC1-3 card where you want to change line or threshold settings.

Step 2 Click the **Provisioning > EC-1** tab.

Step 3 Depending on the setting you need to modify, click the **Line** or **SONET Thresholds** tab.

Note If you want to modify a threshold setting, it might be necessary to click the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

Note To modify settings on the SONET STS tab, see the "DLP-C99 Enable Intermediate-Path Performance Monitoring" task on page 17-119.

Step 4 Modify the settings found under these subtabs by clicking in the field that 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 4 and 5 for each subtab that has parameters you want to provision.

For definitions of the line settings, see Table 19-11 on page 19-43. For definitions of SONET threshold settings, see Table 19-12 on page 19-45.

Table 19-11 describes the values on the Provisioning > EC-1 > Line tab for the EC-1 ports.

Table 19-11 Line Options for EC-1 Ports

Parameter	Description	Options
Port	(Display only) Port number.	• 1 to 3
Port Name	Port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default See the "DLP-C56 Assign a Name to a Port" task on page 17-75.
Port Rate	(Display only) Port rate	• EC1.

Table 19-11 Line Options for EC-1 Ports (continued)

Parameter	Description	Options
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	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 (default) • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 (default) • 1E-8 • 1E-9
PJSTSMon#	Sets the STS that will be used for pointer justification. If set to Off, no STS is used.	• Off • 1

Table 19-11 Line Options for EC-1 Ports (continued)

Parameter	Description	Options
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450
Rx Equalization	Equalizes the receive level in the ONS 15310-CL. Rx Equalization is always on and cannot be changed. This parameter is not available in the ONS 15310-MA.	• None
AINS Soak	Automatic in-service soak.	• Duration of valid input signal in hh.mm after which the port is set in service by the software • 0 to 48 hours, 15-minute increments

Table 19-12 describes the values on the Provisioning > SONET Thresholds tab for the EC-1 ports.

Table 19-12 SONET Thresholds Options for EC-1 Ports

Parameter	Description
Port	(Display only) Port number. • 1 to 3
CV	Coding violations. Available for Near End line, section, and path; Far End line and path.
ES	Errored seconds. Available for Near End line, section, and path; Far End line and path.
FC	Failure count. Available for Near End line and path; Far End line and path.
SES	Severely errored seconds. Available for Near End line, section and path; Far End Line and Path.
UAS	Unavailable seconds. Available for Near End line and path; Far End line and path.
PPJC-PDET	Positive Pointer Justification Count, STS Path Detected. Available for Near End and Far End path.
NPJC-PDET	Negative Pointer Justification Count, STS Path Detected. Available for Near End and Far End path.
PPJC-PGEN	Positive Pointer Justification Count, STS Path Generated. Available for Near End and Far End path.
NPJC-PGEN	Negative Pointer Justification Count, STS Path Generated. Available for Near End and Far End path.
PJCDIFF	Pointer Justification Count Difference (the absolute value of the difference between the total number of detected pointer justification counts and the total number of generated pointer justification counts). That is, PJCDiff is equal to (PPJC-PGEN - NPJC-PGEN) – (PPJC-PDET – NPJC-PDET). Available for Near End and Far End path.

Table 19-12 SONET Thresholds Options for EC-1 Ports (continued)

Parameter	Description
PJCS-PDET	Pointer Justification Count Seconds, STS Path Detected (PJCS-PDET) is a count of the one-second intervals containing one or more PPJC-PDET or NPJC-PDET. Available for Near End and Far End path.
PJCS-PGEN	Pointer Justification Count Seconds, STS Path Generated (PJCS-PGEN) is a count of the one-second intervals containing one or more PPJC-PGEN or NPJC-PGEN. Available for Near End and Far End path.
PSC	Protection switching count. Available for Near End line.
PSD	Protection switching duration. Available for Near End line.
PSC-W	Protection Switching Count, Working Line. Available for Near End line. **Note** Bidirectional line switched rings (BLSRs) are not supported on the ONS 15310-CL (although the ONS 15310-CL can be part of a network that contains BLSRs); therefore, the PSC-W, PSC-S, and PSC-R performance monitoring parameters do not increment.
PSD-W	Protection Switching Duration, Working Line. Available for Near End line. **Note** BLSRs are not supported on the ONS 15310-CL card (although the ONS 15310-CL can be part of a network that contains BLSRs); therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.

Step 7 Return to your originating procedure (NTP).

DLP-C238 Change Optical Port Line Settings

Purpose	This task changes the line settings for ONS 15310-CL and ONS 15310-MA optical ports. Optical ports for the ONS 15310-CL are located on the 15310-CL-CTX card; optical ports for the ONS 15310-MA are located on the CTX2500 card.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Refer to the “Network Element Defaults” appendix in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for ONS 15310-CL and ONS 15310-MA port default settings.

Step 1 In node view, double-click the 15310-CL-CTX card or the CTX2500 card.

Step 2 Click the **Provisioning > Optical > Line** tabs.

Note If you want to modify a threshold setting, it might be necessary to click 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 19-1 by clicking in the field that you want to modify. In some fields, you can choose an option from a drop-down list; in others you can type a value.

Table 19-13 Optical Port Line Settings

Parameter	Description	Options
Port #	(Display only) Port number.	• 1-1 (OC-3; OC-12;OC-48 [MA only]) • 2-1 (OC3; OC-12; OC-48 [MA only])
Port Name	Provides the ability to assign the specified port a name.	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See the "DLP-C56 Assign a Name to a Port" task on page 17-75.
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 19-13 Optical Port Line Settings (continued)

Parameter	Description	Options
Service State	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 (default) • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 (default) • 1E-8 • 1E-9
Provides Synch	(Display only) If checked, the card is provisioned as a NE timing reference.	• Yes (checked) • No (unchecked)
SyncMsgIn	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.	• Yes (checked, default) • No (unchecked)
Admin SSM	Allows you to override the synchronization traceability unknown (STU) value (default setting).	• 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

Table 19-13 Optical Port Line Settings (continued)

Parameter	Description	Options
Send <FF> DoNotUse	When checked, sends a special DUS (0xff) message on the S1 byte.	• Yes • No
Send DoNotUse	When checked, sends a DUS message on the S1 byte.	• Yes (checked) • No (unchecked, default)
PJSTSMon #	Sets the STS that will be used for pointer justification. If set to 0 (available for the ONS 15310-CL) or OFF (available for the ONS 15310-MA), no STS is monitored. Only one STS can be monitored on each OC-N port.	• 0 or OFF (no STS used) • 1 – 12 (OC-12) • 1 – 48 (OC-48)
AINS Soak	Automatic in-service soak.	• Duration of valid input signal in hh.mm after which the card is set in service by the software • 0 to 48 hours, 15-minute increments
Type	Defines the port as SONET or SDH (15310-MA only).	• SONET • SDH
ALS Mode	Allows you to provision automatic laser shutdown	• Disable: ALS is off; the laser is not automatically shut down when traffic outages (LOS) occur. • Auto Restart: ALS is on; the laser automatically shuts down when traffic outages (LOS) occur. It automatically restarts when the conditions that caused the outage are resolved. • Manual Restart: ALS is on; the laser automatically shuts down when traffic outages (LOS) occur. However, the laser must be manually restarted when conditions that caused the outage are resolved. • Manual Restart for Test: Manually restarts the laser for testing.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

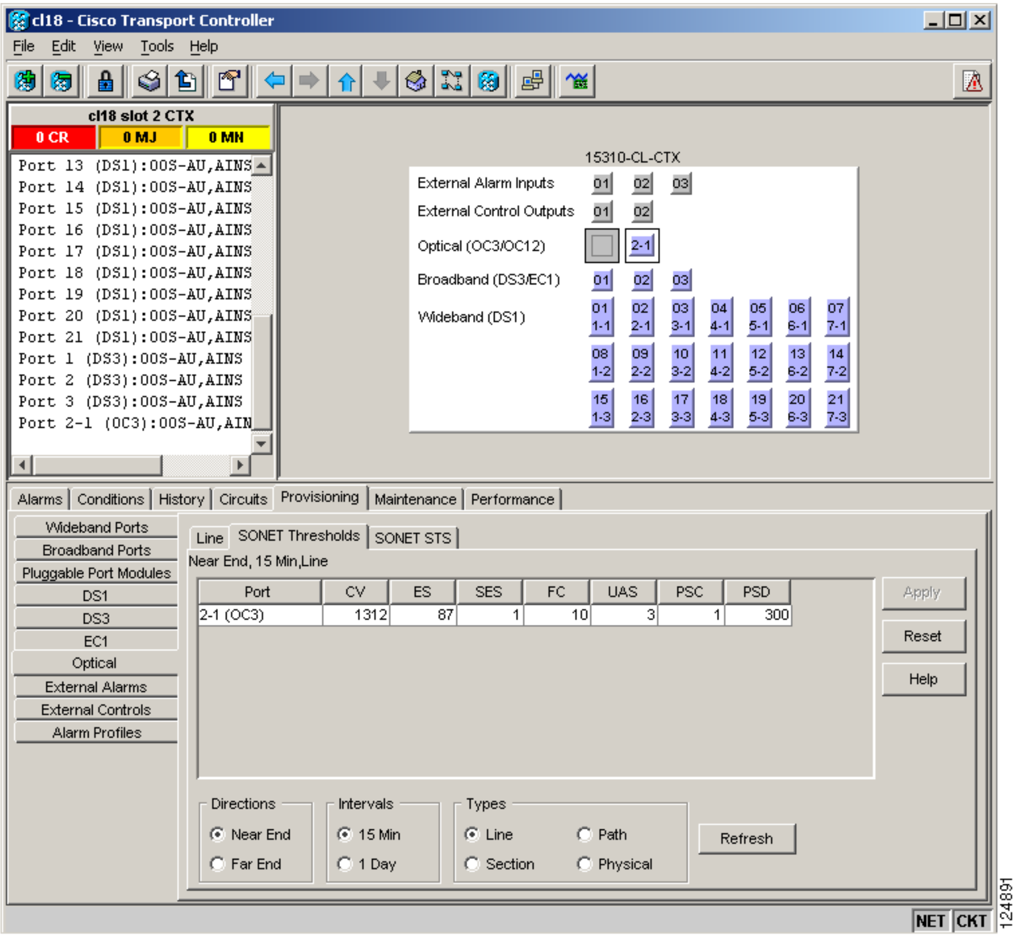
DLP-C239 Change Optical Port SONET Thresholds Settings

Purpose	This task changes SONET thresholds settings for ONS 15310-CL or ONS 15310-MA optical ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the 15310-CL-CTX card or the CTX2500 card.

Step 2 Click the **Provisioning > Optical > SONET Thresholds** tabs (Figure 19-6 and Figure 19-7).

Figure 19-6 Provisioning SONET Thresholds for the ONS 15310-CL Optical Ports



cl18 - Cisco Transport Controller

cl18 slot 2 CTX — 0 CR | 0 MJ | 0 MN

```
Port 13 (DS1):OOS-AU,AINS
Port 14 (DS1):OOS-AU,AINS
Port 15 (DS1):OOS-AU,AINS
Port 16 (DS1):OOS-AU,AINS
Port 17 (DS1):OOS-AU,AINS
Port 18 (DS1):OOS-AU,AINS
Port 19 (DS1):OOS-AU,AINS
Port 20 (DS1):OOS-AU,AINS
Port 21 (DS1):OOS-AU,AINS
Port 1 (DS3):OOS-AU,AINS
Port 2 (DS3):OOS-AU,AINS
Port 3 (DS3):OOS-AU,AINS
Port 2-1 (OC3):OOS-AU,AIN
```

Near End, 15 Min,Line

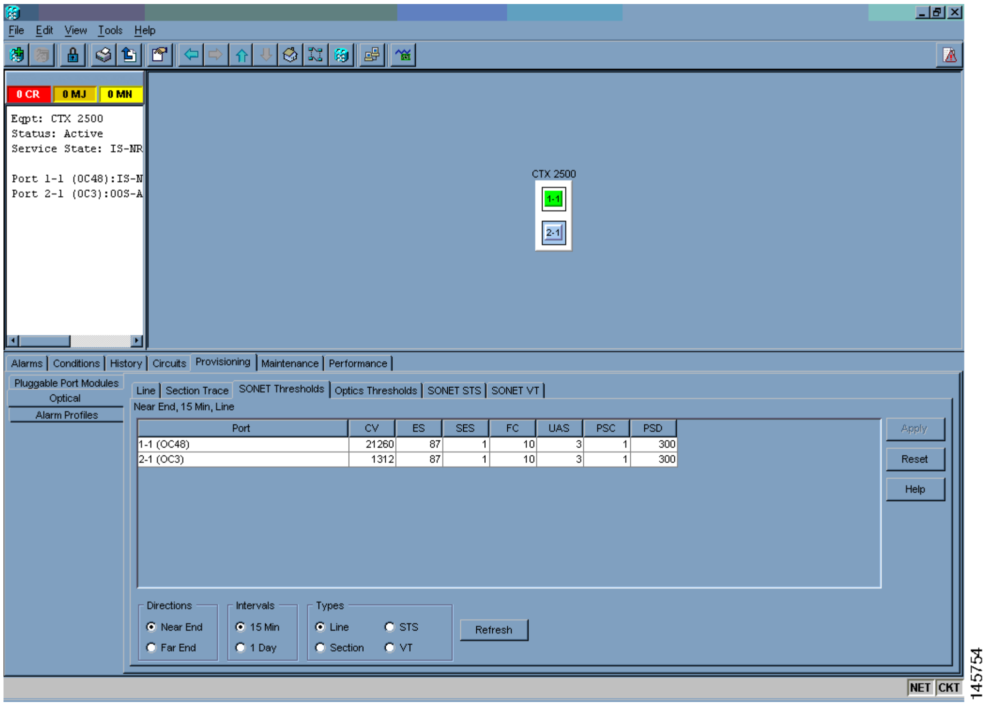
Port	CV	ES	SES	FC	UAS	PSC	PSD
2-1 (OC3)	1312	87	1	10	3	1	300

Directions: ● Near End ○ Far End

Intervals: ● 15 Min ○ 1 Day

Types: ● Line ○ Path ○ Section ○ Physical

Figure 19-7 Provisioning SONET Thresholds for the ONS 15310-MA Optical Ports



Eqpt: CTX 2500
Status: Active
Service State: IS-NR

Port 1-1 (OC48):IS-N
Port 2-1 (OC3):OOS-A

Near End, 15 Min, Line

Port	CV	ES	SES	FC	UAS	PSC	PSD
1-1 (OC48)	21260	87	1	10	3	1	300
2-1 (OC3)	1312	87	1	10	3	1	300

Directions: ● Near End ○ Far End

Intervals: ● 15 Min ○ 1 Day

Types: ● Line ○ STS ○ Section ○ VT

Note If you want to modify a threshold setting, it might be necessary to click 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 19-14 by clicking in the field that you want to modify. In some fields, you can choose an option from a drop-down list; in others you can type a value.

Table 19-14 Optical Port SONET Thresholds Options

Parameter	Description
Port	Port number • 1-1 (OC-3 or OC-12 for the ONS 15310-CL; OC-3, OC-12, or OC-48 for the ONS 15310-MA) • 2-1 (OC-3 or OC-12 for the ONS 15310-CL; OC-3, OC-12, or OC-48 for the OS 15310-MA)
CV	Coding violations. Available for Line, Section, or Path (Near and Far End).
ES	Errored seconds. Available for Line, Section, or Path (Near and Far End).
FC	Failure count. Available for Line and Path (Near End or Far End).
SES	Severely errored seconds. Available for Line, Section, and Path (Near End and Far End).
UAS	Unavailable seconds. Available for Line and Path (Near End and Far End).
PPJC-PDET	Positive Pointer Justification Count, STS Path Detected. Available for Line (Near End and Far End).

Table 19-14 Optical Port SONET Thresholds Options (continued)

Parameter	Description
NPJC-PDET	Negative Pointer Justification Count, STS Path Detected. Available for Line (Near End and Far End).
PPJC-PGEN	Positive Pointer Justification Count, STS Path Generated. Available for Line (Near End and Far End).
NPJC-PGEN	Negative Pointer Justification Count, STS Path Generated. Available for Line (Near End and Far End).
PJCDIFF	Pointer Justification Count Difference is the absolute value of the difference between the total number of detected pointer justification counts and the total number of generated pointer justification counts. That is, PJCDiff is equal to (PPJC-PGEN - NPJC-PGEN) – (PPJC-PDET – NPJC-PDET). Available for Path (Near End and Far End).
PJCS-PDET	Pointer Justification Count Seconds, STS Path Detected (PJCS-PDET) is a count of the one-second intervals containing one or more PPJC-PDET or NPJC-PDET. Available for Path (Near End and Far End).
PJCS-PGEN	Pointer Justification Count Seconds, STS Path Generated (PJCS-PGEN) is a count of the one-second intervals containing one or more PPJC-PGEN or NPJC-PGEN. Available for Path (Near End and Far End).
PSC	Protection Switching Count (Line). Available for Line (Near End and Far End).
PSD	Protection Switching Duration (Line). Available for Line (Near End and Far End).
PSC-W	Protection Switching Count, Working Line. Available for Line (Near End and Far End). **Note** BLSRs are not supported on the ONS 15310-CL (although the ONS 15310-CL can be part of a network that contains BLSRs); therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.
PSD-W	Protection Switching Duration, Working Line. Available for Line (Near End and Far End). **Note** BLSRs are not supported on the ONS 15310-CL (although the ONS 15310-CL can be part of a network that contains BLSRs); therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-C241 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-C31 Provision Path Protection Nodes, page 5-10 DLP-C29 Log into CTC, page 17-44
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-C242 Create a 1+1 Protection Group for the ONS 15310-MA

Purpose	This task creates a 1+1 protection group for ONS 15310-MA optical ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-C130 Manage Pluggable Port Modules, page 10-3 (optional)
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node where you want to create the protection group. If you are already logged in, continue with Step 2.

Step 2 Verify that pluggable port modules (PPM) are provisioned for the same port and port rate on the CTX2500 where you will create the optical protection group.

Note PPMs are referred to as small-form factor pluggables (SFPs) in the hardware chapters.

You can use either of the following methods:

- In node view, move your mouse over the CTX2500 client port. If a PPM is provisioned, two dots appear in the port graphic, and the port and PPM port and rate appear when you move the mouse over the port.
- Display the CTX2500 in card view. Click the **Provisioning > Pluggable Port Module** tabs. Verify that a PPM is provisioned in the Pluggable Port Module area, and the port type and rate is provisioned for it in the Selected PPM area.

The PPM port and port rate must be the same for both CTX2500 ports. As necessary, complete the "NTP-C130 Manage Pluggable Port Modules" procedure on page 10-3 to make PPM changes.

Step 3 From 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** from the drop-down list.
- Protect Port—Choose the protect port from the drop-down list. The menu displays the available optical ports on the CTX2500.
- After you choose the protect port, a list of ports available for protection is displayed under Available Ports.

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 the port to the Working Ports list.

Step 7 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 it 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 port after failure conditions stay corrected for the amount of time entered in the Reversion Time field.
- 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. Reversion time is the amount of time that will elapse before the traffic reverts to the working port. The reversion timer starts after conditions causing the switch are cleared.

Step 8 Click **OK**.

Step 9 Return to your originating procedure (NTP).

DLP-C243 Create an Optimized 1+1 Protection Group for the ONS 15310-MA

Purpose	This task creates an optimized 1+1 protection group for ONS 15310-MA optical ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-C130 Manage Pluggable Port Modules, page 10-3 (optional)
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 Complete the "DLP-C29 Log into CTC" task on page 17-44 at the node where you want to create the protection group. If you are already logged in, continue with Step 2.

Step 2 Verify that pluggable port modules (PPM) are provisioned for the same port and port rate on the CTX2500 where you will create the optical protection group.

Note PPMs are referred to as small-form factor pluggables (SFPs) in the hardware chapters.

You can use either of the following methods:

- In node view, move your mouse over the CTX2500 client port. If a PPM is provisioned, two dots appear in the port graphic, and the port and PPM port and rate appear when you move the mouse over the port.
- Display the CTX2500 in card view. Click the **Provisioning > Pluggable Port Module** tabs. Verify that a PPM is provisioned in the Pluggable Port Module area, and the port type and rate is provisioned for it in the Selected PPM area.

The PPM port and port rate must be the same for both CTX2500 ports. As necessary, complete the "NTP-C130 Manage Pluggable Port Modules" procedure on page 10-3 to make PPM changes.

Step 3 Change the port type from SONET to SDH for each applicable port where you want to provision a 1+1 optimized protection group:

a. In node view, double-click the applicable CTX2500.

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 4 In node view, click the **Provisioning** > **Protection** tabs.

Step 5 In the Protection Groups area, click **Create**.

Step 6 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 optical ports. If the CTX2500s are not provisioned for SDH, no ports appear in the drop-down list.

Step 7 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 8 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 1 second. 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 alarm indication signal–line (AIS-L) failure. Detection guard time is the amount of time elapsed before a traffic switch is initiated to a standby port after the detection of an SD, SF, LOS, LOF, or AIS-L failure on the active port.

Step 9 Click **OK**.

Step 10 Return to your originating procedure (NTP).

DLP-C244 Modify an Optimized 1+1 Protection Group for the ONS 15310-MA

Purpose	This task modifies an optimized 1+1 protection group for ONS 15310-MA optical ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-C243 Create an Optimized 1+1 Protection Group for the ONS 15310-MA, page 19-55 DLP-C29 Log into CTC, page 17-44
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 1 second. 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 port after the detection of an SD, SF, LOS, LOF, or AIS-L failure on the active port.

Step 4 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-C245 Modify a 1:1 Protection Group for the ONS 15310-MA

Purpose	This task modifies a 1:1 protection group for electrical (DS1-28/DS3-EC1-3 or DS1-84/DS3-EC1-3) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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**.

Step 5 Return to your originating procedure (NTP).

DLP-C248 Mount a Single ONS 15310-MA in a Rack

Purpose	This task allows one person to mount the MA shelf assembly in a rack.
Tools/Equipment	#12-24 mounting screws (4) #10-32 ear mounting screws (8) #2 Phillips screwdriver Universal mounting ear 19-inch-rack mounting ear 23-inch-rack mounting ear Fuse and alarm panel, if not installed
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Mounting the ONS 15310-MA in a rack requires a minimum of 10.5 inches of vertical rack space, including the space needed for the standard cable management bracket. If the extended cable management bracket is used, 12.25 inches is required.

Note To install the shelf assembly justified right, secure the universal mounting ear to the right side of the shelf assembly and the appropriate mounting ear for your rack size (19-inch or 23-inch) on the left side. To install the shelf assembly justified left, secure the universal mounting ear to the left side of the shelf assembly and the appropriate mounting ear for your rack size on the right side.

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 instructions. A fuse panel with two fuses per shelf (amperage depends on the fuse and alarm panel you are using) is required for Power A and B feeds.

Caution Maximum amperage rating of the fuse is determined by the rated ampacity of the selected power cable (refer to manufacturer’s instructions). The fuse rating should not exceed 20 A.

Step 2 Align the screw holes on the desired mounting ear with the screw holes at the front of the shelf assembly, and install four #10-32 screws.

Step 3 Repeat Step 2 for the other mounting ear.

Step 4 Lift the shelf assembly to the desired rack position.

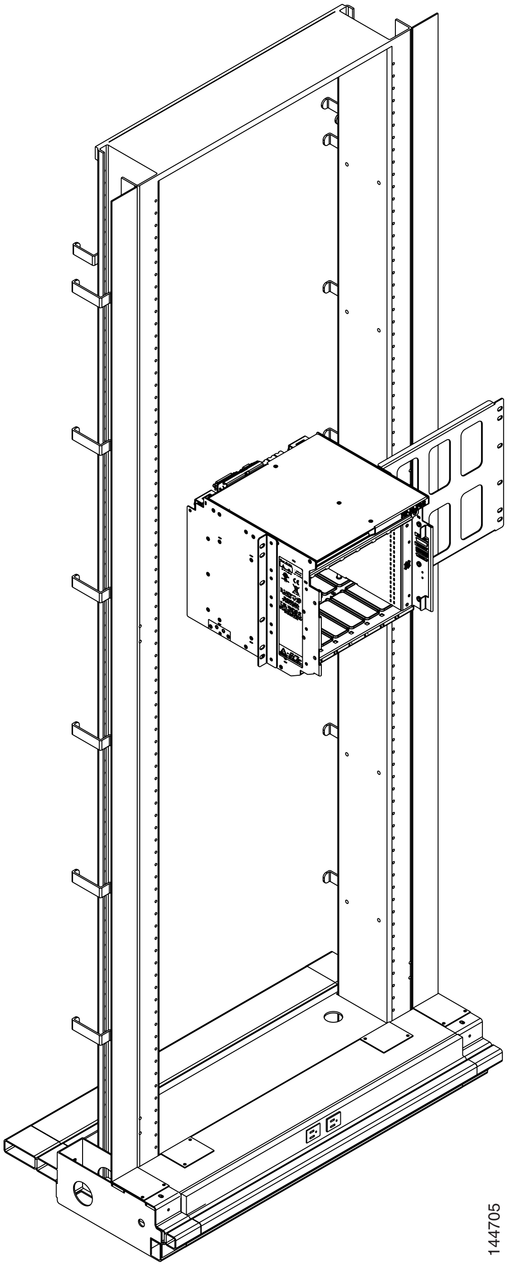
Step 5 Align the screw holes on the mounting ears with the mounting holes in the rack.

Step 6 Using the Phillips screwdriver, install one #12-24 mounting screws in each side of the assembly.

Step 7 When the shelf assembly is secured to the rack, install the remaining two mounting screws through the rack into the shelf assembly.

Figure 19-8 shows a single ONS 15310-MA being mounted in a rack.

Figure 19-8 Mounting a Single, Left-Justified ONS 15310-MA in a Rack



Note If you want to install a tie-down bar on the rack, be sure to leave 1 RU spacing between the ONS 15310-MA and any adjacent equipment you plan to install on the rack. This will provide adequate space for the tie-down bar and cabling.

Step 8 Return to your originating procedure (NTP).

DLP-C249 Mount Dual ONS 15310-MA Shelf Assemblies in a Rack

Purpose	This task simultaneously installs two shelf assemblies in a rack.
Tools/Equipment	#2 Phillips screwdriver #12-24 mounting screws (4) #10-32x0.31 length screws (7) #10-32x0.375 length ear mounting screws (9) #10-32 nut (1) Universal mounting ears (2) Dual-assembly plate
Prerequisite Procedures	None
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 is not present, you must install one according to manufacturer instructions. A fuse panel with two fuses per shelf (amperage depends on the fuse and alarm panel you are using) is required for Power A and B feeds.

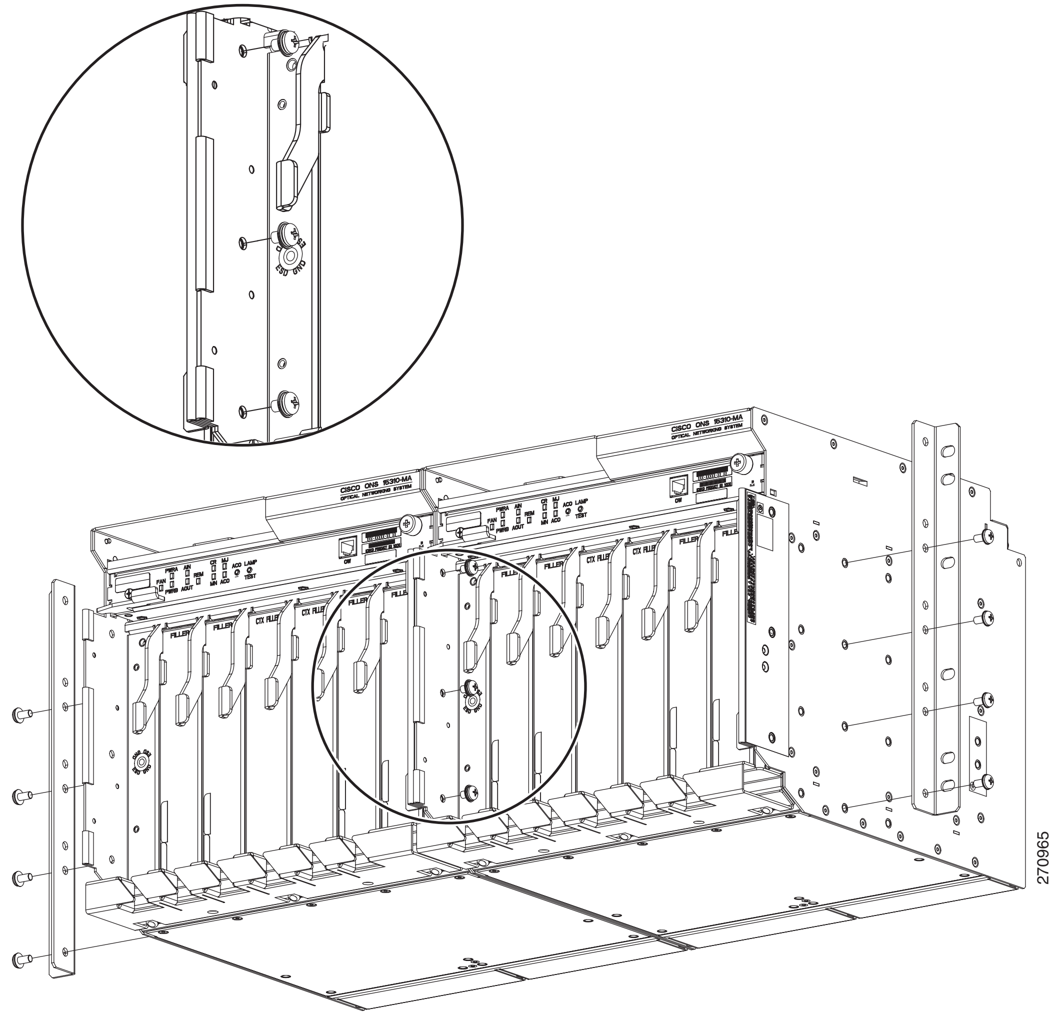
Caution Maximum amperage rating of the fuse is determined by the rated ampacity of the selected power cable (refer to manufacturer's instructions). The fuse rating should not exceed 20 A.

Step 2 Align the screw holes on a universal mounting ear with the screw holes at the left front of the shelf assembly, and install four #10-32x0.375 screws.

Step 3 Align the screw holes on a universal mounting ear with the screw holes at the right front of the other shelf assembly, and install four #10-32x0.375 screws.

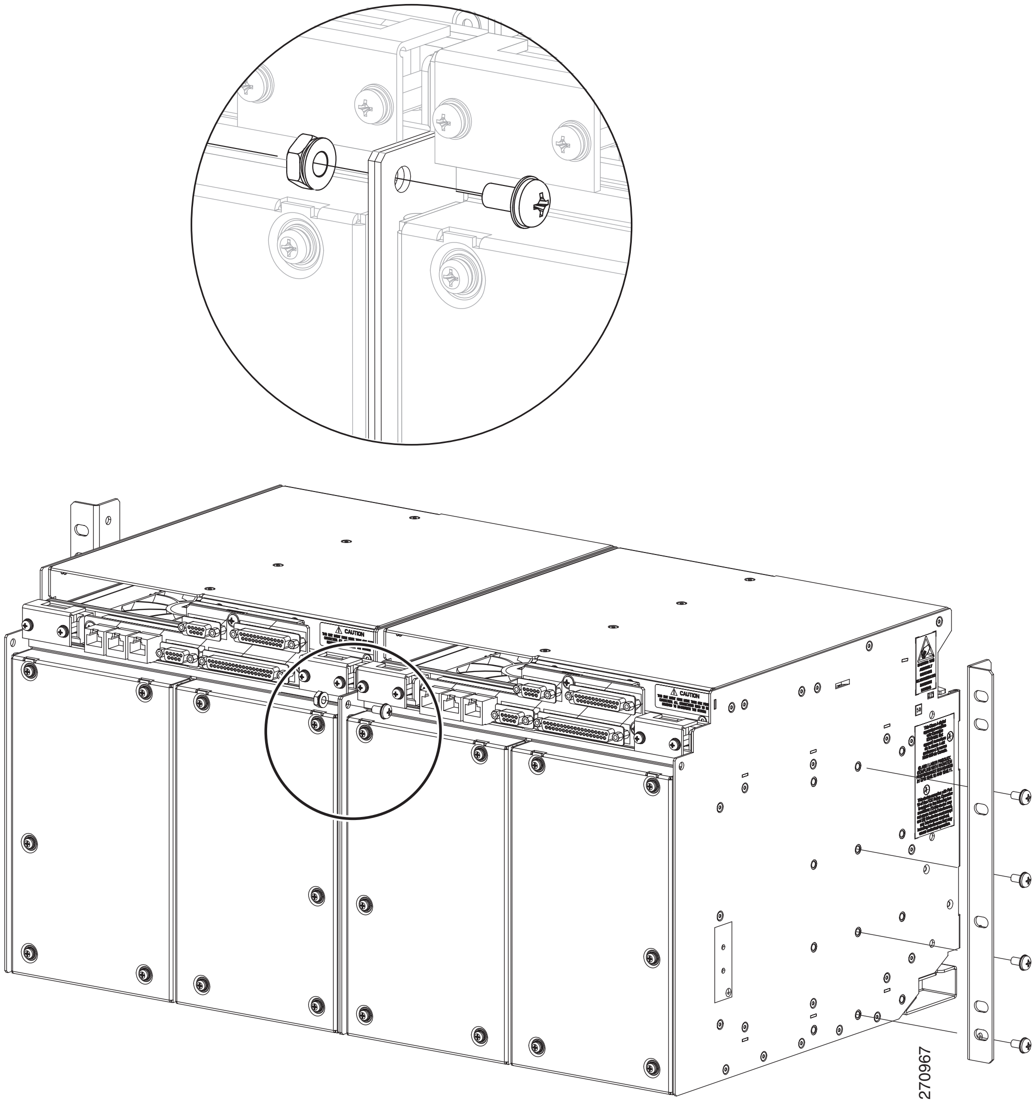
Step 4 Align the two shelves on the front, common lateral side. Using the Phillips screwdriver, install three mounting screws; #10-32x0.31 length. Figure 19-9 shows the two shelves aligned along a common lateral side.

Figure 19-9 ONS 15310-MA Shelves Aligned along a Common Lateral Side



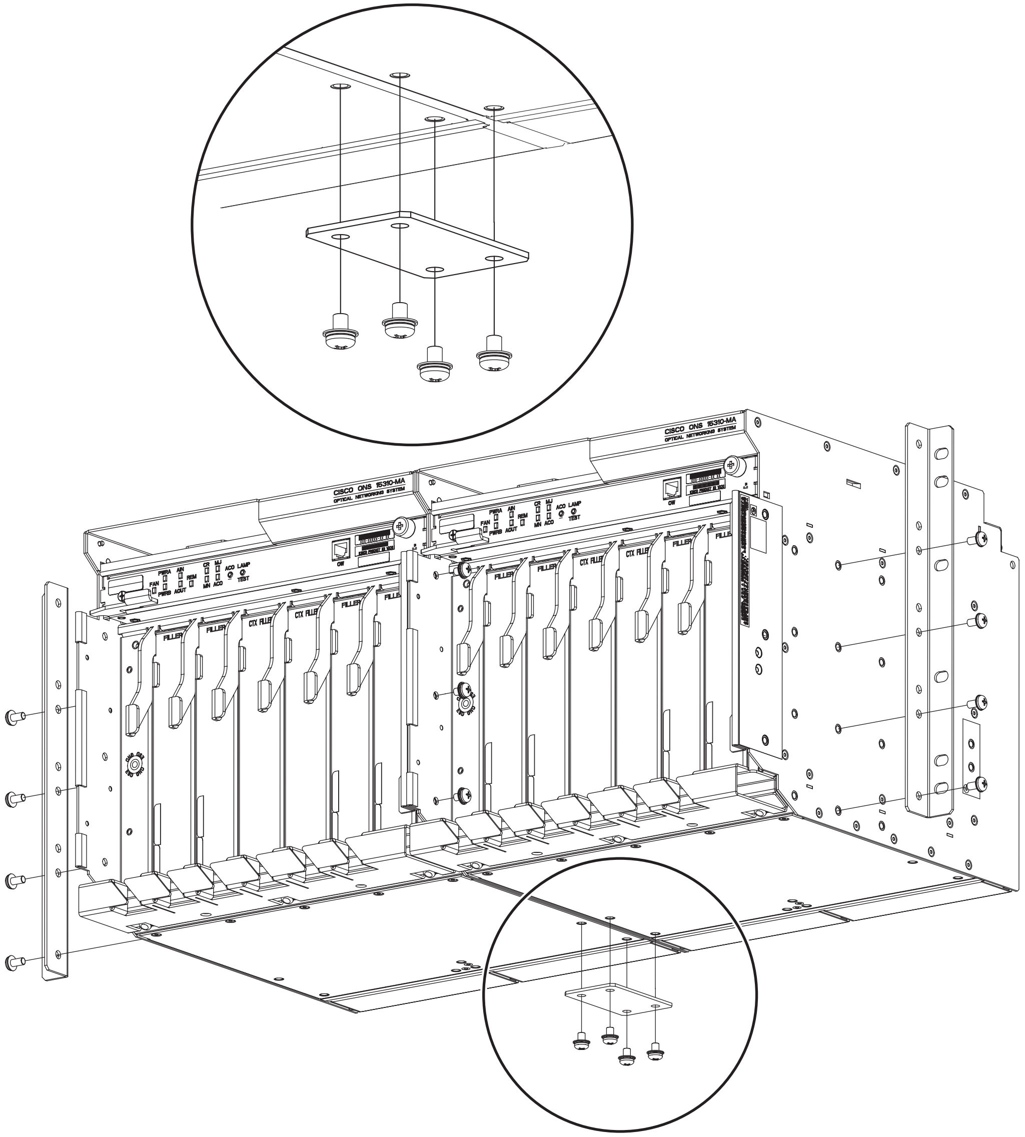
Step 5 Install screws #10-32x0.375 length with its #10-32 nut on the rear common lateral side as shown in Figure 19-10.

Figure 19-10 ONS 15310-MA Shelves Aligned on the Rear Common Lateral Side



Step 6 Install the dual-assembly plate at the bottom of the shelf assembly by aligning it with four screws #10-32x0.31 length as shown in Figure 19-11.

Figure 19-11 Dual-Assembly Plate aligned to the ONS 15310-MA Shelf



Step 7 Lift the dual-shelf assembly to the desired rack position.

Step 8 Align the screw holes on the mounting ears with the mounting holes in the rack.

Step 9 Using the Phillips screwdriver, install one #12-24 mounting screws in each side of the assembly.

Step 10 When the shelf assembly is secured to the rack, install the remaining two mounting screws through the rack into the shelf assembly.

Note If you want to install a tie-down bar on the rack, be sure to leave 1 RU spacing between the ONS 15310-MA and any adjacent equipment you plan to install on the rack. This will provide adequate space for the tie-down bar and cabling.

Step 11 Repeat the task with the remaining ONS 15310-MA nodes.

Step 12 Return to your originating procedure (NTP).

DLP-C250 Connect the Office Ground to the ONS 15310-MA

Purpose	This task connects ground to the ONS 15310-MA shelf.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Screws Ground cable, #6 AWG, copper conductors, 194°F [90°C]) #6 AWG dual-hole, 5/8-in. (1.59-cm) spaced grounding lug 10-32 screws Crimp tool Wire strippers Wire cutter
Prerequisite Procedures	DLP-C248 Mount a Single ONS 15310-MA in a Rack, page 19-58
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify that the office ground cable (#6 AWG stranded) is connected to the top of the rack according to local site practice.

Note Additional ground cables may be added depending on the local site practice. The ONS 15310-MA is designated for a Common Bonding Network (CBN) only, according to definitions in section 9.3 of GR1089 issue 4.

Step 2 Ensure to remove paint and other nonconductive coatings from the surfaces between the shelf ground and the rack frame ground posts. Clean the mating surfaces and apply an appropriate antioxidant compound to the bare conductors.

Step 3 Locate the ground connection points, which are located on left, right, and bottom of the ONS 15310-MA shelf assembly.

Figure 19-12 and Figure 19-13 show the ground locations on the ONS 15310-MA.

Figure 19-12 Ground Holes on the Bottom of the ONS 15310-MA Shelf Assembly

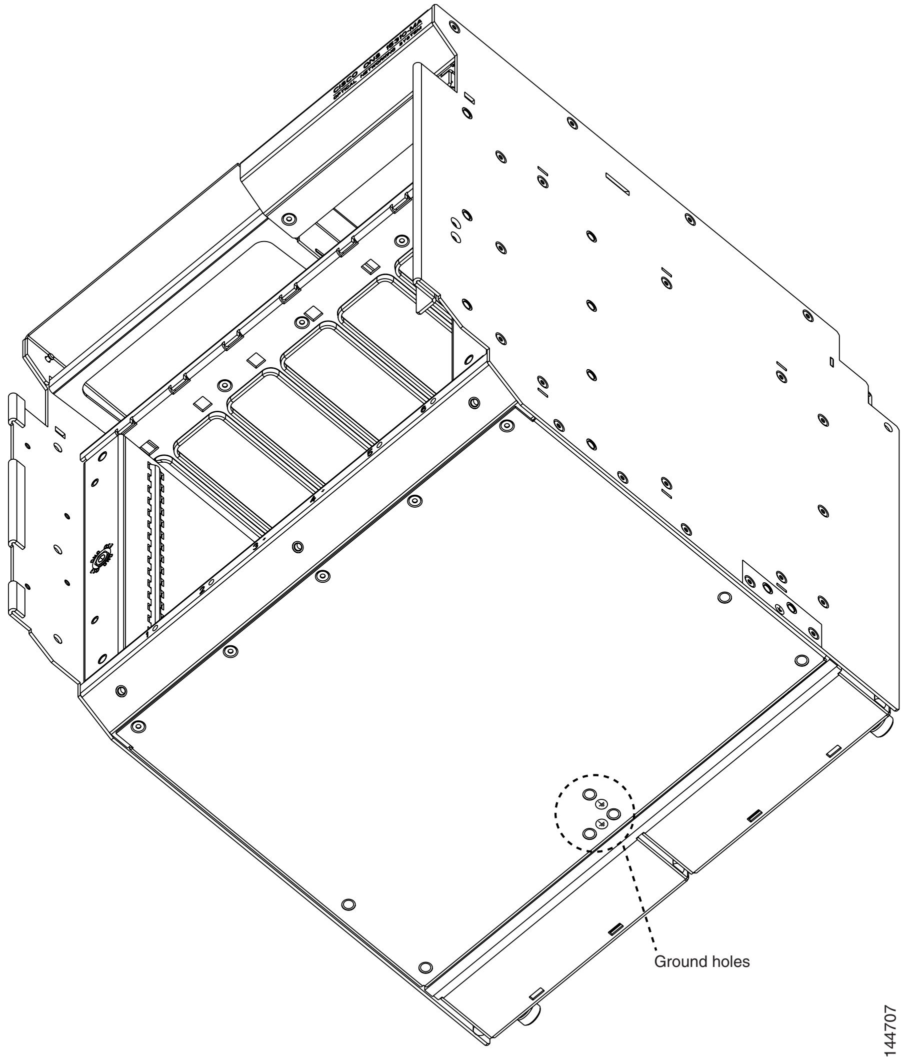
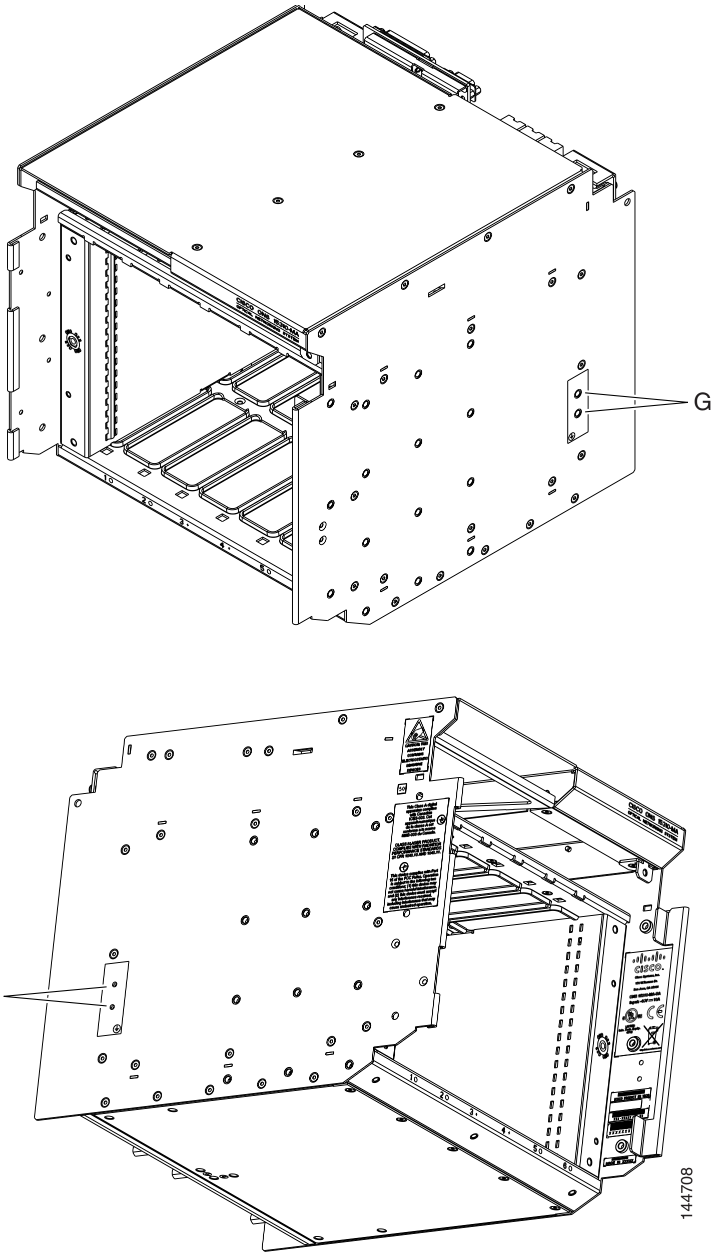


Figure 19-13 Ground Holes on the Left and Right Sides of the ONS 15310-MA Shelf Assembly



Step 4 Using a wire stripper, strip 0.875 in. (2.22 cm) from the end of a #6 AWG ground cable.

Step 5 Crimp the two-hole lug to the #6 AWG ground cable.

Step 6 Line up the holes on the lug with the holes on the ground connection point. Use two 10-32 screws to attach the lug to the ground connection point.

Step 7 Attach the other end of the shelf ground cable to the rack.

Step 8 Return to your originating procedure (NTP).

DLP-C251 Connect Office Power to the ONS 15310-MA

Purpose	This task connects office power to the ONS 15310-MA shelf.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Wire wrapper Wire cutters Wire strippers Fuse and alarm panel Power cable (from fuse and alarm panel to assembly), #12 AWG, stranded (41 strands, 0.010 in. [0.025 cm]) Listed pressure terminal connectors such as ring and fork types; 12 AWG, stranded (41 strands, 0.010 in. [0.025 cm])
Prerequisite Procedures	DLP-C250 Connect the Office Ground to the ONS 15310-MA, page 19-65
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note If you encounter problems with the power supply, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA 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 15310-MA from the fuse panel.

Step 3 Dress the power cabling according to local site practice.

Step 4 Remove or loosen the power terminal screws on the ONS 15310-MA. 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.

Note The battery return connection (+48Vdc) can be treated as DC-I , as defined in Telcordia GR-1089-CORE Issue 4. Connect the battery return (+48Vdc) to ground at the power source level.

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.

Note 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 away 0.2 in. of insulation at one end of two 12 AWG wires.

Step 6 Crimp the lugs onto the ends of all power leads.

Step 7 Using a Phillips screwdriver, remove the two screws that hold the plastic covers over the A and B power terminal strips. (There are two screws on each for A and B power.)

Step 8 Terminate the return 1 lead to the RET1 backplane terminal. Use oxidation-prevention grease to keep connections noncorrosive.

Step 9 Terminate the negative 1 lead to the negative BAT1 backplane power terminal. Use oxidation prevention grease to keep connections noncorrosive.

Step 10 If you use redundant power leads, terminate the return 2 lead to the positive RET2 terminal on the ONS 15310-MA. Terminate the negative 2 lead to the negative BAT2 terminal on the ONS 15310-MA. Use oxidation-preventative grease to keep connections noncorrosive.

Step 11 Replace and tighten the screws that hold the plastic covers over the A and B power terminal strips.

Step 12 Return to your originating procedure (NTP).

DLP-C252 Turn On and Verify Office Power to the ONS 15310-MA

Purpose	This task verifies the chassis LED activity and measures the DC power to verify correct power and returns.
Tools/Equipment	Voltmeter
Prerequisite Procedures	DLP-C250 Connect the Office Ground to the ONS 15310-MA, page 19-65
	DLP-C251 Connect Office Power to the ONS 15310-MA, page 19-68
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 -44 VDC and -52 VDC. Place the red test lead on the B-side connection and verify that it is between -44 VDC and -52 VDC.

Note The voltages -44 VDC and -52 VDC are the minimum and maximum voltages required to power the chassis. The nominal steady-state voltage is -48 VDC.

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. Place the red test lead on the B-side return ground and verify that no voltage is present.

Step 2 According to site practice, insert a fuse into the fuse position.

Step 3 Using a voltmeter, verify the shelf for –48 VDC battery and ground:

a. To verify the A-side of the shelf, place the black lead of the voltmeter to the frame ground. Place the red test lead to the BAT1 (A-side battery connection) red cable. Verify that it reads between –44 VDC and –52 VDC. Then place the red test lead of the voltmeter to the RET1 (A-side return ground) black cable and verify that no voltage is present.

b. To verify the B-side of the shelf, place the black test lead of the voltmeter to the frame ground. Place the red test lead to the BAT2 (B-side battery connection) red cable. Verify that it reads between –44 VDC and –52 VDC. Then place the red test lead of the voltmeter to the RET2 (B-side return ground) black cable and verify that no voltage is present.

Step 4 Return to your originating procedure (NTP).

DLP-C253 Install External Alarm Cables on the ONS 15310-MA

Purpose	This task installs alarm cables on the ONS 15310-MA so that you can provision external (environmental) alarms and controls.
Tools/Equipment	Alarm In cable, unshielded cable terminated with a DB-37 connector Alarm Out cable, unshielded cable terminated with a DB-25 connector
Prerequisite Procedures	NTP-C150 Install the Shelf Assembly, page 2-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the alarm cable terminated with a DB-37 connector into the ALARM IN port at the rear of the ONS 15310-MA.

Step 2 Plug the other end of the cable into the alarm-collection equipment according to local site practice.

Step 3 Plug one end of the alarm cable terminated with a DB-25 connector into the ALARM OUT port at the rear of the ONS 15310-MA.

Step 4 Plug the other end of the cable into the alarm-collection equipment according to local site practice.

Step 5 To define the 32 external alarm inputs and 8 external alarm outputs using CTC, see the "NTP-C63 Provision External Alarms and Controls" procedure on page 9-8. Table 19-15 shows the default input alarm pinouts and the corresponding alarm numbers assigned to each port. Table 19-16 shows the default output alarm pinouts and the corresponding alarm numbers assigned to each port. Refer to these tables when connecting alarm cables to the ONS 15310-MA.

Table 19-15 Default Alarm Pin Assignments—Inputs

DB-37 Pin Number	Function	DB-37 Pin Number	Function
1	Alarm 1	20	Alarm 18
2	Alarm 2	21	Alarm 19
3	Alarm 3	22	Alarm 20
4	Alarm 4	23	Alarm 21
5	Alarm 5	24	Alarm 22
6	Alarm 6	25	Alarm 23
7	Alarm 7	26	Alarm 24
8	Alarm 8	27	Common 17–24
9	Common 1–8	28	Alarm 25
10	Alarm 9	29	Alarm 26
11	Alarm 10	30	Alarm 27
12	Alarm 11	31	Alarm 28
13	Alarm 12	32	Alarm 29
14	Alarm 13	33	Alarm 30
15	Alarm 14	34	Alarm 31
16	Alarm 15	35	Alarm 32
17	Alarm 16	36	Common 25–32
18	Common 9–16	37	N/C
19	Alarm 17	—	—

Table 19-16 Default Alarm Pin Assignments—Outputs

DB-25 Pin Number	Function	DB-25 Pin Number	Function
1	Out 1+	14	Out 2+
2	Out 1–	15	Out 2–
3	—	16	Out 3+
4	—	17	Out 3–
5	—	18	Out 4+
6	—	19	Out 4–
7	—	20	Out 5+
8	—	21	Out 5–
9	—	22	Out 6+
10	—	23	Out 6–
11	—	24	Out 7+
12	Out 8+	25	Out 7–
13	Out 8–	—	—

Step 6 Return to your originating procedure (NTP).

DLP-C254 Install Timing Cables on the ONS 15310-MA

Purpose	This task installs timing cables so that you can provide building integrated timing supply (BITS) timing to the ONS 15310-MA.
Tools/Equipment	BITS timing port cable, CAT-3/CAT-5 terminated with DB-9 connector
Prerequisite Procedures	NTP-C150 Install the Shelf Assembly, page 2-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the timing cable into the BITS 1 port at the rear of the ONS 15310-MA.

Step 2 Plug the other end of the cable into the BITS clock according to local site practice. Table 19-17 shows the BITS cable pin assignments.

Table 19-17 BITS Cable Pin Assignments

DSub-9 Pin Number	Function
1	BITS Output+
2	BITS Output–
3	—
4	—
5	—
6	BITS Input+
7	BITS Input–
8	—
9	—

Step 3 Repeat Steps 1 and 2 for the BITS 2 port.

Note For more detailed information about timing, refer to the “Timing” chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*. To set up system timing, see the “NTP-C23 Set Up Timing” procedure on page 4-11.

Step 4 Return to your originating procedure (NTP).

DLP-C255 Install the Serial Cable for TL1 Craft Interface on the ONS 15310-MA

Purpose	This task installs the serial cable for the TL1 craft interface on the ONS 15310-MA.
Tools/Equipment	Craft port serial cable, CAT-5 terminated with RJ-45
Prerequisite Procedures	NTP-C150 Install the Shelf Assembly, page 2-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the TL1 cable into the CRAFT port on the CTX2500 faceplate.

Step 2 Connect the other end to the PC that you want to use to access the craft.

Table 19-18 shows the serial cable pin assignments.

Table 19-18 TL1 Serial Cable Pin Assignments

RJ-45 Pin Number	Function
1	RTS
2	DTR
3	TXD
4	GND
5	GND
6	RXD
7	DSR
8	CTS

Step 3 Return to your originating procedure (NTP).

DLP-C256 Install the UDC Cable on the ONS 15310-MA

Purpose	This task installs the user data channel (UDC) cable on the ONS 15310-MA. A UDC circuit allows you to create a dedicated data channel between nodes.
Tools/Equipment	EIA/TIA-232 port cable, CAT-5 terminated with RJ-45
Prerequisite Procedures	NTP-C150 Install the Shelf Assembly, page 2-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the UDC cable into the UDC port at the rear of the 15310-MA.

Step 2 Connect the other end to terminating equipment, such as a 64-Kbps codirectional ITU-T G.703 equipment interface or EIA/TIA-232-compliant equipment.

Table 19-19 shows the serial cable pin assignments.

Table 19-19 UDC Cable Pin Assignments

RJ-45 Pin Number	RS-232/64K Mode
1	TX +
2	TX –
3	RX +
4	—
5	—
6	RX –
7	—
8	—

Step 3 Return to your originating procedure (NTP).

DLP-C257 Install the LAN Cable for the CTC Interface on the ONS 15310-MA

Purpose	This task installs the LAN cable to provide a 10/100 Mbps Ethernet interface for CTC and TL1 provisioning.
Tools/Equipment	Management LAN cable, CAT-5 terminated with RJ-45
Prerequisite Procedures	NTP-C2 Install the Shelf Assembly, page 1-4
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the LAN cable into the LAN port on the CTX2500 faceplate.

Step 2 Connect the other end to the PC you want to use to access CTC.

Table 19-20 shows the LAN cable pin assignments.

Table 19-20 LAN Cable Pin Assignments

RJ-45 Pin Number	Function
1	TX +
2	TX –
3	RX +
4	—
5	—

Table 19-20 LAN Cable Pin Assignments (continued)

RJ-45 Pin Number	Function
6	RX –
7	—
8	—

Step 3 Return to your originating procedure (NTP).

DLP-C258 Install CHAMP Cables for DS-1 Connection

Purpose	This task installs DS-1 cables.
Tools/Equipment	Electrical cable, terminated with a 64-pin CHAMP connector
Prerequisite Procedures	NTP-C157 Install Wires to Alarm, Timing, Craft, LAN, and UDC Pin Connections, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

⚠ **Caution** Always use the supplied ESD wristband when working with a powered ONS 15310-MA. Plug the wristband cable into either of the ESD jacks, on the far left and right faceplates in the shelf.

Step 1 Prepare a cable terminated with a 64-pin CHAMP connector.

Table 19-21 lists the Champ connector pin assignments and the corresponding EIA connector mapping for connectors J8 and J9 on the EIA installed on the A side, and connectors J21 and J22 on the EIA installed on the B side.

Table 19-21 Champ Connector Pin Assignments—Side-A EIA, Connectors J8 and J9; Side-B EIA, Connectors J21 and J22

Signal	Pin	Signal	Pin
Ring Port 1	1	Tip Port 1	33
Ring Port 2	2	Tip Port 2	34
Ring Port 3	3	Tip Port 3	35
Ring Port 4	4	Tip Port 4	36
Ring Port 5	5	Tip Port 5	37
Ring Port 6	6	Tip Port 6	38
Ring Port 7	7	Tip Port 7	39
Ring Port 8	8	Tip Port 8	40
Ring Port 9	9	Tip Port 9	41
Ring Port 10	10	Tip Port 10	42

Table 19-21 Champ Connector Pin Assignments—Side-A EIA, Connectors J8 and J9; Side-B EIA, Connectors J21 and J22 (continued)

Signal	Pin	Signal	Pin
Ring Port 11	11	Tip Port 11	43
Ring Port 12	12	Tip Port 12	44
Ring Port 13	13	Tip Port 13	45
Ring Port 14	14	Tip Port 14	46
Ring Port 15	15	Tip Port 15	47
Ring Port 16	16	Tip Port 16	48
Ring Port 17	17	Tip Port 17	49
Ring Port 18	18	Tip Port 18	50
Ring Port 19	19	Tip Port 19	51
Ring Port 20	20	Tip Port 20	52
Ring Port 21	21	Tip Port 21	53
Ring Port 22	22	Tip Port 22	54
Ring Port 23	23	Tip Port 23	55
Ring Port 24	24	Tip Port 24	56
Ring Port 25	25	Tip Port 25	57
Ring Port 26	26	Tip Port 26	58
Ring Port 27	27	Tip Port 27	59
Ring Port 28	28	Tip Port 28	60
Unused	29	Unused	61
Unused	30	Unused	62
Unused	31	Unused	63
Unused	32	Unused	64

Table 19-22 lists the Champ connector pin assignments and the corresponding EIA connector mapping for connectors J10 and J11 on the EIA installed on the A side, and connectors J23 and J24 on the EIA installed on the B side.

Table 19-22 Champ Connector Pin Assignments—Side-A EIA, Connectors J10 and J11; Side-B EIA, Connectors J23 and J24

Signal	Pin	Signal	Pin
Ring Port 29	1	Tip Port 29	33
Ring Port 30	2	Tip Port 30	34
Ring Port 31	3	Tip Port 31	35
Ring Port 32	4	Tip Port 32	36
Ring Port 33	5	Tip Port 33	37
Ring Port 34	6	Tip Port 34	38
Ring Port 35	7	Tip Port 35	39

Table 19-22 Champ Connector Pin Assignments—Side-A EIA, Connectors J10 and J11; Side-B EIA, Connectors J23 and J24 (continued)

Signal	Pin	Signal	Pin
Ring Port 36	8	Tip Port 36	40
Ring Port 37	9	Tip Port 37	41
Ring Port 38	10	Tip Port 38	42
Ring Port 39	11	Tip Port 39	43
Ring Port 40	12	Tip Port 40	44
Ring Port 41	13	Tip Port 41	45
Ring Port 42	14	Tip Port 42	46
Ring Port 43	15	Tip Port 43	47
Ring Port 44	16	Tip Port 44	48
Ring Port 45	17	Tip Port 45	49
Ring Port 46	18	Tip Port 46	50
Ring Port 47	19	Tip Port 47	51
Ring Port 48	20	Tip Port 48	52
Ring Port 49	21	Tip Port 49	53
Ring Port 50	22	Tip Port 50	54
Ring Port 51	23	Tip Port 51	55
Ring Port 52	24	Tip Port 52	56
Ring Port 53	25	Tip Port 53	57
Ring Port 54	26	Tip Port 54	58
Ring Port 55	27	Tip Port 55	59
Ring Port 56	28	Tip Port 56	60
Unused	29	Unused	61
Unused	30	Unused	62
Unused	31	Unused	63
Unused	32	Unused	64

Note Refer to the "Shelf Assembly Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for specific information on DS-1 cables and DS-1 connectors, including product numbers and compatibility.

Step 2 Connect the male connector on the cable to the female connector on the electrical interface assembly (EIA) at the back of the ONS 15310-MA.

Step 3 Tighten the two thumbscrews on the male connector.

Step 4 Return to your originating procedure (NTP).

DLP-C259 Install DS-3/EC-1 Cables

Purpose	This task installs the DS-3/EC-1 cables to connect DS-3/EC-1 signals to the ONS 15310-MA.
Tools/Equipment	Shielded coaxial cable terminated with BNC connectors for DS-3/EC-1 ports BNC insertion/removal tool (see the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for information about obtaining the BNC insertion/removal tool)
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution Always use the supplied ESD wristband when working with a powered ONS 15310-MA. Plug the wristband cable into either of the ESD jacks, on the far left and right faceplates in the shelf.

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 notched 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 Return to your originating procedure (NTP).

DLP-C260 Route Cables

Purpose	This task routes electrical, optical, alarm, and timing cables away from the ONS 15310-MA. You can install optional tie-bars specifically designed for the ONS 15310-MA.
Tools/Equipment	Tie-wraps or other securing devices, according to local practice Tie-bar(s)
Prerequisite Procedures	NTP-C158 Install the Electrical Cables, page 2-24 NTP-C160 Install Optical Cables, page 2-28 NTP-C157 Install Wires to Alarm, Timing, Craft, LAN, and UDC Pin Connections, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 As needed, install a tie-bar or other strain-relief device, according to local site practice.

Caution You must provide some type of strain relief for the ONS 15310-MA cabling.

Step 2 Route the cables to the appropriate side of the shelf assembly according to local site practice.

Step 3 Secure the cables to the strain-relief device using tie-wraps or other site-specific methods.

Step 4 Label all cables at each end of the connection to avoid confusion with cables that are similar in appearance.

Step 5 Return to your originating procedure (NTP).

DLP-C264 Clear All PM Thresholds

Purpose	This task clears and resets all PM thresholds to default values.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
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** > **Thresholds** 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-C265 Set Up a Solaris Workstation for a Craft Connection to an ONS 15310-CL or ONS 15310-MA

Purpose	This task sets up a Solaris workstation for a craft connection to the ONS 15310-CL/ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
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 15310-CL/ONS 15310-MA 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 15310-CL/ONS 15310-MA 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-C29 Log into CTC" task on page 17-44 to complete the login. If the Login dialog box does not appear, complete Steps c and d.

c. At the prompt, type:

ping *ONS 15310-CL/ONS 15310-MA-IP-address*

or

For example, to connect to an ONS 15310-CL with a default IP address of 192.1.0.2, type:

ping 192.1.0.2

If your workstation is connected to the ONS 15310-CL/ONS 15310-MA, 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 fromx.x.x.x" (UNIX) message appears. Verify the IP and subnet mask information. Check that the cables connecting the workstation to the ONS 15310-CL/ONS 15310-MA 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: **# man ndd**.

Step 7 Return to your originating procedure (NTP).

DLP-C266 Install the CTC Launcher Application from a Release 8.5 Software CD

Purpose	This task installs the CTC Launcher from a Release 8.5 software CD.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
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 8.5 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-C267 Install the CTC Launcher Application from a Release 8.5 Node

Purpose	This task installs the CTC Launcher from an ONS 15310-CL or ONS 15310-MA node running Software R8.5.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
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 on the local hard drive.

Step 4 Click **Save**.

Step 5 Return to your originating procedure (NTP).

DLP-C268 Connect to ONS Nodes Using the CTC Launcher

Purpose	This task starts the CTC Launcher from an ONS node.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Start the CTC Launcher:

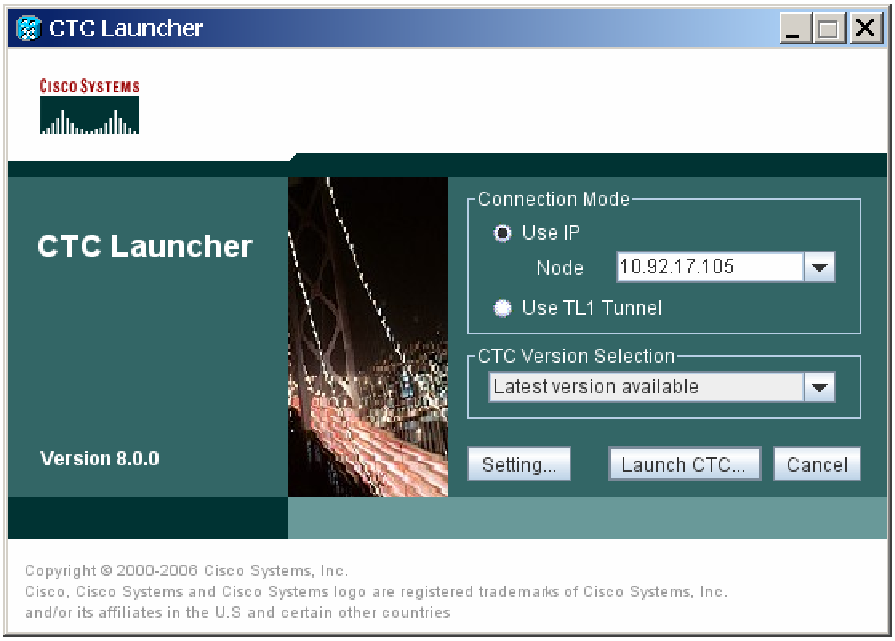
- Windows: navigate to the directory containing the StartCTC.exe file and double-click it. (You can also use the Windows Start menu Run command.)
- Solaris: assuming the StartCTC.exe file is accessible from the current shell path, navigate to the directory containing the CtcLauncher.jar file and type:

  % java -jar StartCTC.exe

Step 2 In the CTC Launcher dialog box, choose **Use IP**.

Figure 19-14 shows the CTC Launcher window.

Figure 19-14 CTC Launcher Window



Connection Mode

● Use IP

Node 10.92.17.105

○ Use TL1 Tunnel

CTC Version Selection

Latest version available

Copyright © 2000-2006 Cisco Systems, Inc.
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc.
and/or its affiliates in the U.S and certain other countries

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-C269 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-C13 Set Up Computer for CTC, page 3-2
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-C270 Create a TL1 Tunnel Using CTC

Purpose	This task creates a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

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-C271 View TL1 Tunnel Information

Purpose	This task views a TL1 tunnel created using the CTC Launcher.
Tools/Equipment	None
Prerequisite Procedures	NTP-C13 Set Up Computer for CTC, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

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 19-23.

Table 19-23 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.
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-C272 Edit a TL1 Tunnel Using CTC

Purpose	This task edits a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

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-C273 Delete a TL1 Tunnel Using CTC

Purpose	This task deletes a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

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-C274 Provision the Designated SOCKS Servers

Purpose	This task identifies the ONS 15310-CL and ONS 15310-MA 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-C29 Log into CTC, page 17-44
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note To complete this task, you must have either the IP addresses or DNS names of all ONS 15310-CL and ONS 15310-MAs 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, ONS 15454, ONS 15454 SDH, ONS 15600, and 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.

Note If you cannot log into a network node, complete the "DLP-C29 Log into CTC" task on page 17-44 choosing the Disable Network Discovery option. Complete this task, then login again with network discovery enabled.

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 15310-CL or ONS 15310-MA SOCKS server. The ONS 15310-CL or ONS 15310-MA 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 15310-CL or ONS 15310-MA nodes 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 15310-CL or ONS 15310-MA nodes, 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-C275 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-C13 Set Up Computer for CTC, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Insert the Cisco ONS 15310-CL or Cisco ONS 15310-MA Software Release 8.5 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 the 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-C276 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 Performa 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 If you start CTC by downloading the CTC Launcher application from the node then you do need to perform this procedure. See DLP-C267 Install the CTC Launcher Application from a Release 8.5 Node, page 19-82. This procedure is needed only if CTC is launched from the Internet Explorer browser.

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-C277 Create User Defined Alarm Types

Purpose	This task creates alarm types for external alarms on the 15310-CL-CTX and CTX2500.
Tools/Equipment	None
Prerequisite Procedures	"DLP-C29 Log into CTC" task on page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The alarms and controls are provisioned using the 15310-CL-CTX and CTX2500 card view. For information about the 15310-CL-CTX and CTX2500 external alarms and controls, virtual wire, and orderwire, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*

Step 1 In the node view, double-click the active 15310-CL-CTX or CTX2500 card. The card view appears.

Step 2 Click the **Provisioning > External Alarms > User Defined Alarms** tabs.

Step 3 Click **Add**. The **Enter New Alarm Type** dialog box will display.

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-C278 Configure Link Integrity Timer

Purpose	This task sets the link integrity soak timer for each port in the Ethernet card.
Tools/Equipment	None
Prerequisite Procedures	“DLP-C29 Log into CTC” task on page 17-44
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 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.

Note If the check box under the Link Integrity Disable column is checked, the Link Integrity Timer field for the corresponding port number will be disabled.

Step 4 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 ms and 10000 ms, in multiples of 100 ms.

Note The default link integrity timer value is 200 ms.

Step 5 Click **Apply** to set the specified link integrity soak timer.

Step 6 Return to your originating procedure (NTP).

DLP-C289 Enable Node Secure Mode

Purpose	This task enables secure mode on the ONS 15310-MA. 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 CTX2500 RJ-45 TCP/IP (LAN) port.
Tools/Equipment	
Prerequisite Procedures	CTX2500 cards must be installed. NTP-C102 Back Up the Database, page 15-2 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note The IPv4 address assigned to the CTX2500 TCP/IP (LAN) port must reside on a different subnet from the backplane LAN port and the ONS 15310-MA default router. Verify that the new IPv4 address meets this requirement and is compatible with the ONS 15310-MA network IPv4 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 and click **Next**.

Step 4 Enter the IPv4 address and subnet mask for the CTX2500 LAN (TCP/IP) port in the CTX2500 Ethernet Port page, . The IPv4 address cannot reside on the same subnet as the backplane LAN port or the ONS 15310-MA default router.

Step 5 Click **Next**.

Step 6 You can modify the backplane IPv4 address, subnet mask, and default router in the Backplane Ethernet Port page, if needed.

Note Normally, you do not need to modify these fields if no ONS 15310-MA 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 15310-MA where the CTC computer is connected. The computer is not visible to the 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 CTX2500 cards reboot. CTC switches to network view, and the CTC Alerts dialog box appears. In network view, the node changes to gray and the condition changes to DISCONNECTED.

Step 10 In the CTC Alerts dialog box, click **Close**. Wait for the reboot to finish. (This may 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. Select 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 CTX2500 IP (LAN) port address becomes the IPv4 address of the node. The backplane LAN port has a different IPv4 address.

Step 12 Return to your originating procedure (NTP).

APPENDIX A

CTC Information and Shortcuts

This appendix describes the Cisco Transport Controller (CTC) views, menu 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 15310-CL and Cisco ONS 15310-MA 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 and Views

CTC provides three views of the ONS 15310-CL or ONS 15310-MA and ONS network:

- Node view appears when you first log into an ONS 15310-CL or ONS 15310-MA. This view shows a graphic of the ONS 15310-CL or ONS 15310-MA shelf and provides access to tabs and subtabs that you use to manage the node.
- Card view provides access to individual ONS 15310-CL or ONS 15310-MA cards. This view provides a graphic of the card and 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 from one view to another. For example, in network view, click a node, then click the down arrow.
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.

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-2 shows the actions that are available from the CTC menu and toolbar.

Table A-2 CTC Menu and Toolbar Options

Menu	Menu Option	Toolbar	Description
File	Add Node		Adds a node to the current session. See the "DLP-C32 Add a Node to the Current Session or Login Group" task on page 17-48.
	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-C222 Print CTC Data" task on page 19-18.
	Export		Exports CTC data. See the "DLP-C223 Export CTC Data" task on page 19-20.
	Exit	—	Closes the CTC session.
Edit	Preferences		Displays the Preferences dialog box: • General—Allows you to change event defaults and manage preferences. • Login Node Groups—Allows you to create login node groups. See the "DLP-C31 Create Login Node Groups" task on page 17-47. • Map—Allows you to customize the network view. See the "DLP-C131 Change the Network View Background Color" task on page 18-38 and the "DLP-C133 Apply a Custom Network View Background Map" task on page 18-39. • Circuit—Allows you to change the color of circuit spans. See the "DLP-C113 Change Active and Standby Span Color" task on page 18-19. • Firewall—Sets the Internet Inter-ORB Protocol (IIOP) listener ports for access to the ONS 15310-CL or ONS 15310-MA through a firewall. See the "NTP-C22 Set Up the ONS 15310-CL or ONS 15310-MA for Firewall Access" procedure on page 4-8. • JRE—Allows you to select another Java Runtime Environment (JRE) version. See the "DLP-C35 Change the JRE Version" task on page 17-50.

Table A-2 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 choose the node name of 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-2 CTC Menu and Toolbar Options (continued)

Menu	Menu Option	Toolbar	Description
Tools	Circuits	—	Displays the following options: • Repair Circuits—(Cisco ONS 15454 only) 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. Refer to the "NTP-C76 Reconfigure Circuits" procedure on page 7-11. • Set Path Selector Attributes—Allows you to edit path protection circuit path selector attributes. See the "DLP-C114 Edit Path Protection Circuit Path Selectors" task on page 18-20. • Set Circuit State—Allows you to change a circuit service state. See the "DLP-C111 Change a Circuit Service State" task on page 18-17. • Roll Circuit—Allows you to reroute live traffic without interrupting service. See the *"NTP-C129 Bridge and Roll Traffic" procedure on page 7-10*. • Delete Rolls—Allows you to delete roll circuits. See the *"NTP-C129 Bridge and Roll Traffic" procedure on page 7-10*. • 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—(ONS 15454 only) Shows the RPR ring for the circuit selected on the Circuits window. Refer to the *Cisco ONS 15454 Procedure Guide*.
	Overhead Circuits	—	(ONS 15454 only) Displays the Repair IP Tunnels option, which fixes circuits that are in the PARTIAL status as a result of node IP address changes. Refer to the *Cisco ONS 15454 Procedure Guide*.
	Topology Upgrade	—	Displays the following options: • Convert Path Protection to BLSR—(ONS 15454 only) Converts a path protection configuration to a bidirectional line switch ring (BLSR). Refer to the *Cisco ONS 15454 Procedure Guide* for more information. • Convert Unprotected to Path Protection option—Converts a point-to-point or linear add/drop multiplexer (ADM) to path protection. See the "NTP-C96 Convert an Unprotected Point-to-Point or Linear ADM to a Path Protection Configuration Automatically" procedure on page 13-6.
	Manage VLANs	—	Displays a list of VLANs that have been created and allows you to delete VLANs. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.
	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*.
	Open IOS Connection		(ONS 15454 only) Displays the Cisco IOS command line interface dialog box if a Cisco IOS capable card (ML-100T-8, CL-100T-8) is installed in the node. Refer to the *Cisco ONS 1310-CL and Cisco ONS 15310-MA 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.

Table A-2 CTC Menu and Toolbar Options (continued)

Menu	Menu Option	Toolbar	Description
Help	Contents and Index	—	Displays the online help window.
	User Manuals	—	Displays the Cisco ONS 15310-CL and Cisco ONS 15310-MA documentation.
	About CTC	—	Displays the software version and the nodes in the CTC session.
—	Network Scope	—	Displays the selected network scope (applies to ONS 15454 nodes only). 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—(ONS 15454 nodes only) GCC, OTS, PPC • TDM—DCC, PPC, server trail
—	—	⊞	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 (see the Toolbar column left for comparison). 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 "DLP-C115 Delete Circuits" task on page 18-21. 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-C36 Configure the CTC Alerts Dialog for Automatic Popup" task on page 17-51.

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-3 lists the CTC window mouse shortcuts.

Table A-3 CTC Window Mouse Shortcuts

Technique	Description
Double-click	• Node in network view—Displays the node view. • Domain in network view—Displays the nodes in a domain. • Card in node view—Displays the card view. • Alarm/Event—Displays the alarm or event raising object. • 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, or update circuits with a new node. • Span in network view—Displays a menu that you can use to view information about the span 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. You can also expand and collapse links. • Card in node view—Displays a menu that you can use to open, delete, and reset cards. The card that you select 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.
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. • Over domain in network view—Displays domain name and the number of nodes in the domain. • Over card in node view—Displays card type, card status, and alarm profile status. • 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.

Node View Shortcuts

Table A-4 shows actions on ONS 15310-CL or ONS 15310-MA cards that you can perform by moving your mouse over the CTC window.

Table A-4 Performing Node View Card Shortcuts

Action	Shortcut
Display card information	Move your mouse over cards in the graphic to display tooltips with the card type, card present or card provisioned but not present, the highest level of alarm (if any), and the alarm profile used by the card.
Open, reset, or delete a card	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 that you want to provision in the slot from the shortcut menu. For the ONS 15310-CL, see the "NTP-C10 Preprovision a Card Slot" procedure on page 1-15. For the ONS 15310-MA, see the "NTP-C162 Preprovision a Card Slot" procedure on page 2-31.

Network View Tasks

Right-click the network view graphic area or a node, span, or domain to display shortcut menus. Table A-5 lists the actions that are available from the network view.

Table A-5 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 CTC 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 tabs.
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."
Save a node icon position	On the network view map, right-click and choose **Save Node Position**. Click **Yes** on the Save Node Position dialog box.
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.

Table A-5 Network Management Tasks in Network View (continued)

Action	Task
Provision a circuit	Right-click a node. From the shortcut menu, choose **Provision Circuit To** and select 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	Any of the following: • Move your 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. See also the "DLP-C166 Initiate a Path Protection Force Switch on a Span" task on page 18-60.
Upgrade a span	Right-click a span and choose **Upgrade Span** from the shortcut menu. **Note** Span upgrades do not upgrade SONET topologies, for example, a 1+1 group to a path protection configuration. See Chapter 13, "Convert Network Configurations" for topology upgrade procedures.
Upgrade terminal to linear	Right-click a span and choose **Upgrade Protection > Terminal to Linear** from the shortcut menu. See the "NTP-C136 Convert a Point-to-Point to a Linear ADM Automatically" procedure on page 13-2.

Table Display Options

Right-clicking a table column displays a menu. Table A-6 shows table display options, which include rearranging or hiding CTC table columns and sorting table columns by primary or secondary keys.

Table A-6 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*

Table A-6 Table Display Options (continued)

Task	Click	Right-Click Shortcut Menu
Display all hidden columns	—	Choose **Reset Columns Order/Visibility**.
Sort table (primary)	Click a column header; each click changes the 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 listed next to “Row Count”; it is the last item on the shortcut menu.

Equipment Inventory

In node view, the Inventory tab displays information about the ONS 15310-CL or ONS 15310-MA equipment, including:

- Delete Button—After highlighting a card with your mouse, use this button to delete the card from node view.
- Hard-Reset Button—After highlighting a card with your mouse, use this button to hard-reset a card. A hard reset temporarily removes power and clears all buffer memory. Before you hard-reset a 15310-CL-CTX card and CTX2500 card, put the card in standby mode by completing a soft-reset.
- Soft-Reset Button—After highlighting a card with your mouse, use this button to soft-reset a card. A soft reset reboots the card and reloads the operating system and the application software.
- 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, CE-100T-8 or CTX-CL600.
- Actual Eqpt Type—Displays the specific card name.
- Admin State—Changes the card service state unless network conditions prevent the change.
  - 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. Card service states include:
  - IS-NR (In-Service and Normal)
  - OOS-AU,AINS & MEA (Out-of-Service and Autonomous,Auto In-Service and Mismatched Equipment)
  - OOS-AU,AINS & SWDL (Out-of-Service and Autonomous,Auto In-Service and Software Download)
  - OOS-AU,AINS & UEQ (Out-of-Service and Autonomous,Auto In-Service and Unequipped)

  - OOS-AU,MEA (Out-of-Service and Autonomous,Mismatched Equipment)
  - OOS-AU,SWDL (Out-of-Service and Autonomous,Software Download)
  - OOS-AU,UEQ (Out-of-Service and Autonomous,Unequipped)
  - OOS-AUMA,MEA & MT (Out-of-Service and Autonomous Management,Mismatched Equipment and Maintenance)
  - OOS-AUMA,MEA & UAS (Out-of-Service and Autonomous Management,Mismatched Equipment and Unassigned)
  - OOS-AUMA,MT & SWDL (Out-of-Service and Autonomous Management,Maintenance and Software Download)
  - OOS-AUMA,MT & UEQ (Out-of-Service and Autonomous Management,Maintenance and Unequipped)
  - OOS-AUMA,UAS *(Out-of-Service and Autonomous Management,Unassigned)*
  - OOS-AUMA,UAS & UEQ (Out-of-Service and Autonomous Management,Unassigned and Unequipped)
  - OOS-MA,MT (Out-of-Service and Management,Maintenance)
- 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.
- Version ID—Displays the manufacturing version identifier for a fan tray, chassis, or card.

INDEX