CISCO SYSTEMS

# Cisco ONS 15600 SDH Reference Manual

Product and Documentation Release 8.0
Last Updated: April 2010

# CONTENTS

**Cisco ONS 15600 SDH Reference Manual, R8.0** ■

**FIGURES**

**TABLES**

# About this Manual

This section explains the objectives, intended audience, conventions, related documentation, and technical assistance information for the *Cisco ONS 15600 SDH Reference Manual*.

This section provides the following information:

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

# Revision History

| Date | Notes |
|------|-------|
| October 2007 | • Added this Revision History Table<br>• Updated About this Guide chapter |
| September 2008 | • Updated the Computer Requirements for CTC table in Chapter 4, Cisco Transport Controller Operation.<br>• Updated voltage and current rating in section A.1.15 Power Specifications.<br>• Added a note in Card Default Settings and Node Default Settings section of Appendix C, Network Element Defaults. |
| November 2008 | Updated Server Trail section in Chapter 7, Circuits and Tunnels. |
| April 2010 | Updated the section "SNMP Overview" in the chapter "SNMP". |

# Document Objectives

The *Cisco ONS 15600 SDH Reference Manual* provides technical information for the Cisco ONS 15600 SDH.

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

# Audience

To use this reference manual you should be familiar with Cisco or equivalent optical transmission equipment.

# Related Documentation

Use the *Cisco ONS 15600 SDH Reference Manual* in conjunction with the following referenced publications:

- *Cisco ONS 15600 SDH Procedure Guide*
  Provides installation, turn up, test, and maintenance procedures.

- *Cisco ONS 15600 SDH Troubleshooting Guide*
  Provides alarm descriptions and troubleshooting procedures, general troubleshooting procedures, error messages, and transient conditions.

- *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Command Guide, Release 8.0*
  Provides a full Transaction Language One (TL1) command and autonomous message set including parameters, access identifiers (AIDs), conditions, and modifiers for the Cisco ONS 15454 SDH and Cisco ONS 15600 SDH.

- *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Reference Guide, Release 8.0*
  Provides general information, procedures, and errors for TL1 in the Cisco ONS 15454 SDH and Cisco ONS 15600 SDH.

- *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Command Quick Reference Guide, Release 8.0*
  Provides most commonly used Transaction Language One (TL1) command and autonomous message set including parameters, access identifiers (AIDs), conditions, and modifiers for the Cisco ONS 15454 SDH and Cisco ONS 15600 SDH.

- *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 for Beginners, Release 8.0*
  Provides Transaction Language One (TL1) command and autonomous message set information for novice Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 users.

- *Release Notes for the Cisco ONS 15600 SDH Release 8.0*
  Provides caveats, closed issues, and new features 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/ps2006/prod_eol_notices_list.html.

# Document Conventions

This publication uses the following conventions:

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

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

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

**Warning** **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, Obtaining Support, and Security Guideliens section.

# Where to Find Safety and Warning Information

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

# Cisco Optical Networking Product Documentation CD-ROM

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

# Obtaining Documentation and Submitting a Service Request

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

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

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

# Shelf and Backplane Hardware

This chapter provides a description of Cisco ONS 15600 SDH shelf and backplane hardware. Card and cable descriptions are provided in Chapter 2, "Card Reference."

To install equipment, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Chapter topics include:

**Note**   The Cisco ONS 15600 SDH assembly is intended for use with telecommunications equipment only.

**Note**   The ONS 15600 SDH is designed to comply with Telcordia GR-1089-CORE Type 2 and Type 4 equipment. Install and operate the ONS 15600 SDH 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).

## 1.1  Installation Overview

The ONS 15600 SDH is a Network Equipment Building System III (NEBS III)-compliant, environmentally hardened shelf assembly that ships as a single shelf in a bay assembly for Release 8.0. The ONS 15600 SDH comes with the power distribution unit (PDU), shelf, fans, and backplane already

installed. The front door of the ONS 15600 SDH allows access to the shelf assembly, fan-tray assembly, and cable-management area. The customer access panel (CAP) or customer access panel version 2 (CAP2) on the back of the shelf provide access to alarm contacts, external interface contacts, and timing contacts. Power and ground terminals are located on the top left and right sides of the bay.

⚠

**Caution**     Voltage to the alarm circuits should not exceed –48 VDC.

The ONS 15600 SDH comes mounted in a custom, certified NEBS-2000 rack. The bay assembly, including the rack, fan trays, and PDU weighs approximately 500 pounds (226.8 kg) with no cards installed.

ONS 15600 SDH STM-N cards have OGI connectors on the card faceplate; available connector termination types are SC, ST, and FC. Fiber optic cables are routed to the front of the STM-N cards.

The ONS 15600 SDH is powered using –48 VDC power but may range from –40.5 to –72 VDC. Input power is accessible from the sides of the bay, and output power is accessible at the rear of the bay. Cisco supports dual office-power feeds only.

Install the ONS 15600 SDH in compliance with your local and national electrical codes:

- United States: National Fire Protection Association (NFPA) 70; United States National Electrical Code

- Canada: Canadian Electrical Code, Part I, CSA C22.1

- Other countries: If local and national electrical codes are not available, refer to IEC 364, Part 1 through Part 7.

# 1.2  Bay Installation

In this chapter, the terms "ONS 15600 SDH" and "bay assembly" are used interchangeably. In the installation context, these terms have the same meaning. Otherwise, bay assembly refers to the physical steel enclosure that holds the shelves and power distribution unit (PDU), and ONS 15600 SDH refers to the entire system, both hardware and software.

To install the ONS 15600 SDH, you must first unpack the bay assembly. Two custom ramps and two dollies are available to assist you with the removal of the bay from the shipping pallet and transportation to the installation location. Figure 1-1 shows the bay assembly with the dollies installed.

**Figure 1-1        ONS 15600 SDH with Dollies Installed**
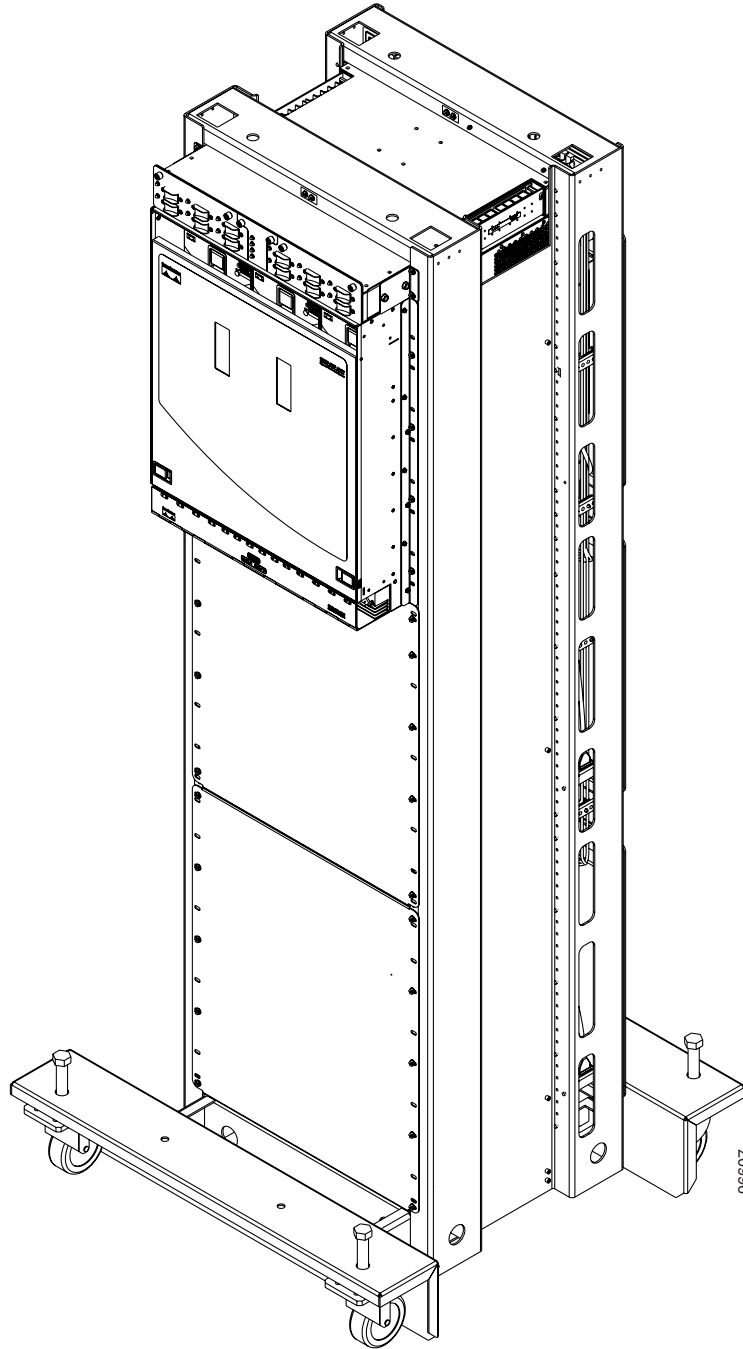


The ONS 15600 SDH shelf measures 25 inches high, 19-9/16 inches wide, and 23 inches deep (63.5 cm H x 49.7 cm W x58.3 cm D). A maximum of three ONS 15600 SDHs can fit in a custom seven-foot equipment rack. The ONS 15600 SDH that ships within a rack is 83-7/8 inches high, 23-5/8 inches wide, and 23-5/8 inches deep (213 cm H x 60 cm W x 60 cm D).

**Note**     Cisco supports only one ONS 15600 SDH shelf per bay.

# 1.3  Front Door

The ONS 15600 SDH features a door to the front compartment that you can open by releasing the latches on the bottom left and right sides of the door. The front door provides access to the shelf, cable-management tray, and fans (Figure 1-2).

*Figure 1-2*        ***ONS 15600 SDH Front Door***
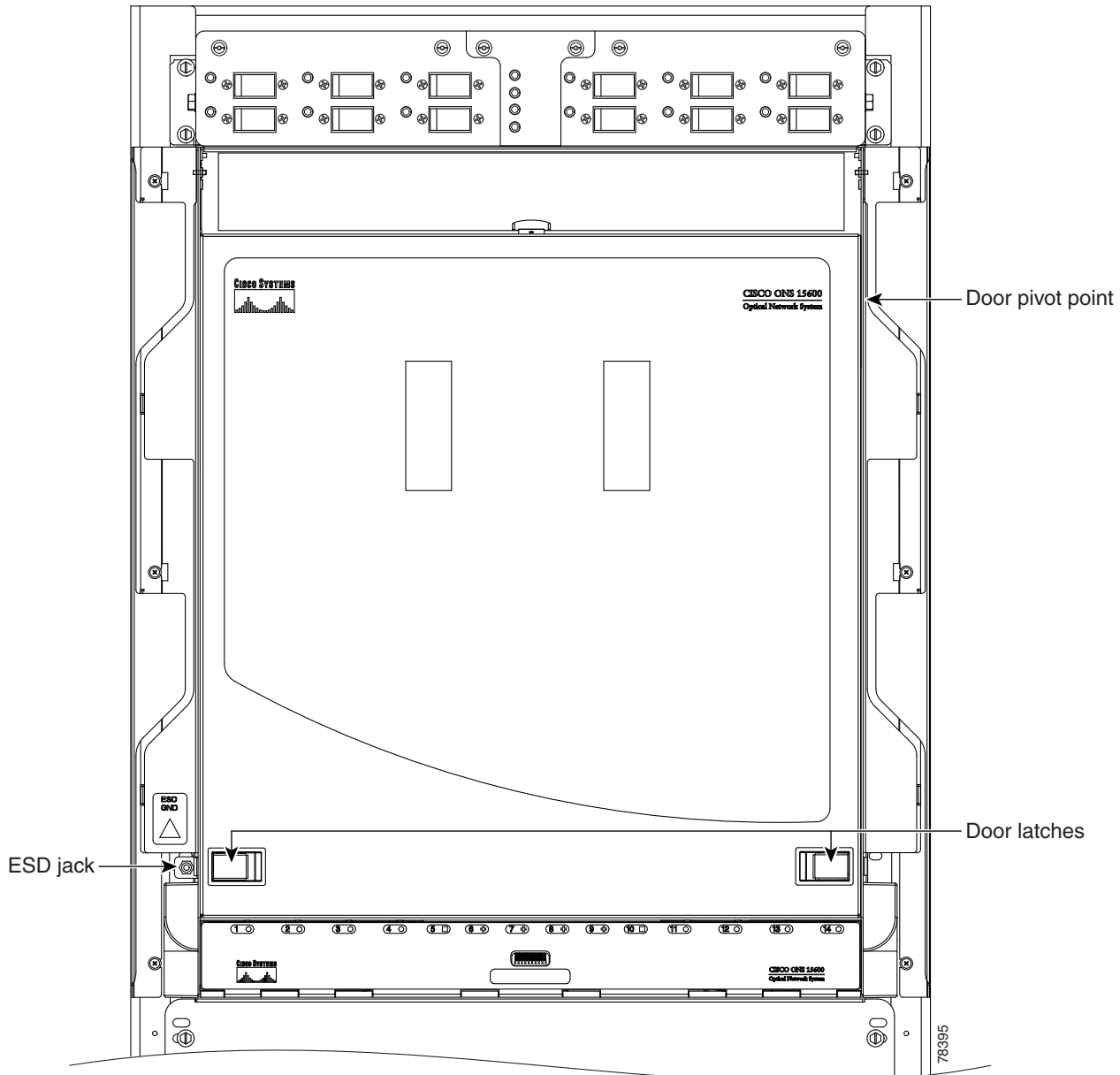


You can remove the front door of the ONS 15600 SDH to provide unrestricted access to the front of the shelf. A label is pasted in a box in the center of the swing-down door that covers the fiber routers (Figure 1-3). This label designates the position of the rack and shelf in a lineup.

*Figure 1-3        Bay Label*

RACK 01   SHELF 01
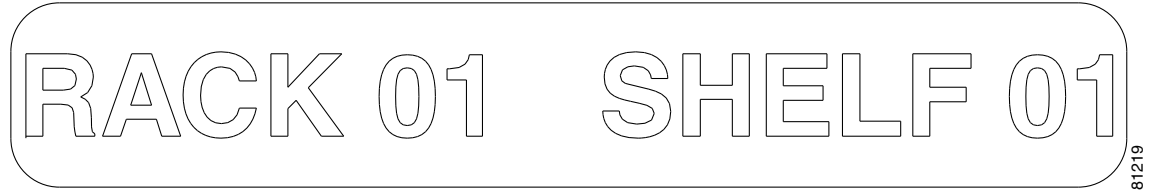
81219

The front door also has a Class I laser warning (Figure 1-4).

*Figure 1-4        Laser Warning Label*

CISCO SYSTEMS, INC.
170 WEST TASMAN DRIVE
SAN JOSE, CA  95134

DATE OF MFG:
CLASS 1 LASER PRODUCT

COMPLIES WITH FDA PERFORMANCE STANDARDS FOR LASER
PRODUCTS EXCEPT FOR DEVIATIONS PURSUANT TO LASER
NOTICE NO. 50, DATED JULY 26,2001.
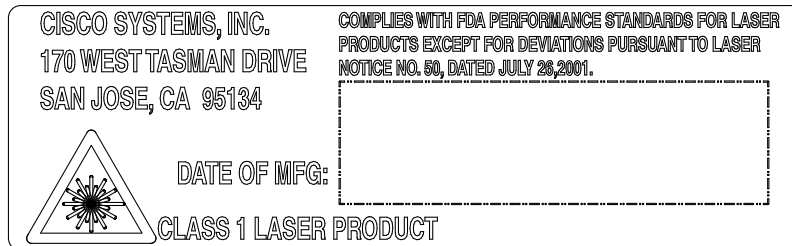
83121

# 1.4  Rear Covers

The ONS 15600 SDH has an optional plastic rear cover that is held in place with six 6-32 x 3/8 inch Phillips screws. This plastic cover provides additional protection for the cables and connectors on the backplane (Figure 1-5).

**Figure 1-5** **Plastic Rear Cover**
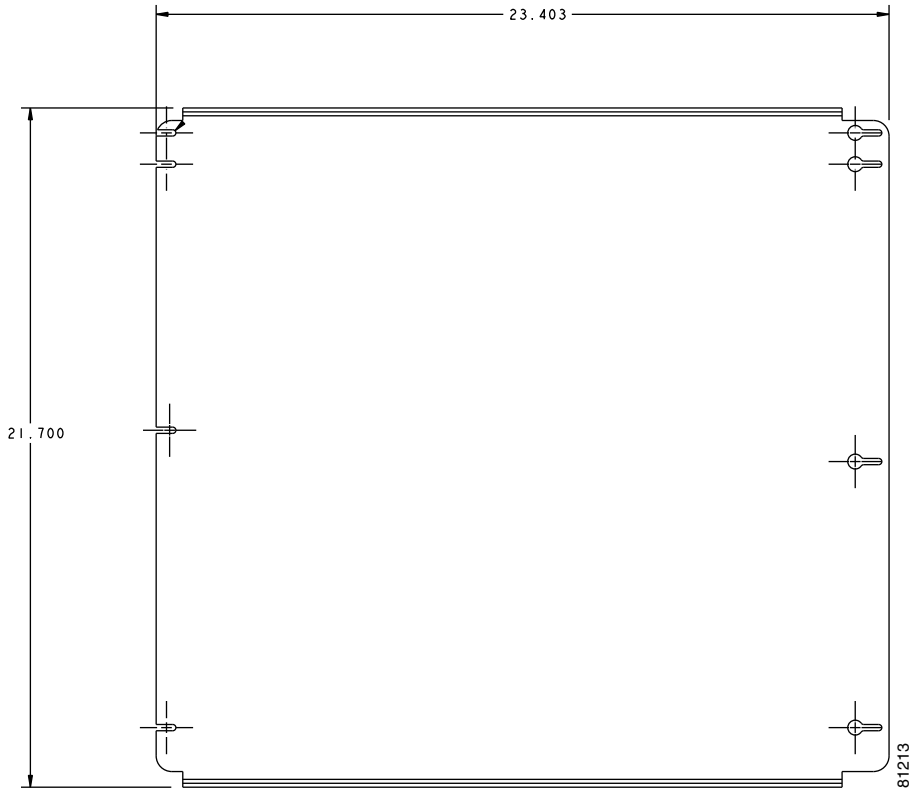


Figure 1-6 shows the bus bar covers.

**Figure 1-6** **PDU Bus Bar Cover**
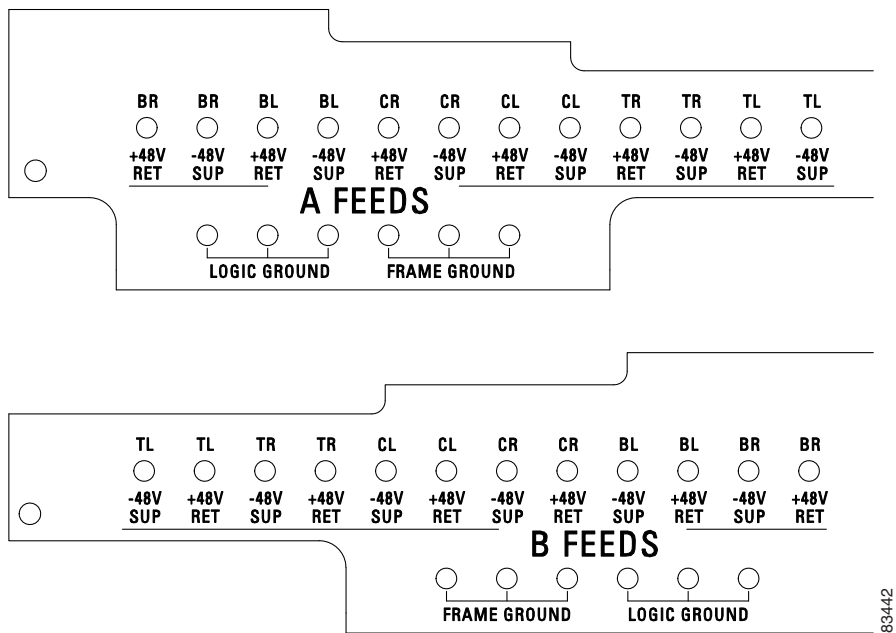
# 1.5 Cable Routing

The narrow and wide cable routing modules (CRMs) can be installed on the sides of the bay to manage and contain the optical cables as they are routed away from the bay. You can use both types of fiber routing systems with overhead or under-floor cabling.

# 1.6 Customer Access Panel

The Customer Access Panel (CAP or CAP2) is located in the middle on the rear of the shelf. The CAP and CAP2 provide an alarm pin field, timing, and LAN connections. The CAP or CAP2 plugs into the backplane using 2mm Hard Metric connectors with 752 pins and is held in place with one large captive bolt and multiple screws.

The CAP2 has the additional capability of providing provisionable power monitoring.

Figure 1-7 shows the location of the CAP or CAP2 on the back of the shelf.

**Note**   The ONS 15600 SDH supports only T1 (100 ohm) building integrated timing supply (BITS).

*Figure 1-7        Rear of the ONS 15600 SDH, Including the CAP/CAP2*
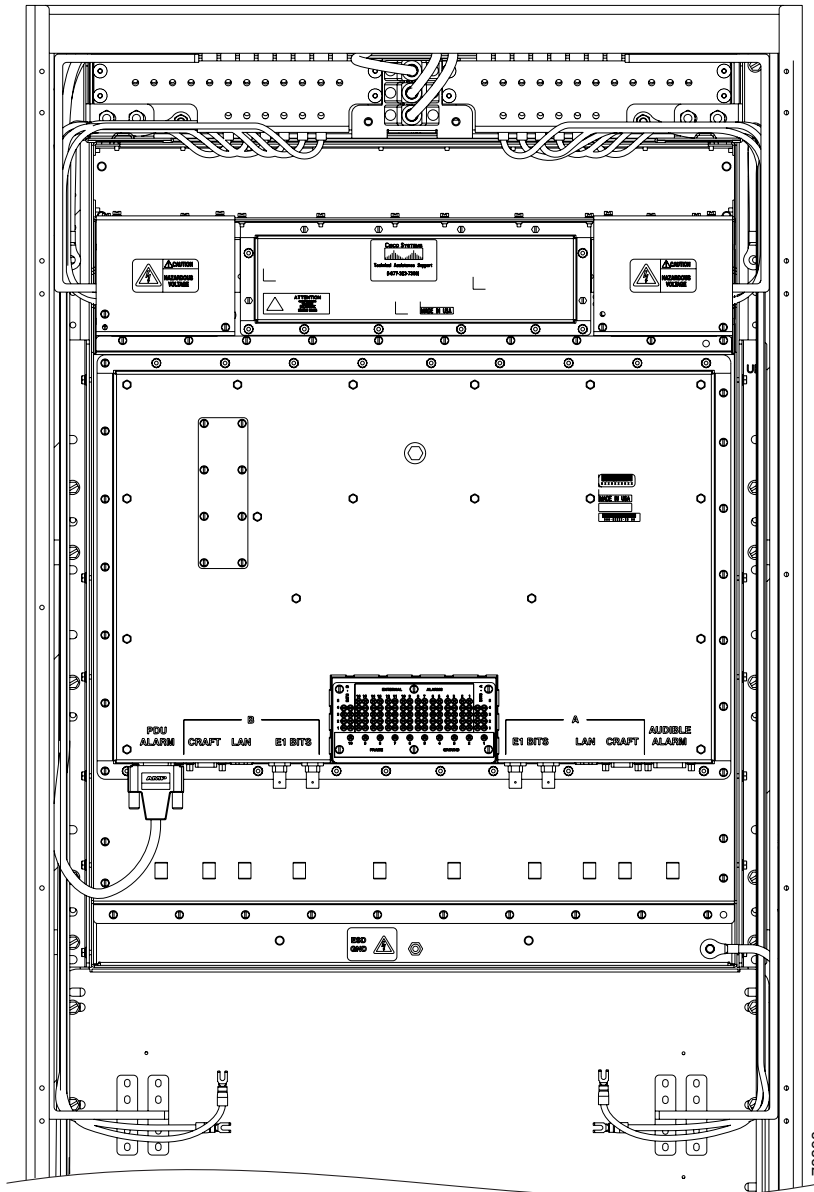


The ONS 15600 SDH CAP and CAP2 provide the following features:

- BITS T1 (100 ohm) interfaces via wire-wrap pins.

- Two Ethernet interfaces via RJ-45 connectors with internal transformer isolation.

- An EIA/TIA-232 craft interface via DB-9 connectors. This interface is surge-protected and provides EMI filtering. Two interfaces are provided for redundancy.

- Four audio alarm interfaces via a DB-15 connector that is surge-protected and EMI-filtered. The audio alarm indication is provided by the TSC card and this interface can receive a signal to disable the audio alarm.

- Four visual alarm interfaces via a DB-15 connector that is surge-protected and EMI-filtered. The visual alarm indication is provided by the TSC card and the signal is connected to the PDU where LEDs indicate the alarm status and severity.

- Environmental (external) alarms and controls (16 inputs and 16 outputs) via wire-wrap pins. The interface is surge-protected and provides isolation by using an opto-isolator for alarm inputs and relays for alarm outputs. By connecting to different wire-wrap pins on the CAP/CAP2, the alarm outputs can be configured for either normally open (NO) or normally closed (NC) operation. Alarms are initiated by shorting these contacts. The alarm input interface provides a pair of positive and negative wire-wrap pins.

The isolation and termination meet the intra-building lightning surge specification in Telcordia GR-1089. The CAP and CAP2 have –48 VDC monitoring with an $I^2C$ interface and nonvolatile memory to store the CAP/CAP2 revision information.

Figure 1-8 shows the CAP faceplate.

*Figure 1-8*      ***CAP Faceplate and Connections***
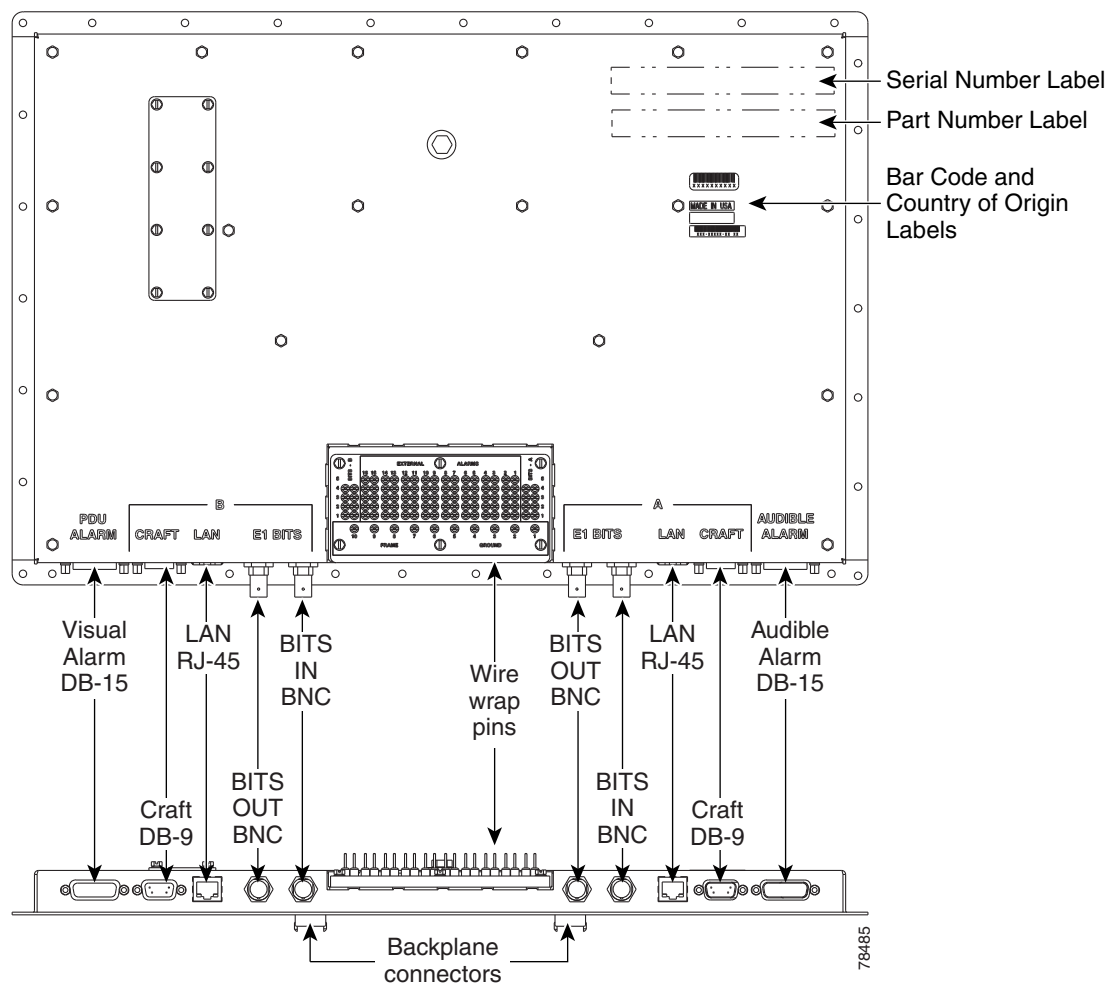


If the CAP/CAP2 fails, the node raises an EQPT alarm. You can replace the CAP/CAP2 on an in-service node without affecting traffic. To replace a CAP, refer to the *Cisco ONS 15600 SDH Procedure Guide*. Always replace the CAP during a maintenance window.

# 1.7 Alarm, Timing, LAN, and Craft Pin Connections

⚠

**Caution**    Always use the supplied ESD wristband when working with a powered ONS 15600 SDH or any ONS 15600 SDH components. Plug the wristband cable into one of the ESD jacks located on the lower-left outside edge of the bay assembly and at the bottom rear of the shelf.

The ONS 15600 SDH has a backplane pin field located at the bottom rear of the shelf that is part of the CAP. The CAP provides 0.045 square inch (0.290 square centimeter) wire-wrap pins for enabling alarm inputs and outputs and timing input and output. This section describes the backplane pin field and pin assignments, as well as timing and LAN connections. See the "1.6  Customer Access Panel" section on page 1-7 for more information.

## 1.7.1 External Alarm and Control Contact Installation

The external (environmental) alarm contacts consist of the wire-wrap pin field and two D-Sub 15s. The alarm pin field supports up to 16 alarm inputs (external alarms) and 16 alarm outputs (external controls). The two D-Sub 15s support four audible alarms, four visual alarms, one alarm cutoff (ACO), a PDU Fail A, and a PDU Fail B.

By connecting to different wire-wrap pins on the CAP or CAP2, the alarm outputs can be configured for either normally open (NO) or normally closed (NC) operation (see Figure 1-9). The alarm inputs consist of two wire-wrap pins on the CAP or CAP2 and the alarm outputs consist of three wire-wrap pins.

### 1.7.1.1 Visual and Audible Alarms

Visual and audible alarm contacts are provisioned as Critical, Major, Minor, and Remote. Figure 1-9 shows alarm pin assignments.

*Figure 1-9        Alarm Pin Assignments on the CAP/CAP2*
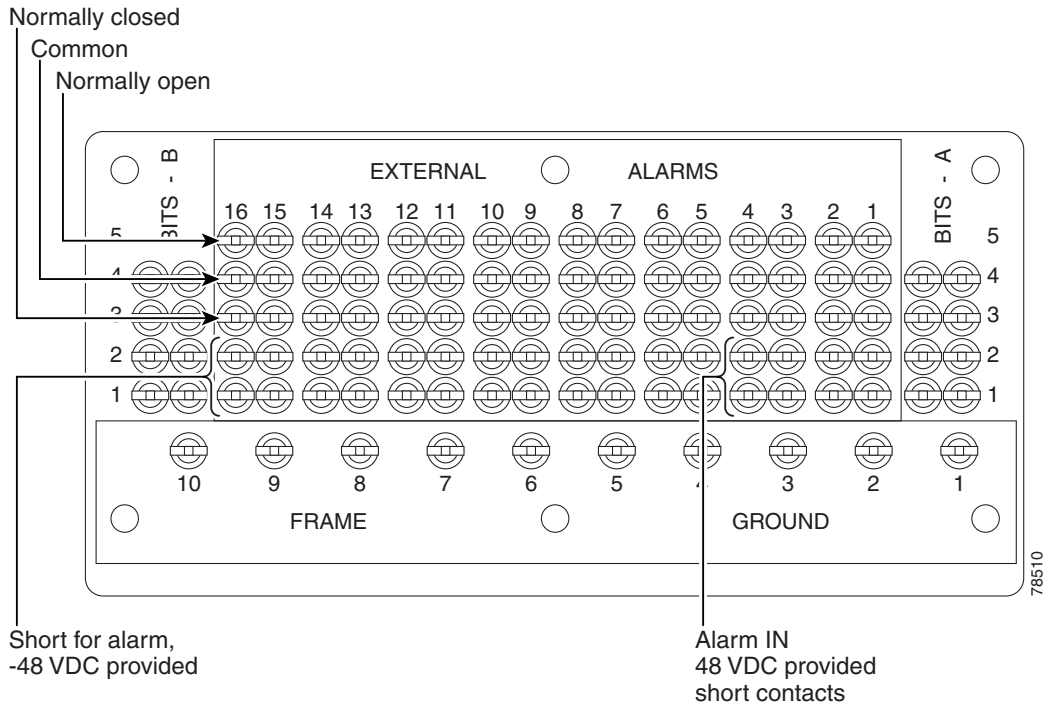


Visual and audible alarms can be wired to trigger an alarm light at a central alarm collection point when the corresponding contacts are closed.

### 1.7.1.2  Alarm Cutoff and PDU Alarms

The PDU Alarm connection controls the visual alarm indicators on the front of the PDU. You can also activate the alarm cutoff (ACO) function by pressing the ACO button on the TSC card faceplate. The ACO function extinguishes all audible alarm indications, but the alarm is still raised in Cisco Transport Controller (CTC).

## 1.7.2  Timing Installation

The ONS 15600 SDH backplane supports two 100-ohm BITS clock pin fields. Figure 1-10 shows the pin assignments for the BITS timing pin fields.

**Note**    Refer to Telcordia SR-NWT-002224 for rules about provisioning timing references.

**Note**    See Chapter 6, "Timing," for more information.

*Figure 1-10 BITS Timing Connections on the CAP/CAP2*
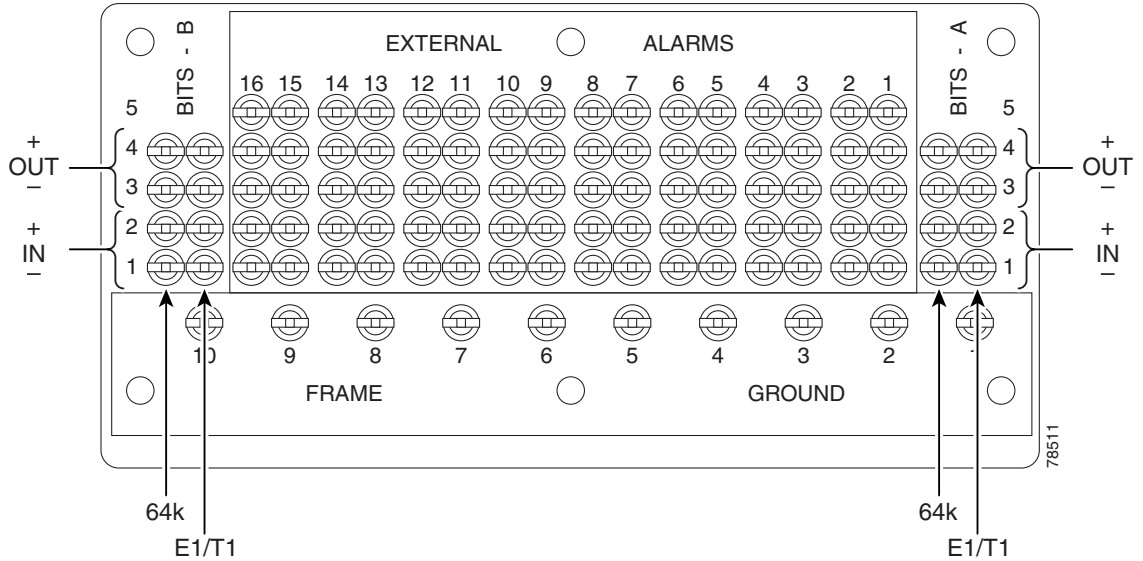


## 1.7.3 LAN Installation

Use a straight-through LAN cable with the LAN port on the CAP or CAP2 to connect the
ONS 15600 SDH to a hub, switch, or a LAN modem for remote access to the node. Use a crossover cable
when connecting the CAP or CAP2 to a workstation. You can also use a straight-through or crossover
LAN cable with the LAN port on the active TSC faceplate to connect directly to the local ONS 15600
SDH.

**Note**  Do not use the LAN port on the active TSC card for remote monitoring because you will lose
connectivity to the node if the other TSC card in the shelf becomes the active TSC card.

## 1.7.4 TL1 Craft Interface Installation

To open a TL1 session using the craft interface on a PC, use the RJ-45 port on the active TSC card to
access the system using a standard web browser. If a browser is not available, you can access the system
using one of the two EIA/TIA-232 ports on the CAP or CAP2. Each EIA/TIA-232 port supports VT100
emulation so that you can enter TL1 commands directly without using a web browser. Because the CAP
and CAP2 EIA/TIA-232 port is set up as a data terminal equipment (DTE) interface, you must use a
3-pair swapping null modem adapter when you are working in a UNIX or PC environment so that the
TXD/RXC, DSR/DTR, and CTS/RTS pins are swapped. Use a standard pin D-sub cable when
connecting to a PC. Refer to the *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Command
Guide* for more information.

**Note**  Do not use the LAN port on the active TSC card for remote monitoring because you will lose
connectivity to the node if the other TSC card in the shelf becomes the active TSC card.

# 1.8  Power Distribution Unit

The PDU consists of a mounting chassis, A- and B-side power modules, an alarm module, and a rear I/O unit. The ONS 15600 SDH PDU has LEDs that alert you to Critical, Major, Minor, and remote alarms on the node. Each module can support three 100A input power feeds, 48 VDC power load (based on a fully loaded ONS 15600 SDH shelf). The PDU supplies six 50A power feeds to the shelves. (The PDU provided with the ONS 15600 SDH is capable of supplying power to up to three shelves.)

A three-shelf bay at the minimum operational voltage of –36 VDC requires 69-A per feed (207 A total). A three-shelf bay at the nominal operational voltage of –48 VDC requires 52-A per feed (156 A total). Each of the three feeds should be protected by its own 100-A breaker. A bus bar system, rather than wiring, provides a reliable, low resistance path to the ONS 15600 SDH shelf. Figure 1-6 on page 1-6 shows the PDU output covers found at the top rear of the bay.

**Note**    Cisco supports only one ONS 15600 SDH shelf per bay.

# 1.9  Power and Ground Description

Ground the equipment according to Telcordia standards or local practices. The ground connection is located on the front of the bay's top horizontal rails. The ONS 15600 SDH provides two #12 tapped holes to accommodate the grounding lug. The lug must be a dual-hole type and rated for at least 125-A capacity. Figure 1-11 shows the front and rear bay ground holes.

*Figure 1-11      Front and Rear Bay Ground Holes*
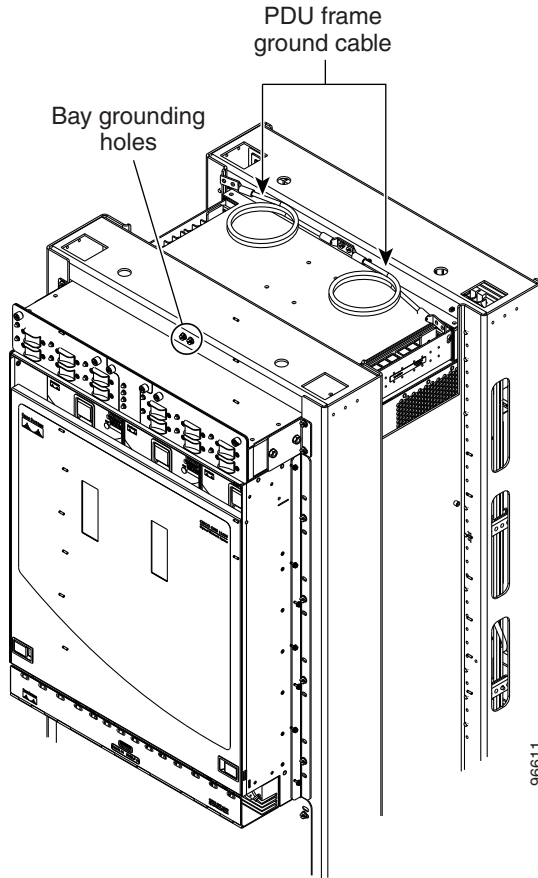


The main power connections are made at the PDU side terminals at the top of the bay. To install redundant power feeds, use four power cables and ground cables. For a single power feed, only two power cables and one ground cable (all rated for at least 125-A capacity) are required. Use a conductor with low impedance to ensure circuit overcurrent protection. The ground conductor must have the capability to safely conduct any faulty current that might be imposed.

Cisco recommends the following wiring conventions, but customer conventions prevail:

- Red wire for battery connections (–48 VDC)

- Black wire for battery return connections (0 VDC)

- The battery return connection is treated as DC-I, as defined in Telcordia GR-1089-CORE, issue 3

The ONS 15600 SDH shelf has redundant –48 VDC power terminals on its backplane. The terminals are labeled A FEEDS and B FEEDS and are located at the top left and right sides of the shelf behind clear plastic covers.

# 1.10  Fan-Tray Assembly

The fan-tray assembly is located at the top of the ONS 15600 SDH shelf front compartment. The fan-tray assembly has three removable drawers that hold two fans each and fan-control circuitry for the ONS 15600 SDH (Figure 1-12). You should only need to access the fans if a fan fails.

**Figure 1-12** **Fan-Tray Assembly**



71045
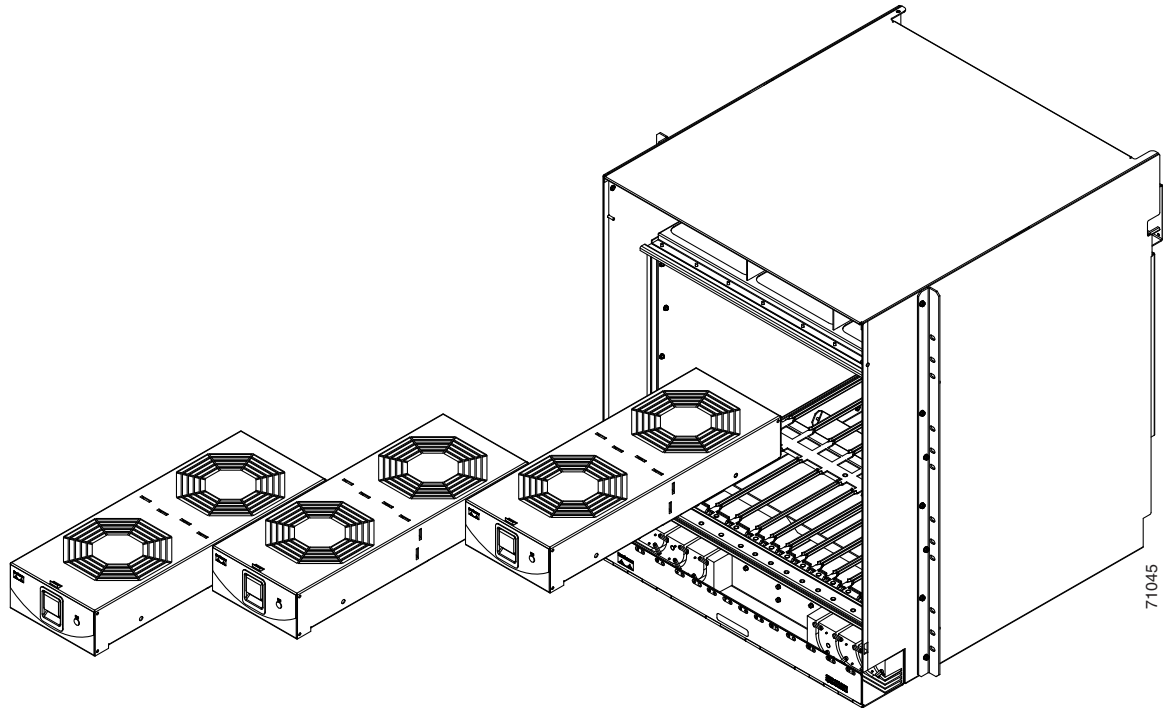
## 1.10.1 Air Filter

The ONS 15600 SDH contains a reusable air filter that is made of an open-cell polyurethane foam that is flame retardant and fungi resistant. The air filter is located above the three fan trays (Figure 1-13). This disposable filter is designed to be cleaned using only mild detergents. You can order air filter replacements from Cisco Systems (P/N 700-13116-05). Keep spare filters in stock. Refer to the *Cisco ONS 15600 SDH Procedure Guide* for information about replacing the fan-tray air filter.

⚠
**Caution**    Inspect the air filter every 30 days, and clean the filter every three to six months. Replace the air filter every two to three years. Avoid cleaning the air filter with harsh cleaning agents or solvents.

⚠
**Caution**    Do not operate an ONS 15600 SDH without a fan-tray air filter. A fan-tray filter is mandatory.

*Figure 1-13      Air Filter and one Fan Tray Pulled Out*
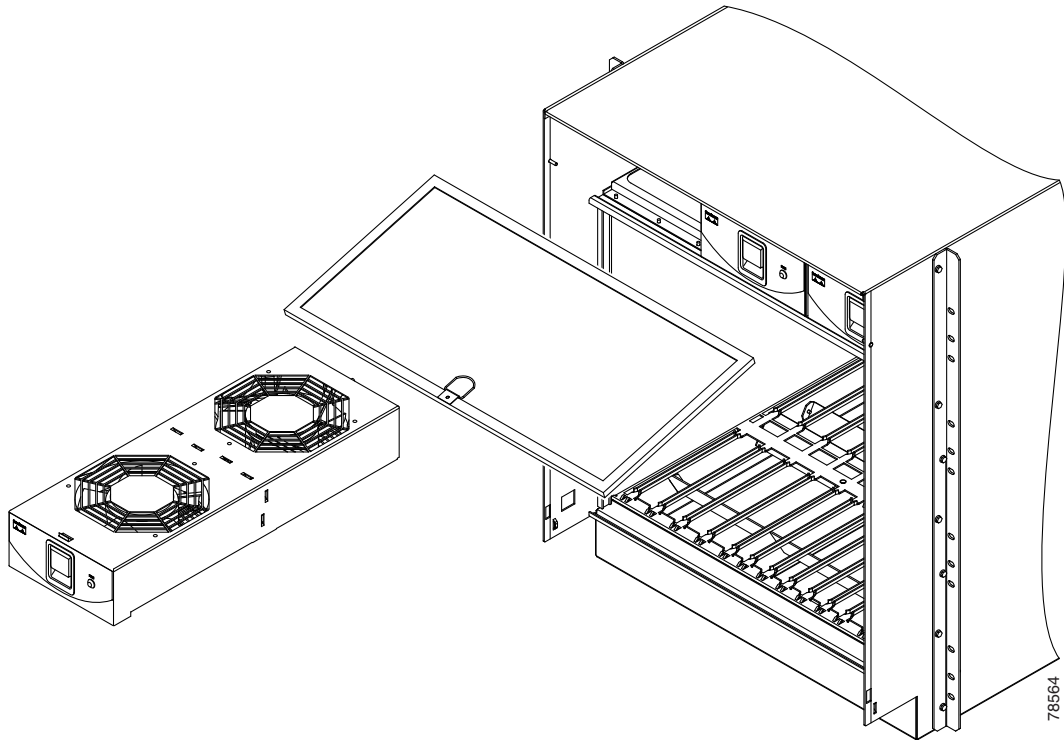


## 1.10.2 Fan Speed and Failure

If one or more fans fail on the fan-tray assembly, replace the fan tray where that fan resides. You cannot replace individual fans. The red FAN LED on the front of the fan tray turns on when one or more fans fail. For fan-tray replacement instructions, refer to the *Cisco ONS 15600 SDH Procedure Guide*. The red FAN LED clears after you install a working fan tray.

⚠

**Caution**      If both fans in the center fan tray are inoperative, you must replace the fan tray within five minutes of failure to avoid affecting traffic because CTC software will shut down one of the SSXC cards.

⚠

**Caution**      The ONS 15600 SDH requires at least one working fan in each of the three fan trays. When a single fan in a tray fails, Cisco recommends replacing the tray with a fully working tray as soon as possible.

✎

**Note**      Each fan tray contains two fans. The FAN LED indicates if one or both fans fail in that fan tray.

Fan speed is determined by card temperature sensors that report temperature data to the active TSC card. The sensors measure the input and output air temperature for each card. Fan speed options are low, medium, and high. For example, if a card exceeds permissible operational temperature, the fan speed

increases appropriately. At initial turn-up, the default fan speed is high until the node initializes. If both TSC cards fail, the fans automatically shift to high speed. If a single TSC card fails, the active TSC card will still control the fan speed. Table 1-1 shows the power requirements for an individual fan in a fan tray.

*Table 1-1       Power Requirements for an Individual Fan*

| Condition | Watts | Amps | BTU/Hr. |
|---|---|---|---|
| Min at 48 V (ambient temperature less than 25 degrees C) | 12 | 0.25 | 41 |
| Max at 48 V (ambient temperature greater than 25 degrees C) | 46 | 0.95 | 157 |

# 1.11  Cards and Slots

When a card is inserted in a card slot, it will contact the shelf backplane but is not fully installed until the ejectors are fully closed.

## 1.11.1  Card Slot Requirements

The ONS 15600 SDH shelf has 14 card slots numbered sequentially from left to right. Slots 1 to 4 and 11 to 14 are reserved for optical (STM-N) traffic cards. These slots can host any of the ONS 15600 SDH optical cards. Slots 6/7 and 8/9 are dedicated to SSXC cards, and Slots 5 and 10 house the TSC cards. Each card is keyed to fit only in an appropriate slot for that card. Unused card slots should be occupied by a filler card (blank faceplate).

⚠

**Caution**      Do not operate the ONS 15600 SDH with a single TSC card or a single SSXC card installed. Always operate the shelf with one active and one redundant standby TSC card and two SSXC cards.

Shelf assembly slots have symbols indicating the type of cards that you can install in them. Each ONS 15600 SDH card has a corresponding symbol. The symbol on the card must match the symbol on the slot.

Table 1-2 shows the slot and card symbol definitions.

*Table 1-2       Slot and Card Symbols*

| Symbol Color/Shape | Definition |
|---|---|
| Orange/Circle | Any traffic card (STM-16, STM-64, ASAP) |
| Purple/Square | TSC slot; only install ONS 15600 SDH cards with a square symbol on the faceplate |
| Green/Cross | SSXC slot; only install ONS 15600 SDH cards with a cross symbol on the faceplate |

Refer to Chapter 2, "Card Reference," for more information about ONS 15600 SDH cards.

All physical connections to the optical cards are made through OGI connectors on the card faceplate. Table 1-3 lists the number of ports and the line rates for ONS 15600 SDH optical cards.

*Table 1-3*          ***Optical Card Ports and Line Rates***

| Card | Ports | Line Rate per Port |
|------|-------|--------------------|
| OC48/STM16 LR/LH 16 Port 1550; OC48/STM16 SR/SH 16 Port 1310 | 4 physical interfaces; 4 ports per interface, totalling 16 STM-16 ports per card | 2488.32 Mbps (VC4-16c) |
| OC192/STM64 LR/LH 4 Port 1550; OC192/STM64 SR/SH 4 Port 1310 | 4 physical interfaces; 1 port per interface, totalling four STM-64 ports per card | 9.95 Gbps (VC4-64c) |
| Any-Service Any-Port (ASAP) card (STM-1, STM-3, STM-16, STM-64, or Gigabit Ethernet) | 4 physical interfaces; 1 to 4 ports per interface, depending on the Pluggable Input/Output Module used; totalling a maximum of four STM-64 ports per card | Up to 9.95 Gbps (VC4-64c) |

# 1.11.2  OGI Cables

The ONS 15600 SDH faceplate has OGI connectors that terminate in either SC, ST, or FC connectors. Figure 1-14 shows the OGI to SC cable breakout for the STM-16 card.

*Figure 1-14*          ***OGI Cable Breakout***
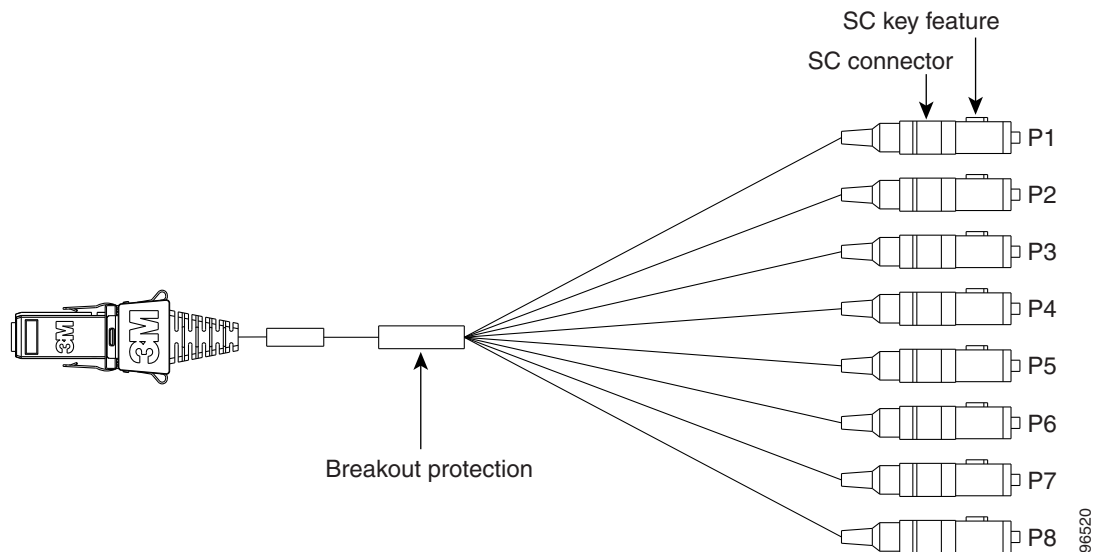


Figure 1-15 show the OGI pin breakout for the STM-16 card.

*Figure 1-15      OGI Pin Breakout*
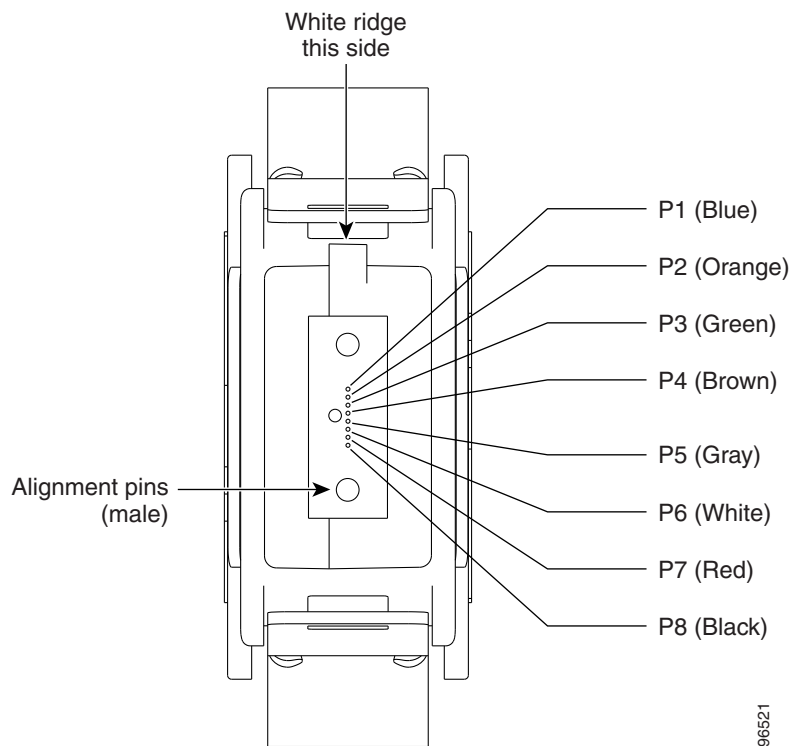


## 1.11.3 Optical Card Cable Routing

The ONS 15600 SDH has a cable-management tray with discrete fiber routing paths for each optical card's cables. Each fiber routing path has a plastic cable latch for securing the cables in the fiber routing path. You can rotate the cable latch into two positions, open or closed; make sure that the cable latch is always completely open before you insert or remove the optical cables. Make sure all fiber-optic cables are disconnected from a card before you remove it.

## 1.11.4 Card Replacement

To replace an ONS 15600 SDH card with another card of the same type, you do not need to make any changes to the database; remove the old card and replace it with a new card. You can use the CTC Change Card feature to replace a card with a new card while maintaining all existing provisioning. To replace a card with a card of a different type, delete the original card from CTC, physically remove the card, and replace it with the new card.

⚠

**Caution**    Removing any active/working card from the ONS 15600 SDH can result in traffic interruption. Use caution when replacing cards and verify that only inactive or standby cards are being replaced. If the active card needs to be replaced, switch it to standby prior to removing the card from the node.

**Note** An improper removal (IMPROPRMVL) alarm is raised whenever a card pull is performed, unless the card is deleted in CTC first. The alarm will clear after the card replacement is complete. If the alarm does not clear, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15600 SDH Troubleshooting Guide*.

**C H A P T E R 2**

# Card Reference

This chapter describes Cisco ONS 15600 SDH card features and functions.

Chapter topics include:

## 2.1  Card Overview

⚠

**Caution**    When working with cards, wear the supplied ESD wristband to avoid ESD damage to the card. Plug the wristband cable into the ESD jack located on the lower-left outside edge of the shelf assembly.

### 2.1.1  Card Summary

Table 2-1 lists the ONS 15600 SDH cards and provides a short description and cross-reference to each.

*Table 2-1        ONS 15600 SDH Cards and Descriptions*

| Card | Description | For Additional Information... |
|------|-------------|-------------------------------|
| TSC | The TSC card performs all system-timing functions for each ONS 15600 SDH. | See the "2.2  TSC Card" section on page 2-3. |
| SSXC | The SSXC card is the central cross-connect element for ONS 15600 SDH switching. | See the "2.3  SSXC Card" section on page 2-6. |

*Table 2-1* ***ONS 15600 SDH Cards and Descriptions (continued)***

| Card | Description | For Additional Information... |
|------|-------------|-------------------------------|
| **OC48/STM16 LR/LH 16 Port 1550** | The OC48/STM16 LR/LH 16 Port 1550 card provides 16 long-range, Telcordia GR-253-CORE compliant, SDH STM-16 ports per card. | See the "2.4 OC48/STM16 LR/LH 16 Port 1550 Card" section on page 2-8. |
| **OC48/STM16 SR/SH 16 Port 1310** | The OC48/STM16 SR/SH 16 Port 1310 card provides 16 short-range, Telcordia GR-253-CORE compliant, SDH STM-16 ports per card. | See the "2.5 OC48/STM16 SR/SH 16 Port 1310 Card" section on page 2-11. |
| **OC192/STM64 LR/LH 4 port 1550** | The OC192/STM64 LR/LH 4 port 1550 card provides four long-range, Telcordia GR-253-CORE compliant, SDH STM-64 ports per card. | See the "2.6 OC192/STM64 LR/LH 4 Port 1550 Card" section on page 2-14. |
| **OC192/STM64 SR/SH 4 Port 1310** | The OC192/STM64 SR/SH 4 Port 1310 card provides four short-range, Telcordia GR-253-CORE compliant, SDH STM-64 ports per card. | See the "2.7 OC192/STM64 SR/SH 4 Port 1310 Card" section on page 2-17. |
| **ASAP** | The Any-Service Any-Port (ASAP) card provides up to 16 Telcordia GR-253-CORE compliant, SDH STM-1, STM-4, STM-16, STM-64, or Gigabit Ethernet ports per card, with certain limitations on line rate combinations. | See the "2.8 ASAP Card" section on page 2-19. |
| **Filler** | The filler card is used to fill unused optical (STM-N) traffic card slots in the ONS 15600 SDH shelf. | See the "2.9 Filler Card" section on page 2-25. |

## 2.1.2 Card Compatibility

Table 2-2 lists Cisco Transport Controller (CTC) software release compatibility for each card. In Table 2-2, "Yes" means the cards are compatible with the listed software versions. Table cells with dashes mean cards are not compatible with the listed software versions.

.

*Table 2-2* ***ONS 15600 SDH Software Release Compatibility Per Card***

| Card | R1.0 | R1.x.x | R5.0 | R6.0 | R7.0 | R7.2 | R8.0 |
|------|------|--------|------|------|------|------|------|
| **TSC** | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| **CXC** | Yes | Yes | — | — | — | — | — |
| **SSXC** | — | — | Yes | Yes | Yes | Yes | Yes |

**Table 2-2        ONS 15600 SDH Software Release Compatibility (continued)Per Card**

| Card | R1.0 | R1.x.x | R5.0 | R6.0 | R7.0 | R7.2 | R8.0 |
|---|---|---|---|---|---|---|---|
| OC48/STM16 LR/LH 16 Port 1550 | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| OC48/STM16 SR/SH 16 Port 1310 | — | Yes | Yes | Yes | Yes | Yes | Yes |
| OC192/STM64 LR/LH 4 Port 1550 | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| OC192/STM64 SR/SH 4 Port 1310 | — | Yes | Yes | Yes | Yes | Yes | Yes |
| OC192/STM64 4 Port ITU C-Band | — | — | — | — | — | — | Yes |
| ASAP | — | — | Yes[1] | Yes | Yes | Yes | Yes |

1. The ASAP card is compatible with the R5.xx maintenance release

# 2.2  TSC Card

**Note**    For hardware specifications, see the "A.2.1  TSC Card Specifications" section on page A-5.

**Caution**    Do not operate the ONS 15600 SDH with an unprotected, single TSC card or a single SSXC card installed. Always operate the shelf with one active card and one protect card for each of these control cards.

The TSC card performs all system-timing functions for each ONS 15600 SDH. The TSC card monitors the recovered clocks from each traffic card and two building integrated timing supply (BITS) interfaces for frequency accuracy. The TSC card is provisionable, allowing timing from any optical interface source, a BITS input source, or the internal Stratum 3E as the system-timing reference. You can provision any of the clock inputs as primary or secondary timing sources. If you specify external timing references, your options are BITS1, BITS2, and the internal Stratum 3E sources. If you select line timing, you can specify up to two line ports from which to derive timing, as well as the internal stratum 3E sources. The TSC card also supports BITS OUT. A slow-reference tracking loop allows the TSC to synchronize with the recovered clock and enables holdover if the reference is lost.

The TSC card also provides shelf control related functions. The TSC card has a 100-Mbps Ethernet link to each card on the shelf and monitors the presence of these cards. The TSC provides bulk memory for nonvolatile storage of system software and data and provides EIA-TIA 232 and Ethernet customer interfaces. The TSC card processes and routes RS-DCC and MS-DCC traffic as well as routing the K1, K2, and K3 overhead bytes between traffic (line) cards and SSXC cards. The TSC card controls and monitors the shelf fans and all of the alarm interfaces.

## 2.2.1  TSC Slots and Connectors

Install TSC cards in Slots 5 and 10 for redundancy. If the active TSC card fails, timing reference and control function switches to the protect TSC card.

**Note**    All TSC card protection switches conform to the Telcordia protection switching standard of equal to or less than 50 ms.

The TSC card has an RJ-45 10/100 Base-T LAN port on the faceplate. Two additional RJ-45 10/100 Base-T LAN ports and two EIA/TIA-232 DB-9 type craft user interfaces are available on the Customer Access Panel (CAP/CAP2) on the backplane.

## 2.2.2 TSC Faceplate and Block Diagram

Figure 2-1 shows the TSC card faceplate and a block diagram of the card.

*Figure 2-1*        *TSC Card Faceplate and Block Diagram*
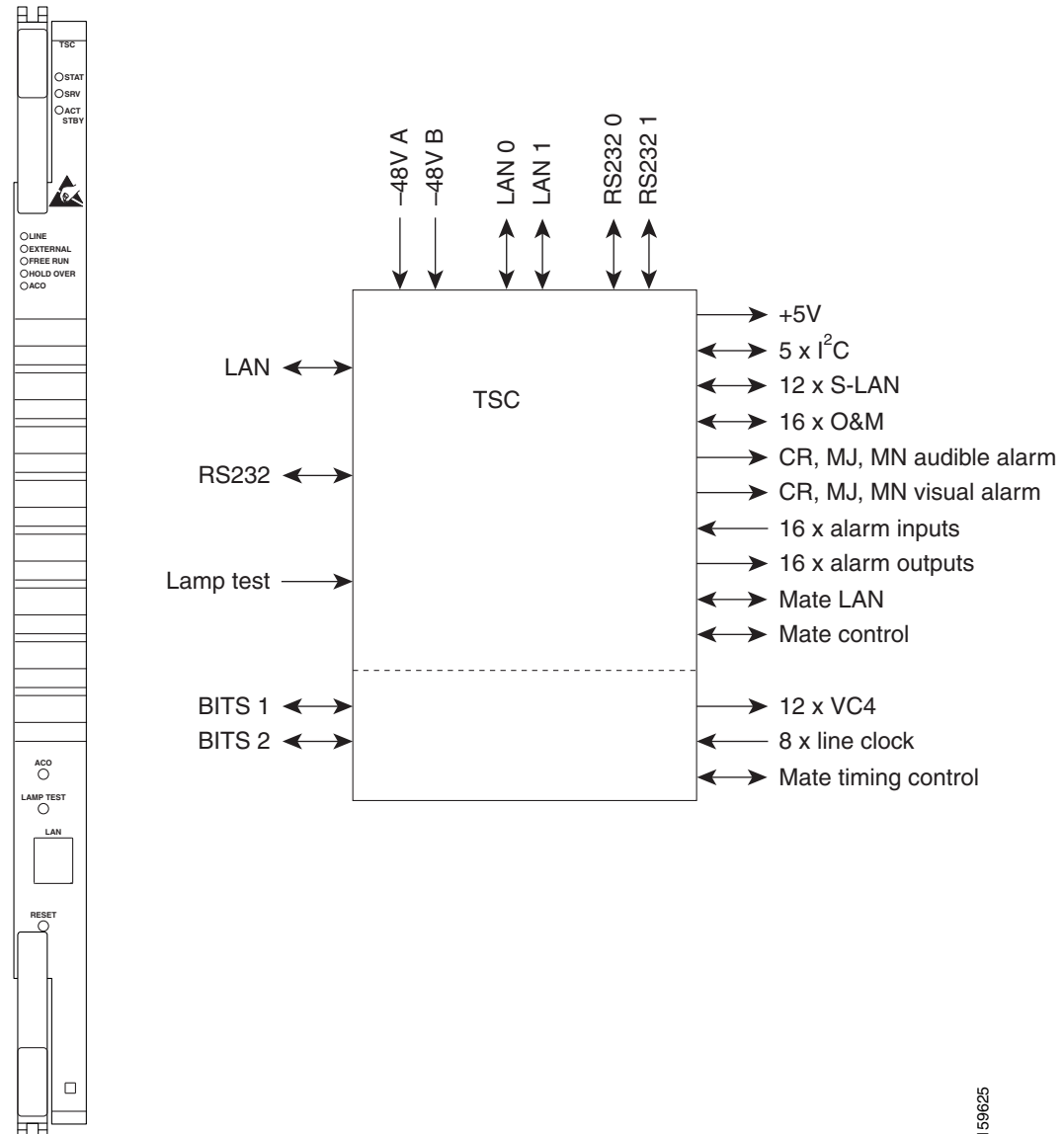
## 2.2.3  TSC Card-Level Indicators

Table 2-3 describes the functions of the card-level LEDs on the TSC card faceplate.

*Table 2-3*        *TSC Card-Level Indicators*

| Indicator | Color | Definition |
|-----------|-------|------------|
| **STAT** | Red | Indicates a hardware fault; this LED is off during normal operation. Replace the card if the STAT LED persists. During diagnostics, the LED flashes quickly during initialization and slowly during configuration synchronization. |
| **SRV** | Green | The service mode of the card. Green indicates that the card is in use, amber indicates that the card is out of service, and off indicates that the card is either booting or has no power applied. |
| **ACT/STBY** | Green | The ACT/STBY (Active/Standby) LED indicates that the TSC is active (green) or standby (off). |

## 2.2.4  TSC Network-Level Indicators

Table 2-4 describes the functions of the network-level LEDs on the TSC card faceplate.

*Table 2-4*        *TSC Network-Level Indicators*

| Indicator | Color | Definition |
|-----------|-------|------------|
| **LINE** | Green | Node timing is synchronized to a line timing reference. |
| **EXTERNAL** | Green | Node timing is synchronized to an external timing reference. |
| **FREE RUN** | Green | Node is not using an external timing reference. Indicated when the timing mode is set to an internal reference or after all external references are lost. |
| **HOLDOVER** | Amber | External/line timing references have failed. The TSC has switched to internal timing and the 24-hour holdover period has not elapsed. |
| **ACO** | Amber | The alarm cutoff (ACO) push button has been activated. After pressing the ACO button, the amber ACO LED turns on. The ACO button opens the audible closure on the backplane. The ACO state is stopped if a new alarm occurs. After the originating alarm is cleared, the ACO LED and audible alarm control are reset. |

## 2.2.5 TSC Push-Button Switches

Table 2-5 describes the functions of the push-button switches on the TSC card faceplate.

*Table 2-5        TSC Card Push-Button Switches*

| Push-Button | Function |
|---|---|
| ACO | Extinguishes external audible (environmental) alarms. When this button is activated, the amber-colored ACO LED turns on. |
| LAMP TEST | Verifies that all the LEDs in the shelf are functioning properly. When this button is activated, all of the front-panel LEDs in the shelf turn on temporarily to verify operation. |
| RESET | Activates a soft reset of all of the main processor memory on the card.<br><br>**Note**     The RESET button is recessed to prevent accidental activation. |

# 2.3 SSXC Card

**Note**     For hardware specifications, see the "A.2.2  SSXC Specifications" section on page A-6.

The SSXC is the central element for ONS 15600 SDH switching. The SSXC card establishes connections and performs time division switching (TDS) at VC3 and VC4-Nc levels between ONS 15600 SDH traffic cards.

The SSXC card works with the TSC card to maintain connections and set up cross-connects within the ONS 15600 SDH. You establish cross-connect and provisioning information using CTC or TL1. The TSC card stores the proper internal cross-connect information and relays the setup information to the SSXC card.

## 2.3.1 SSXC Switch Matrix

The switch matrix on each SSXC card consists of 6,144 bidirectional VC3 ports, with a maximum of 6,144 bidirectional VC3 cross-connections. When creating bidirectional VC3 cross-connects, each bidirectional cross-connect uses two VC3 ports, with the result that the SSXC card supports 3,072 bidirectional VC3 cross-connects. Any VC3 on any port can be connected to any other port, meaning that the STS cross-connections are nonblocking. Nonblocking connections allow network operators to connect any VC3, VC4, VC4-4c, VC4-8c, VC4-16c, or VC4-64c payload that is received on an STM-16 or STM-64 interface (or additionally any VC4-2c and/or VC4-3c payload that is received on an ASAP interface) to any other interface capable of supporting the bandwidth.

The SSXC card has 128 input ports and 128 output ports capable of VC4-16c. A VC3 on any of the input ports can be mapped to an VC3 output port, thus providing full VC3 time slot assignments (TSAs).

## 2.3.2 SSXC Slots and Connectors

Install an SSXC card in Slot 6 and a second SSXC card in Slot 8 for redundancy. (Slots 7 and 9 are also occupied by the SSXC faceplates.) The SSXC card has no external interfaces. All SSXC card interfaces are provided on the ONS 15600 SDH backplane.

## 2.3.3 SSXC Faceplate and Block Diagram

Figure 2-2 shows the SSXC card faceplate and a block diagram of the card.

*Figure 2-2*        *SSXC Card Faceplate and Block Diagram*
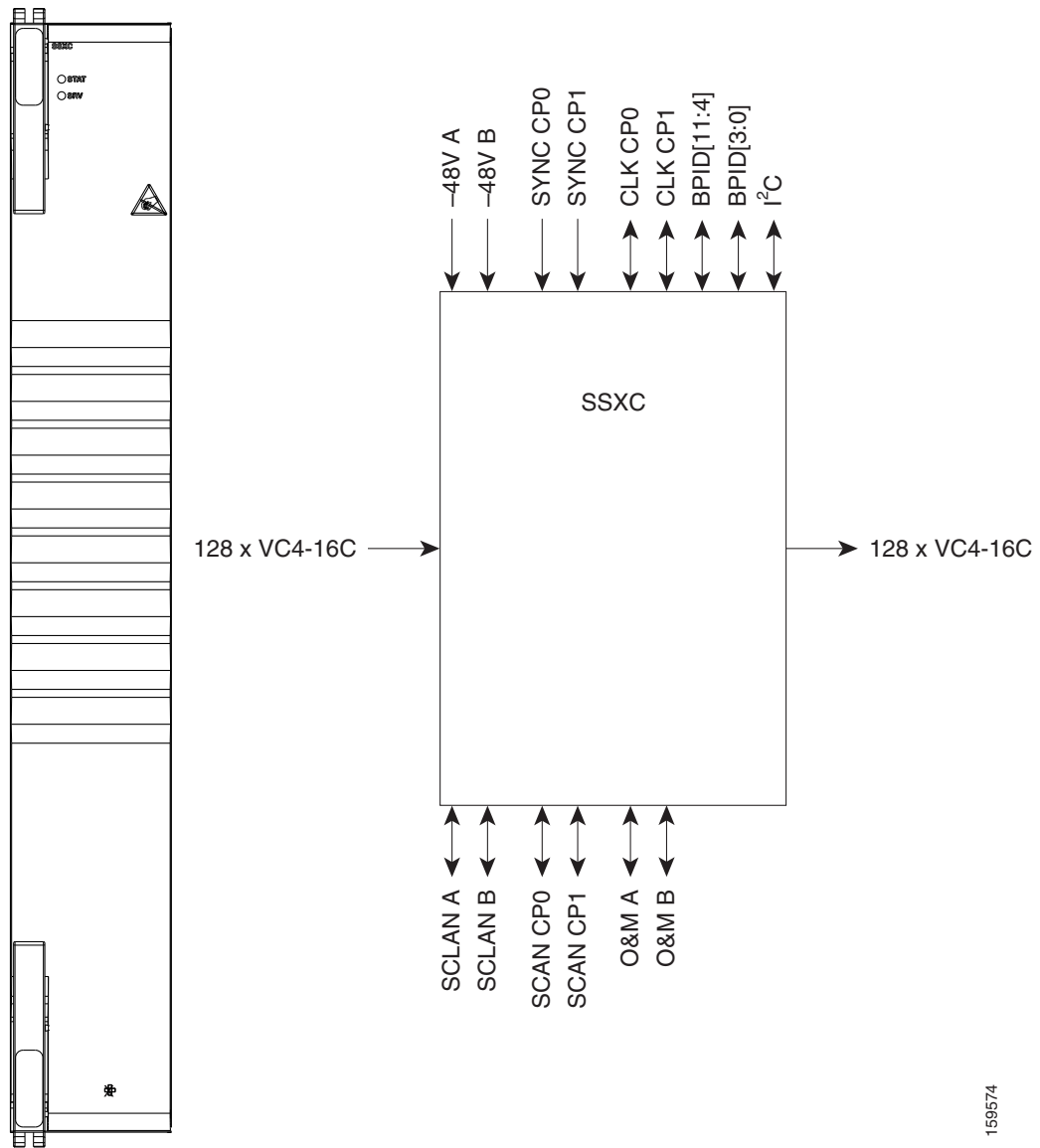
## 2.3.4  SSXC Card-Level Indicators

Table 2-6 describes the functions of the card-level LEDs on the SSXC card faceplate.

*Table 2-6*  **SSXC Card-Level Indicators**

| Indicator | Color | Definition |
|-----------|-------|------------|
| **STAT** | Red | Indicates a hardware fault; this LED is off during normal operation. Replace the card if the STAT LED persists. During diagnostics, the LED flashes quickly during initialization and slowly during configuration synchronization. |
| **SRV** | Green | The service mode of the card. Green indicates the card is in use; off indicates that the card can be removed for service. |
|  | Amber | The service mode of the card. Amber indicates the card is in use; off indicates that the card can be removed for service. |

# 2.4  OC48/STM16 LR/LH 16 Port 1550 Card

**Note**  For card specifications, see the "A.2.3  OC48/STM16 LR/LH 16 Port 1550 Specifications" section on page A-6.

The OC48/STM16 LR/LH 16 Port 1550 card provides 16 long-range, Telcordia GR-253-CORE compliant, SDH STM-16 ports per card. The ports operate at 2488.320 Mbps over a single-mode fiber span. The OC48/STM16 LR/LH 16 Port 1550 card has four physical connector adapters with eight fibers per connector adapter. The card supports VC3 payloads and concatenated payloads at VC4, VC4-4c, VC4-8c, or VC4-16c signal levels.

## 2.4.1  OC48/STM16 LR/LH 16 Port 1550 Slots and Connectors

You can install OC48/STM16 LR/LH 16 Port 1550 cards in Slots 1 through 4 and 11 through 14. The card provides four bidirectional OGI-type connector adapters on the faceplate (angled downward), each carrying eight fiber strands (four transmit and four receive).

## 2.4.2 OC48/STM16 LR/LH 16 Port 1550 Faceplate and Block Diagram

Figure 2-3 shows the OC48/STM16 LR/LH 16 Port 1550 faceplate and a block diagram of the card.

**Figure 2-3** *OC48/STM16 LR/LH 16 Port 1550 Faceplate and Block Diagram*
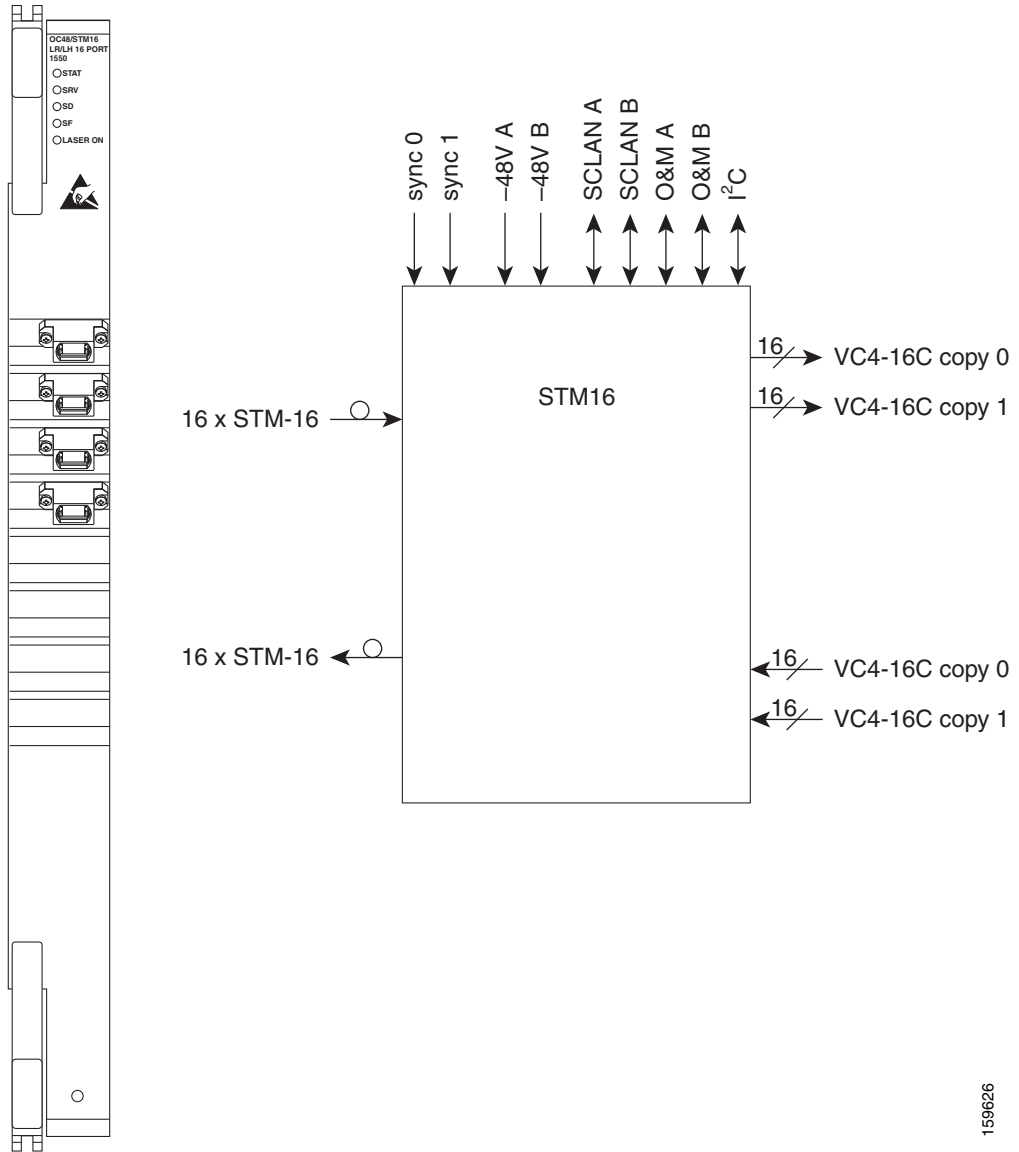
## 2.4.3 OC48/STM16 LR/LH 16 Port 1550 Card-Level Indicators

Table 2-7 describes the functions of the card-level LEDs on the OC48/STM16 LR/LH 16 Port 1550 card.

*Table 2-7*      *OC48/STM16 LR/LH 16 Port 1550 Card-Level Indicators*

| Indicator | Color | Description |
|-----------|-------|-------------|
| **STAT LED** | Red | Indicates a hardware fault; this LED is off during normal operation. Replace the card if the STAT LED persists. During diagnostics, the LED flashes quickly during initialization and slowly during configuration synchronization. |
| **SRV LED** | Green | The service mode of the card. Green indicates that the card is in use, amber indicates that the card is out of service, and off indicates that the card is either booting or has no power applied. |
| **LASER ON** | Green | The green LASER ON LED indicates that at least one of the card's lasers is active. |

## 2.4.4 OC48/STM16 LR/LH 16 Port 1550 Network-Level Indicators

Table 2-8 describes the functions of the network-level LEDs on the OC48/STM16 LR/LH 16 Port 1550 card.

*Table 2-8*      *OC48/STM16 LR/LH 16 Port 1550 Network-Level Indicators*

| Indicator | Color | Description |
|-----------|-------|-------------|
| **SD LED** | Blue | The blue SD LED indicates a signal degrade (SD) or condition such as a low level signal on one or more of the card's ports. |
| **SF LED** | Red | The red SF LED indicates a signal failure (SF) or condition such as loss of signal (LOS), loss of frame alignment (LOF), or turns on when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the LED turns off. |

## 2.4.5 OC48/STM16 LR/LH 16 Port 1550 Card OGI Connector Pinout

Table 2-9 lists the OC48/STM16 LR/LH 16 Port 1550 card OGI connector pinouts.

*Table 2-9*      *OC48/STM16 LR/LH 16 Port 1550 Card OGI Connector Pinout*

| Connector | OGI Pin and Card Port | | | | | | | |
|-----------|-----|-----|-----|-----|-----|-----|-----|-----|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | Transmit 4 | Receive 4 | Transmit 3 | Receive 3 | Transmit 2 | Receive 2 | Transmit 1 | Receive 1 |
| 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | Transmit 8 | Receive 8 | Transmit 7 | Receive 7 | Transmit 6 | Receive 6 | Transmit 5 | Receive 5 |
| 3 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | Transmit 12 | Receive 12 | Transmit 11 | Receive 11 | Transmit 10 | Receive 10 | Transmit 9 | Receive 9 |

**Table 2-9**    *OC48/STM16 LR/LH 16 Port 1550 Card OGI Connector Pinout (continued)*

| Connector | OGI Pin and Card Port | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | Transmit 16 | Receive 16 | Transmit 15 | Receive 15 | Transmit 14 | Receive 14 | Transmit 13 | Receive 13 |

# 2.5  OC48/STM16 SR/SH 16 Port 1310 Card

**Note**    For card specifications, see the "A.2.4  OC48/STM16 SR/SH 16 Port 1310 Specifications" section on page A-8.

The OC48/STM16 SR/SH 16 Port 1310 card provides 16 short-range, Telcordia GR-253-CORE compliant, SDH STM-16 ports per card. The ports operate at 2488.320 Mbps over a single-mode fiber span. The OC48/STM16 SR/SH 16 Port 1310 card has four physical connector adapters with eight fibers per connector adapter. The card supports VC3 payloads and concatenated payloads at VC4, VC4-4c, VC4-8c, or VC4-16c signal levels.

## 2.5.1  OC48/STM16 SR/SH 16 Port 1310 Slots and Connectors

You can install OC48/STM16 SR/SH 16 Port 1310 cards in Slots 1 through 4 and 11 through 14. The card provides four bidirectional OGI-type connector adapters on the faceplate (angled downward), each carrying eight fiber strands (four transmit and four receive).

# 2.5.2 OC48/STM16 SR/SH 16 Port 1310 Faceplate and Block Diagram

Figure 2-4 shows the OC48/STM16 SR/SH 16 Port 1310 faceplate and block diagram.

*Figure 2-4*      *OC48/STM16 SR/SH 16 Port 1310 Faceplate and Block Diagram*
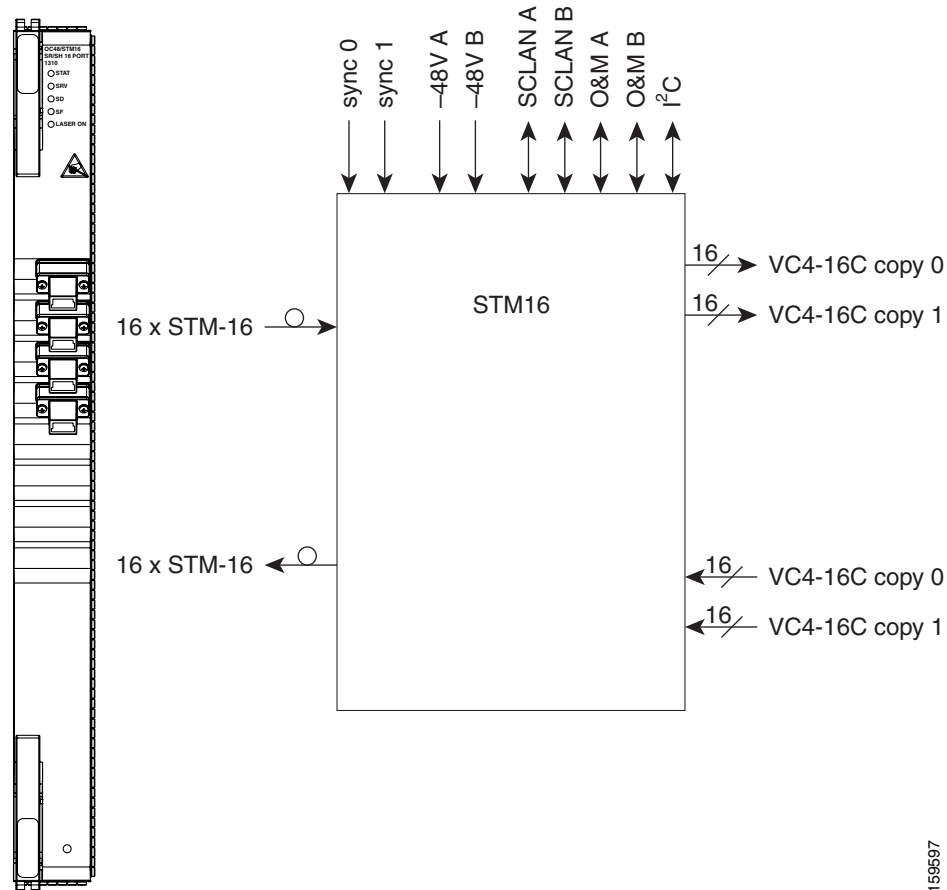


# 2.5.3 OC48/STM16 SR/SH 16 Port 1310 Card-Level Indicators

Table 2-10 describes the functions of the card-level LEDs on the OC48/STM16 SR/SH 16 Port 1310 card.

*Table 2-10*      *OC48/STM16 SR/SH 16 Port 1310 Card-Level Indicators*

| Indicator | Color | Description |
|---|---|---|
| **STAT LED** | Red | Indicates a hardware fault; this LED is off during normal operation. Replace the card if the STAT LED persists. During diagnostics, the LED flashes quickly during initialization and slowly during configuration synchronization. |

*Table 2-10        OC48/STM16 SR/SH 16 Port 1310 Card-Level Indicators (continued)*

| Indicator | Color | Description |
|---|---|---|
| **SRV LED** | Green | The service mode of the card. Green indicates that the card is in use, amber indicates that the card is out of service, and off indicates that the card is either booting or has no power applied. |
| **LASER ON** | Green | The green LASER ON LED indicates that at least one of the card's lasers is active. |

## 2.5.4  OC48/STM16 SR/SH 16 Port 1310 Network-Level Indicators

Table 2-11 describes the functions of the network-level LEDs on the OC48/STM16 SR/SH 16 Port 1310 card.

*Table 2-11        OC48/STM16 SR/SH 16 Port 1310 Network-Level Indicators*

| Indicator | Color | Description |
|---|---|---|
| **SD LED** | Blue | The blue SD LED indicates a SD or condition such as a low signal level on one or more of the card's ports. |
| **SF LED** | Red | The red SF LED indicates a signal failure or condition such as LOS, LOF, or high bit error rate (BER) on one or more of the card's ports. The red SF LED also turns on when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the LED turns off. |

## 2.5.5  OC48/STM16 SR/SH 16 Port 1310 Card OGI Connector Pinout

Table 2-12 lists the OC48/STM16 SR/SH card OGI connector pinouts.

*Table 2-12        OC48/STM16 SR/SH 16 Port 1310 Card OGI Connector Pinout*

| Connector | OGI Pin and Card Port | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | Transmit 4 | Receive 4 | Transmit 3 | Receive 3 | Transmit 2 | Receive 2 | Transmit 1 | Receive 1 |
| 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | Transmit 8 | Receive 8 | Transmit 7 | Receive 7 | Transmit 6 | Receive 6 | Transmit 5 | Receive 5 |
| 3 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | Transmit 12 | Receive 12 | Transmit 11 | Receive 11 | Transmit 10 | Receive 10 | Transmit 9 | Receive 9 |
| 4 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | Transmit 16 | Receive 16 | Transmit 15 | Receive 15 | Transmit 14 | Receive 14 | Transmit 13 | Receive 13 |

# 2.6 OC192/STM64 LR/LH 4 Port 1550 Card

**Note** For card specifications, see the "A.2.5 OC192/STM64 LR/LH 4 Port 1550 Specifications" section on page A-9.

The OC192/STM64 LR/LH 4 port 1550 card provides four long-range, Telcordia GR-253-CORE compliant, SDH STM-64 ports per card. The ports operate at 9953.28 Mbps over a single-mode fiber. The OC192/STM64 LR/LH 4 port 1550 card has four physical connector adapters with two fibers per connector adapter. The card supports VC3 payloads and concatenated payloads at VC4, VC4-4c, VC4-8c, VC4-16c, or VC4-64c signal levels.

## 2.6.1 OC192/STM64 LR/LH 4 Port 1550 Slots and Connectors

You can install OC192/STM64 LR/LH 4 port 1550 cards in Slots 1 through 4 and 11 through 14. The card provides four bidirectional OGI-type connector adapters on the faceplate (angled downward), carrying two fiber strands (one transmit and one receive). Only one transmit and receive pair is used per connector adapter. On a breakout cable, use port three, fiber 4 (transmit) and fiber 3 (receive).

## 2.6.2 OC192/STM64 LR/LH 4 Port 1550 Faceplate and Block Diagram

Figure 2-5 shows the OC192/STM64 LR/LH 4 Port 1550 faceplate and a block diagram of the card.

**Figure 2-5** *OC192/STM64 LR/LH 4 Port 1550 Faceplate and Block Diagram*
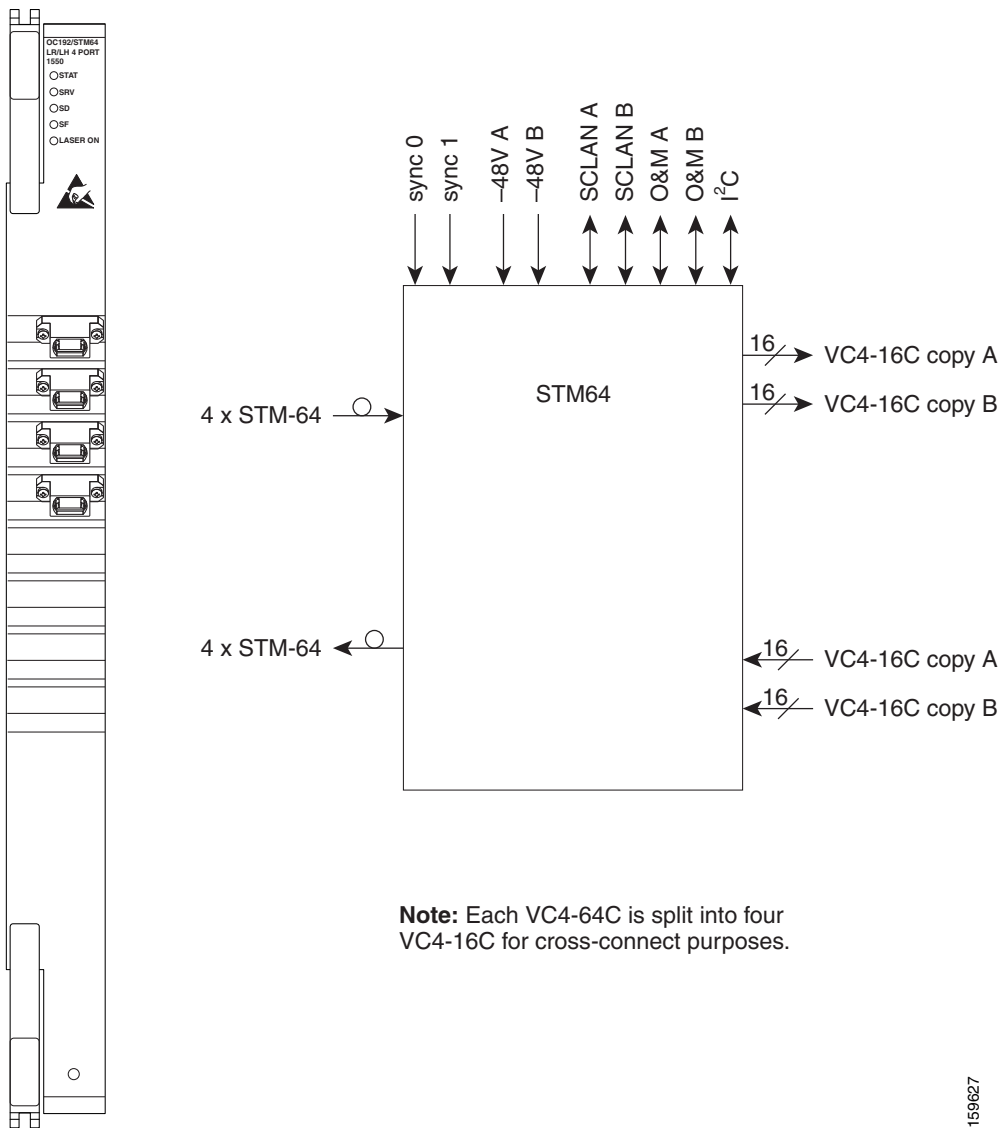
## 2.6.3  OC192/STM64 LR/LH 4 Port 1550 Card-Level Indicators

Table 2-13 describes the functions of the card-level LEDs on the OC192/STM64 LR/LH 4 Port 1550 card.

*Table 2-13      OC192/STM64 LR/LH 4 Port 1550 Card-Level Indicators*

| Indicator | Color | Description |
|---|---|---|
| **STAT LED** | Red | Indicates a hardware fault; this LED is off during normal operation. Replace the unit if the STAT LED persists. During diagnostics, the LED flashes quickly during initialization and slowly during configuration synchronization. |
| **SRV LED** | Green | The service mode of the card. Green indicates that the card is in use, amber indicates that the card is out of service, and off indicates that the card is either booting or has no power applied. |
| **LASER ON** | Green | The green LASER ON LED indicates that at least one of the card's lasers is active. |

## 2.6.4  OC192/STM64 LR/LH 4 Port 1550 Network-Level Indicators

Table 2-14 describes the functions of the network-level LEDs on the OC192/STM64 LR/LH 4 Port 1550 card.

*Table 2-14      OC192/STM64 LR/LH 4 Port 1550 Network-Level Indicators*

| Indicator | Color | Description |
|---|---|---|
| **SD LED** | Blue | The blue SD LED indicates a signal degrade or condition such as a low signal level on one or more of the card's ports. |
| **SF LED** | Red | The red SF LED indicates a signal failure or condition such as LOS, LOF, or high BER on one or more of the card's ports. The red SF LED is also on when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the LED turns off. |

## 2.6.5  OC192/STM64 LR/LH 4 Port 1550 Card OGI Connector Pinout

Table 2-15 lists the OC192/STM64 LR/LH 4 Port 1550 card OGI connector pinouts.

*Table 2-15      OC192/STM64 LR/LH 4 Port 1550 Card OGI Connector Pinout*

| Connector | OGI Pin and Card Port | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  | — | — | Transmit 1 | Receive 1 | — | — | — | — |
| 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  | — | — | Transmit 2 | Receive 2 | — | — | — | — |
| 3 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  | — | — | Transmit 3 | Receive 3 | — | — | — | — |

**Table 2-15** *OC192/STM64 LR/LH 4 Port 1550 Card OGI Connector Pinout (continued)*

| Connector | OGI Pin and Card Port | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | — | — | Transmit 4 | Receive 4 | — | — | — | — |

# 2.7 OC192/STM64 SR/SH 4 Port 1310 Card

**Note** For card specifications, see the "A.2.6 OC192/STM64 SR/SH 4 Port 1310 Specifications" section on page A-10.

The OC192/STM64 SR/SH 4 Port 1310 card provides four short-range, Telcordia GR-253-CORE compliant, SDH STM-64 ports per card. The ports operate at 9953.28 Mbps over a single-mode fiber. The OC192/STM64 SR/SH 4 port 1310 card has four physical connector adapters with two fibers per connector adapter. The card supports VC3 payloads and concatenated payloads at VC4, VC4-4c, VC4-8c, VC4-16c, or VC4-64c signal levels.

## 2.7.1 OC192/STM64 SR/SH 4 Port 1310 Slots and Connectors

You can install OC192/STM64 SR/SH 4 Port 1310 cards in Slots 1 through 4 and 11 through 14. The card provides four bidirectional OGI-type connector adapters on the faceplate (angled downward), carrying two fiber strands (one transmit and one receive). Only one transmit and receive pair is used per connector adapter. On a breakout cable, use port three, fiber 4 (transmit) and fiber 3 (receive).

## 2.7.2  OC192/STM64 SR/SH 4 Port 1310 Faceplate and Block Diagram

Figure 2-6 shows the OC192/STM64 SR/SH 4 Port 1310 faceplate and block diagram.

*Figure 2-6*        *OC192/STM64 SR/SH 4 Port 1310 Faceplate and Block Diagram*



**Note:** Each VC4-64C is split into four VC4-16C for cross-connect purposes.
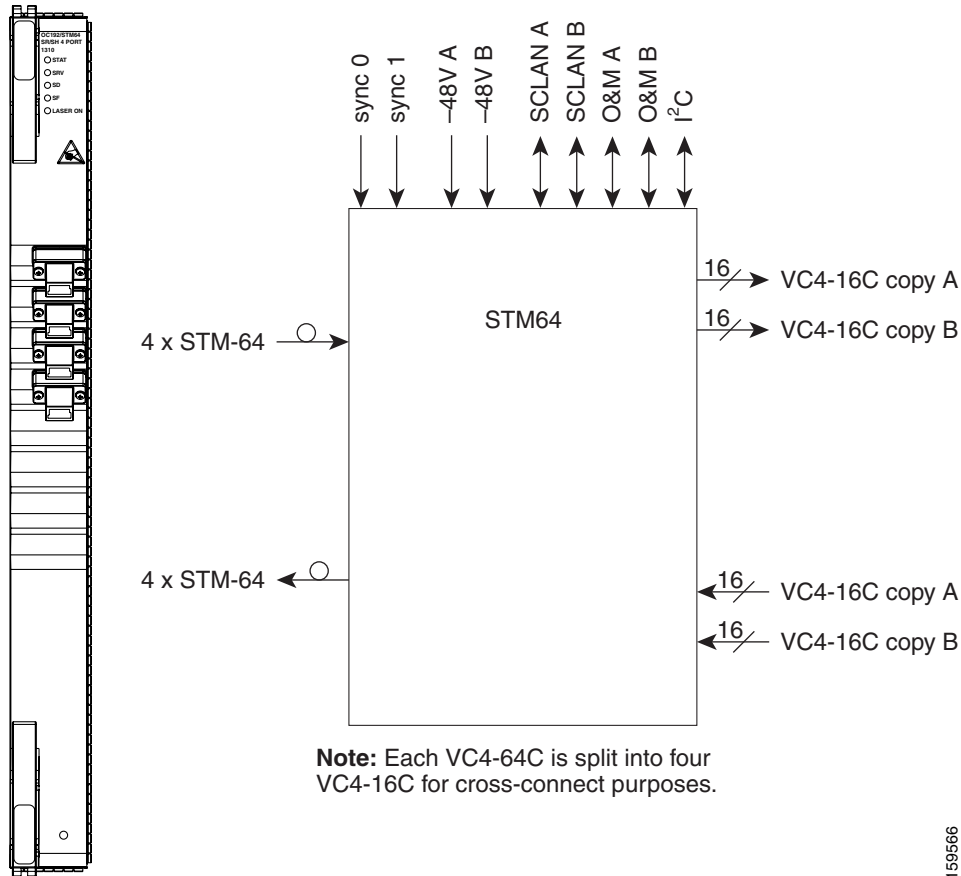
## 2.7.3  OC192/STM64 SR/SH 4 Port 1310 Card-Level Indicators

Table 2-16 describes the functions of the card-level LEDs on the OC192/STM64 SR/SH 4 Port 1310 card.

*Table 2-16*        *OC192/STM64 SR/SH 4 Port 1310 Card-Level Indicators*

| Indicator | Color | Description |
|---|---|---|
| **STAT LED** | Red | Indicates a hardware fault; this LED is off during normal operation. Replace the unit if the STAT LED persists. During diagnostics, the LED flashes quickly during initialization and slowly during configuration synchronization. |

*Table 2-16*      *OC192/STM64 SR/SH 4 Port 1310 Card-Level Indicators (continued)*

| Indicator | Color | Description |
|-----------|-------|-------------|
| **SRV LED** | Green | The service mode of the card. Green indicates that the card is in use, amber indicates that the card is out of service, and off indicates that the card is either booting or has no power applied. |
| **LASER ON** | Green | The green LASER ON LED indicates that at least one of the card's lasers is active. |

## 2.7.4 OC192/STM64 SR/SH 4 Port 1310 Card Network-Level Indicators

Table 2-17 describes the functions of the network-level LEDs on the OC192/STM64 SR/SH 4 Port 1310 card.

*Table 2-17*      *OC192/STM64 SR/SH 4 port 1310 Network-Level Indicators*

| Indicator | Color | Description |
|-----------|-------|-------------|
| **SD LED** | Blue | The blue SD LED indicates a signal degrade or condition such as a low signal level on one or more of the card's ports. |
| **SF LED** | Red | The red SF LED indicates a signal failure or condition such as LOS, LOF, or high BER on one or more of the card's ports. The red SF LED also turns on when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the LED turns off. |

## 2.7.5 OC192/STM64 SR/SH 4 Port 1310 Card OGI Connector Pinout

Table 2-18 lists the OC192/STM64 SR/SH 4 Port 1310 card OGI connector pinouts.

*Table 2-18*      *OC192/STM64 SR/SH 4 Port 1310 Card OGI Connector Pinout*

| Connector | OGI Pin and Card Port | | | | | | | |
|-----------|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|   | — | — | Transmit 1 | Receive 1 | — | — | — | — |
| 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|   | — | — | Transmit 2 | Receive 2 | — | — | — | — |
| 3 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|   | — | — | Transmit 3 | Receive 3 | — | — | — | — |
| 4 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|   | — | — | Transmit 4 | Receive 4 | — | — | — | — |

# 2.8 ASAP Card

**Note**      For card specifications, see the "A.2.7 ASAP Specifications" section on page A-11.

The ASAP card provides up to 16 Telcordia GR-253-CORE compliant, SDH STM-1, STM-4, STM-16, or Gigabit Ethernet ports, or up to 4 Telcordia GR-253-CORE compliant, SDH STM-64 ports, in any combination of line rates. The ASAP card, when used with the 4-Port I/O (4PIO) module, has up to 16 physical connector adapters (known as Small Form-factor Pluggables [SFPs]). The SFP ports operate at up to 2488.320 Mbps over a single-mode fiber. The ASAP card, when used with the 1-Port I/O (1PIO) module, has up to 4 physical connector adapters (known as 10Gigabit Small Form Factor Pluggables [XFPs]). The XFP ports operate at up to 9953.280 Mbps over a single-mode fiber. Both XFP and SFP physical connector adapters have two fibers per connector adapter (transmit [Tx] and receive [Rx]). The ASAP card supports VC3 payloads and concatenated payloads at VC4, VC4-2c, VC4-3c, VC4-4c, VC4-8c, VC4-16c and VC4-64c signal levels. The ASAP card is interoperable with ONS 15454 SDH E-Series, G-Series, and ML-Series Ethernet cards.

There are three major components to the ASAP card:

- Carrier card, which can be installed in Slots 1 through 4 and 11 through 14
- 4PIO and 1PIO modules, also called Pluggable Input/Output Module (PIMs), which plug into the ASAP carrier card
- SFPs/XFPs, called Pluggable Port Modules (PPMs) in CTC, which plug into the 4PIO or 1PIO (PIM) module and provide the fiber interface using a female LC connector

## 2.8.1 ASAP Connectors

An ASAP carrier card supports any combination of four 4PIOs or 1PIOs. Each 4PIO supports up to four SFPs, while each 1PIO supports one SFP/XFP. The maximum configuration for an ASAP card is 16 SFP or 4 XFP ports, or a mix of both. The ports can each be provisioned as either STM-1, STM-4, STM-16, STM64 (1PIO only), or Gigabit Ethernet.

In addition, the ports can be provisioned with STM-16 dense wavelength division multiplexing (DWDM) SFPs. 32 SFPs, each with separate product IDs (PIDs), allow operation on 32 channels, separated by 100 GHz on the ITU grid. The modules offer operation in the red band from 1546.12 to 1560.61 nm and in the blue band from 1530.33 to 1544.53 nm. These SFPs can be used in Metro, Regional, or Long Haul applications. Eight ASAP cards can be installed in a shelf, and up to four ITU-T SFPs can be plugged into each of the four 4PIO/PIMs (or one XFP in the 1PIO), providing a maximum of 128 ITU-T SFPs in a single shelf.

For detailed information about SFPs/XFPs, see the "2.10 SFP/XFP Modules" section on page 2-26. To determine the line rates supported by each SFP/XFP, see the "A.3 SFP/XFP Specifications" section on page A-12.

## 2.8.2 ASAP Covers and Plugs

The covers and plugs that are shipped with the ASAP carrier card, 4PIOs, 1PIOs, and SFPs/XFPs must be used in configurations where any of the these slots are unoccupied.

## 2.8.3 ASAP Card Faceplate and Block Diagram with 4PIOs Installed

Figure 2-7 shows the ASAP card faceplate, with four 4PIOs installed, and block diagram.

*Figure 2-7        ASAP Card Faceplate and Block Diagram (4PIOs Installed)*
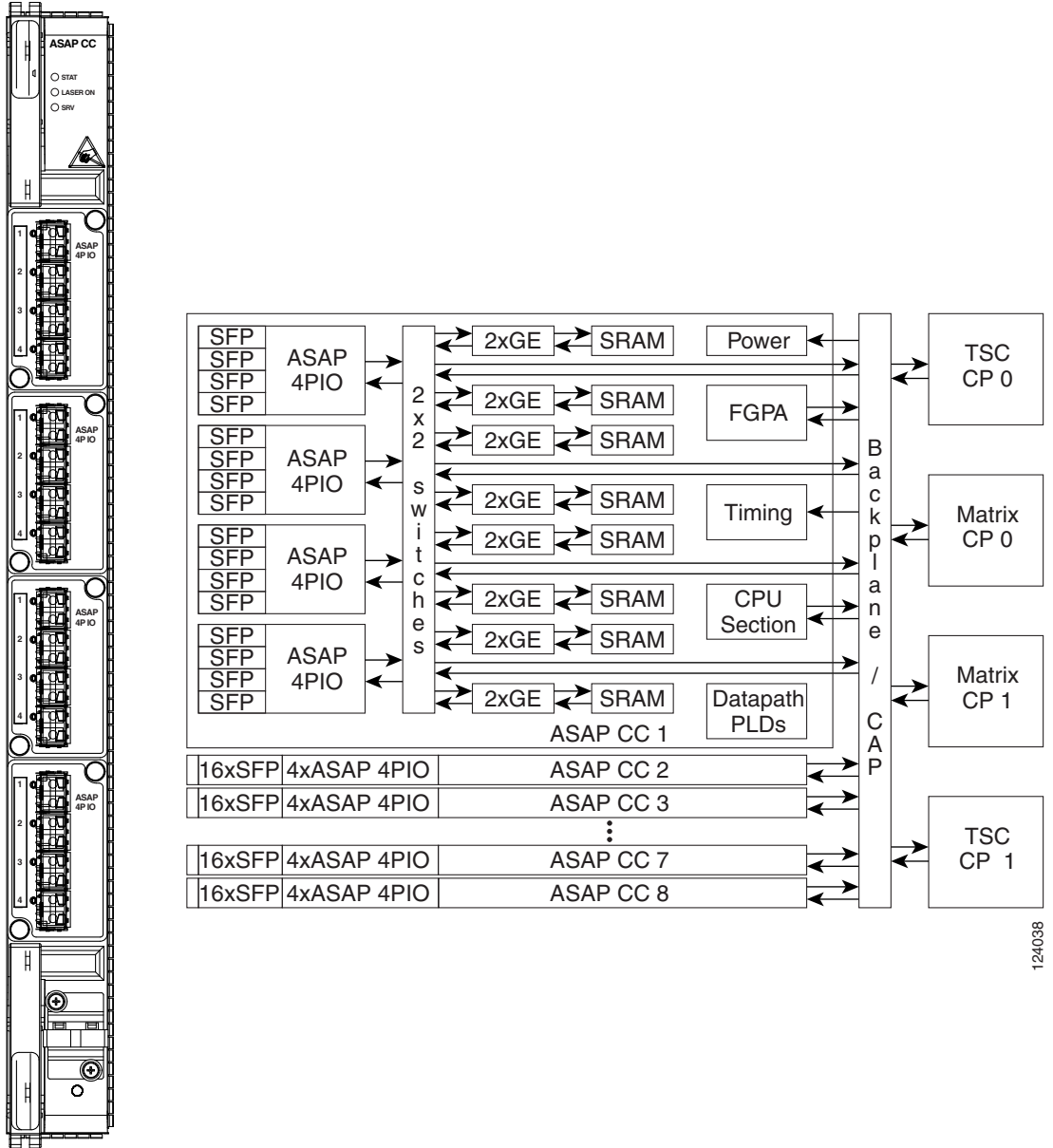
## 2.8.4 4PIO Module Faceplate

Figure 2-8 shows the 4PIO module faceplate.

*Figure 2-8        4PIO Module Faceplate*

Hand tighten, or remove
the label to tighten using
a Phillips screwdriver

ASAP
4P IO

124039
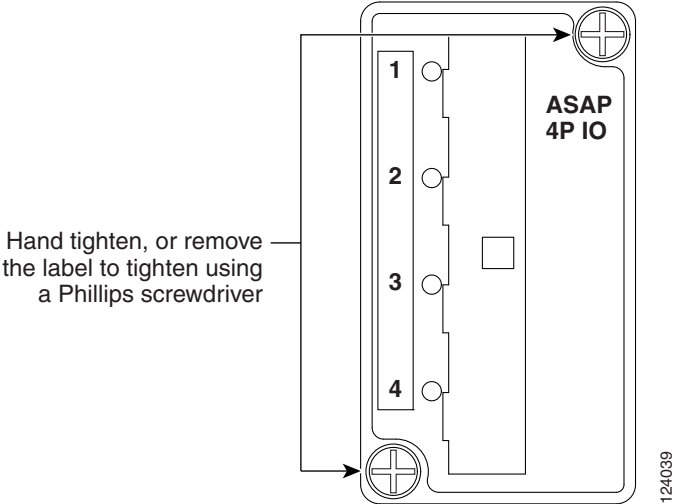
## 2.8.5 1PIO Module Faceplate

Figure 2-9 shows the 1PIO module faceplate.

*Figure 2-9        1PIO Module Faceplate*

Hand tighten, or remove
the label to tighten using
a Phillips screwdriver

ASAP
1P IO

151941
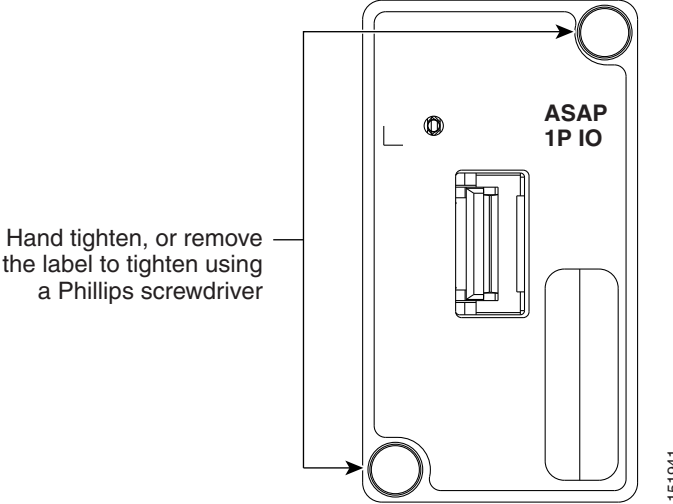
## 2.8.6  ASAP Card-Level Indicators

Table 2-19 describes the functions of the card-level LEDs on the ASAP carrier module.

*Table 2-19      ASAP Card-Level Indicators*

| Indicator | Color | Description |
|-----------|-------|-------------|
| **STAT LED** | Red | Indicates a hardware fault; this LED is off during normal operation. Replace the unit if the STAT LED persists. During diagnostics, the LED flashes quickly during initialization and slowly during configuration synchronization. |
| **SRV LED** | Green/Amber | The service mode of the card. Green indicates that the card is in use, amber indicates that the card is out of service, and off indicates that the card is either booting or has no power applied. |
| **LASER ON** | Green | The green LASER ON LED indicates that at least one of the card's lasers is active. |

## 2.8.7  ASAP Card Port-Level Indicators

Table 2-20 describes the functions of the port-level LEDs on the 4PIO and 1PIO modules, depending on whether the port is configured for SDH or Ethernet. (On the 4PIO modules, the port-level LEDs are numbered 1 through 4.)

*Table 2-20      ASAP (4PIO and 1PIO Module) Port-Level Indicators*

| Color | Description for a SDH-Configured Port | Description for an Ethernet-Configured Port |
|-------|----------------------------------------|----------------------------------------------|
| Green | Indicates that the port is provisioned. | Constant green indicates that there is a link and no traffic. Flashing green indicates that there is a link, and the LED flashes at a rate proportional to the level of traffic being received and transmitted over the port. |
| Amber | Indicates that the signal is degraded. | Amber indicates that the link has an issue inhibiting traffic, such as a signal error, or disabled port. |
| Red | Indicates a signal failure. | Indicates a signal failure. |
| Off | Indicates that the port is unprovisioned. | Indicates that there is no link. |

## 2.8.8 ASAP Card Port Numbering (4PIO Installed)

Figure 2-10 shows the installed 4PIO modules and corresponding port numbers for each SFP slot.

*Figure 2-10     ASAP 4PIO Port Numbering*
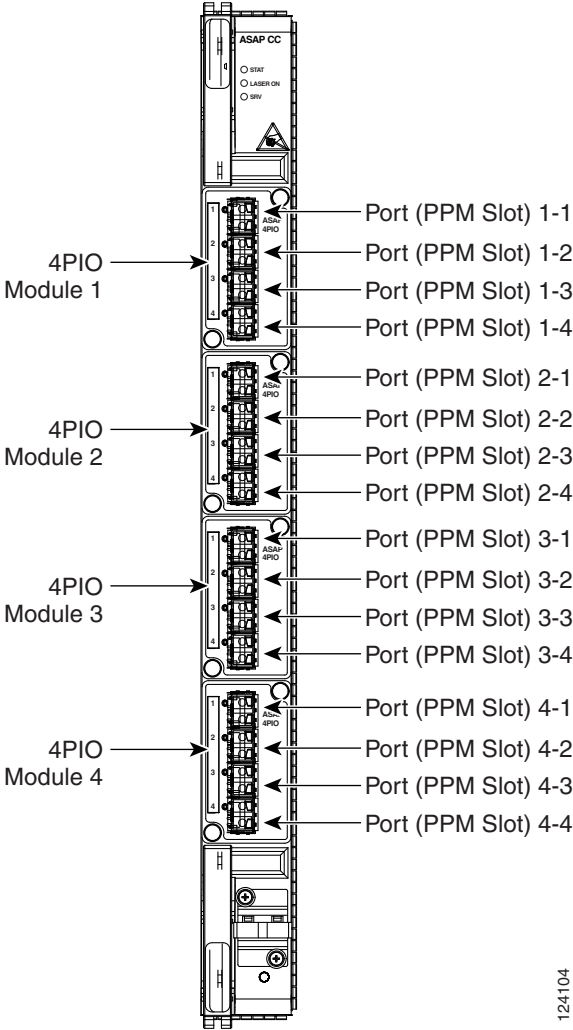
## 2.8.9 ASAP Card Port Numbering (1PIO Installed)

Figure 2-11 shows the installed 1PIO modules and corresponding port numbers for each XFP slot.

*Figure 2-11* **ASAP 1PIO Port Numbering**
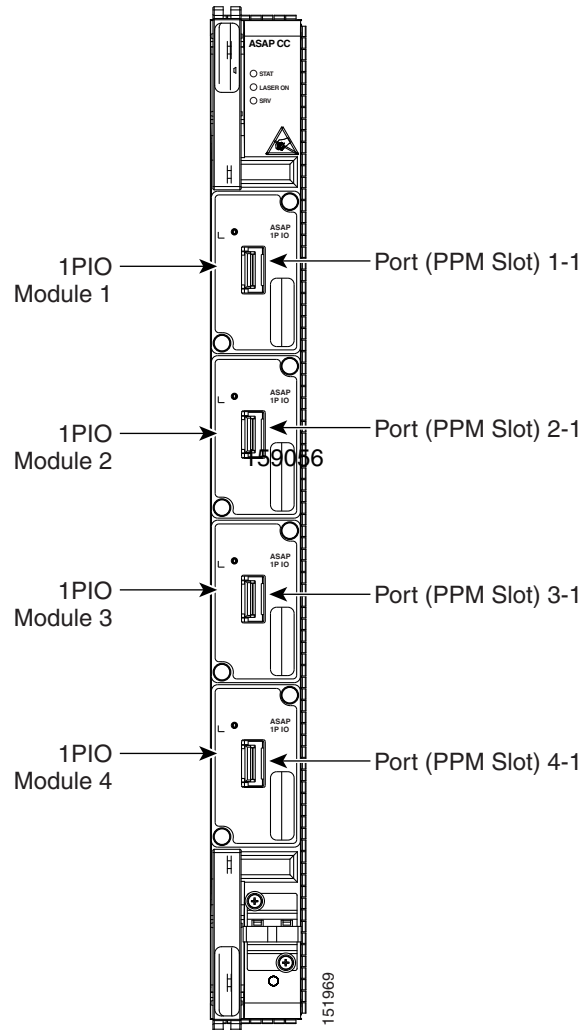


## 2.9 Filler Card

**Note** For card specifications, see the "A.2.8 Filler Card Specifications" section on page A-12.

The Filler card is used to fill unused optical (STM-N) traffic card slots in the ONS 15600 SDH shelf. In Software Release 1.1 and later, the Filler card has a card presence indicator (CPI) that allows the shelf to report the presence of the filler card to CTC. The Filler card uses dummy backplane connectors and a standard faceplate to secure the card in the empty shelf slot.

Figure 2-12 shows the Filler card body and faceplate.

*Figure 2-12* **ONS 15600 SDH Filler Card**
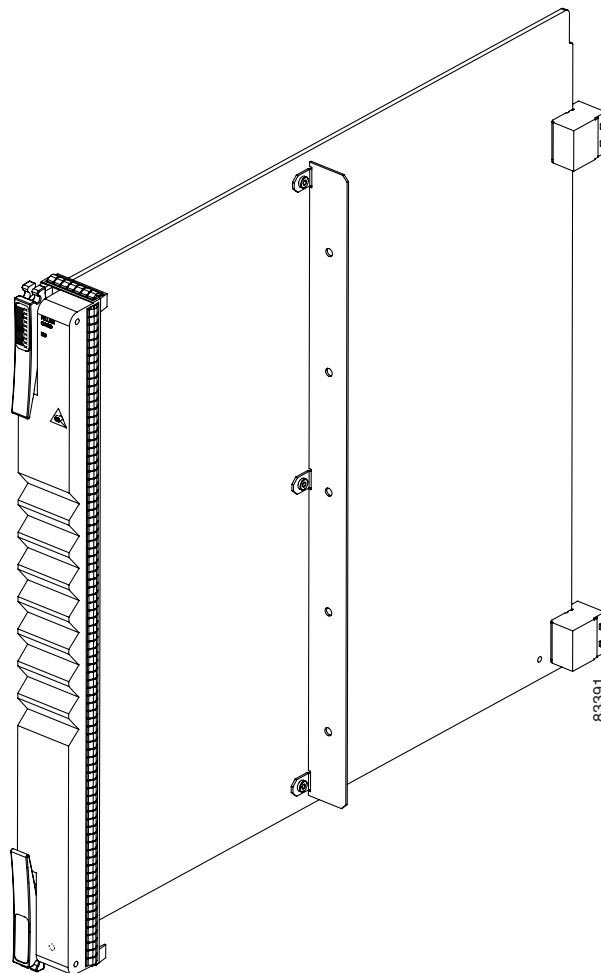


## 2.10 SFP/XFP Modules

This section describes the SFPs that provide the fiber interface to the ONS 15600 SDH ASAP card when used with the 4PIO modules. A line rate (STM-1, STM-4, STM-16, or Gigabit Ethernet) must be assigned to each SFP in the CTC software interface or using TL1. In CTC, SFPs are known as pluggable port modules (PPMs). To provision PPMs, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

**Note** For information about XFPs, which allow you to provision an STM-64 line rate when used with the 1PIO module, see the "2.10.1 XFP Description" section on page 2-28.

Table 2-21 lists the SFPs (PPMs) that are compatible with the ASAP card.

⚠

**Caution**    Use only SFPs certified for use in Cisco Optical Networking Systems. The qualified Cisco SFP pluggable module's top assembly numbers (TANs) are provided in Table 2-21.

*Table 2-21*        *SFP Compatibility*

| Card | Compatible SFP (Cisco Product ID) | Cisco Top Assembly Number (TAN) |
|------|-----------------------------------|----------------------------------|
| ASAP 4PIO only (ONS 15600 SONET/SDH) | ONS-SE-2G-L2 | 10-2013-01 |
| | ONS-SE-Z1 | 10-1971-01 |
| | ONS-SI-622-L2 | 10-1936-01 |
| | ONS-SI-155-L2 | 10-1937-01 |
| | ONS-SC-2G-46.1 through 60.6 | 10-2170-01 through 10-2184-01, and 10-2186-01 |
| | ONS-SC-2G-30.3 through 44.5 | 10-2155-01 through 10-2169-01, and 10-2185-01 |
| | ONS-SI-2G-S1 | 10-1992-01 |

To determine the line rates supported by each SFP/XFP, see the "A.3  SFP/XFP Specifications" section on page A-12.

SFPs are integrated fiber optic transceivers that provide high-speed serial links from a port or slot to the network. Various latching mechanisms can be used on the SFP/XFP modules. There is no correlation between the type of latch and the model type (such as SX or LX/LH) or technology type (such as Gigabit Ethernet). See the label on the SFP/XFP for technology type and model. One type of latch available is a Mylar tab as shown in Figure 2-13, a second type of latch available is an actuator/button (Figure 2-14), and a third type of latch is a bail clasp (Figure 2-15).

SFP dimensions are:

- Height 0.03 in. (8.5 mm)
- Width 0.53 in. (13.4 mm)
- Depth 2.22 in. (56.5 mm)

SFP temperature ranges for are:

- COM—Commercial operating temperature range: 23 to 158 degrees Fahrenheit (–5 to 70 degrees Celsius)
- EXT—Extended operating temperature range: 23  to185 degrees Fahrenheit (–5 to 85 degrees Celsius)
- IND—Industrial operating temperature range: –40 to 185 degrees Fahrenheit (–40 to 85 degrees Celsius)

*Figure 2-13*        *Mylar Tab SFP*
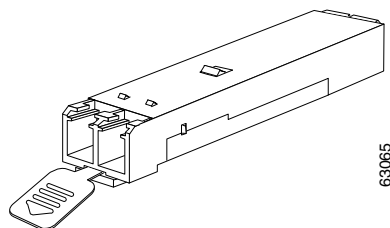
***Figure 2-14      Actuator/Button SFP***
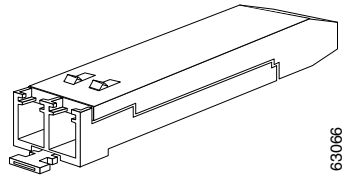


***Figure 2-15      Bail Clasp SFP***
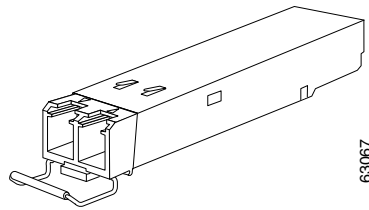


## 2.10.1  XFP Description

The 10-Gbps 1310-nm and 1550-nm XFP transceivers are integrated fiber optic transceivers that provide high-speed serial links at the following signaling rates: 9.95 Gbps, 10.31 Gbps, and 10.52 Gbps. The XFP integrates both the receiver and transmit path. The transmit side recovers and retimes the 10-Gbps serial data and passes it to a laser driver. The laser driver biases and modulates single mode (SMF) optical interfaces at 1310-nm or 1550-nm. The modules support all data encodings through an LC connector. The receive side recovers, retimes the 10-Gbps optical data stream from a positive-intrinsic-negative (PIN) photodetector, transimpedance amplifier and passes it to an output driver.

⚠

**Caution**  Use only XFPs certified for use in Cisco Optical Networking Systems. The qualified Cisco XFP pluggable module's top assembly numbers (TANs) are provided in Table 2-22.

***Table 2-22      XFP Compatibility***

| Card | Compatible XFP (Cisco Product ID) | Cisco Top Assembly Number (TAN) |
|---|---|---|
| ASAP 1PIO only (ONS 15600 SONET/SDH) | ONS-XC-10G-S1 ONS-XC-10G-L2 | 10-2112-01 10-2194-01 |

The XFP module uses the bail clasp latching mechanism, shown unlatched in Figure 2-16 and latched in Figure 2-17. See the label on the XFP for technology type and model.

*Figure 2-16        Bail Clasp XFP (Unlatched)*
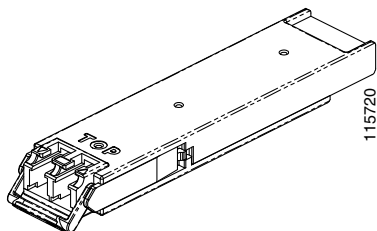


*Figure 2-17        Bail Clasp XFP (Latched)*
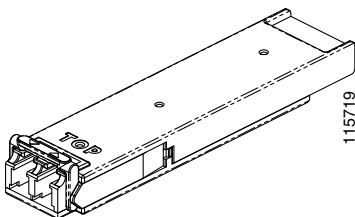


XFP dimensions are:

- Height 0.33 in. (8.5 mm)
- Width 0.72 in. (18.3 mm)
- Depth 3.1 in. (78 mm)

XFP temperature ranges are:

- COM—Commercial operating temperature range: 23 to 158 degrees Fahrenheit (–5 to 70 degrees Celsius)
- EXT—Extended operating temperature range: 23  to185 degrees Fahrenheit (–5 to 85 degrees Celsius)
- IND—Industrial operating temperature range: –40 to 185 degrees Fahrenheit (–40 to 85 degrees Celsius)

## 2.10.2  PPM Provisioning

SFPs and XFPs are known as pluggable-port modules (PPMs) in the CTC. Multirate PPMs for the ASAP card can be provisioned for different line rates in CTC. For more information about provisioning PPMs, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

**C H A P T E R 3**

# Card Protection

This chapter explains the Cisco ONS 15600 SDH card protection configurations.

Chapter topics include:

# 3.1 Optical Port Protection

When you set up protection for ONS 15600 SDH cards, you must choose between maximum protection and maximum port availability. The highest protection reduces the number of available ports; the highest port availability reduces the protection. Table 3-1 contrasts port protection with an unprotected scheme.

*Table 3-1      Port Protection Types*

| Type | Ports | Description |
|------|-------|-------------|
| 1+1 | Any optical | Pairs a working optical port with a protect optical port. Protect ports must match the line rate of the working ports. For example, Port 1 of an STM-16 card can only be protected by another STM-16 port. Ports do not need to be in adjoining slots. For maximum protection, provision the ports/cards in Slots 1 to 4 as working and the ports/cards in Slots 11 to 14 as protect. |
| Unprotected | Any | Unprotected ports can cause traffic loss if a port fails or incurs a signal error. However, because no ports are reserved for protection, unprotected schemes maximize the service available for use on the ONS 15600 SDH.<br><br>**Note**    If you want to protect traffic you should implement either a subnetwork connection protection ring (SNCP) or a multiplex-section shared protection ring (MS-SPRing) protection scheme. |

**Note**    Because there are no electrical cards in the ONS 15600 SDH, 1:1 and 1:N protection is not provided.

Figure 3-1 shows an example of the ONS 15600 SDH in a maximum, 1+1 protected configuration.

*Figure 3-1*      *ONS 15600 SDH in a 1+1 Protected Configuration*



Working STM-N    TSC    SSXC    SSXC    TSC    Protect STM-N
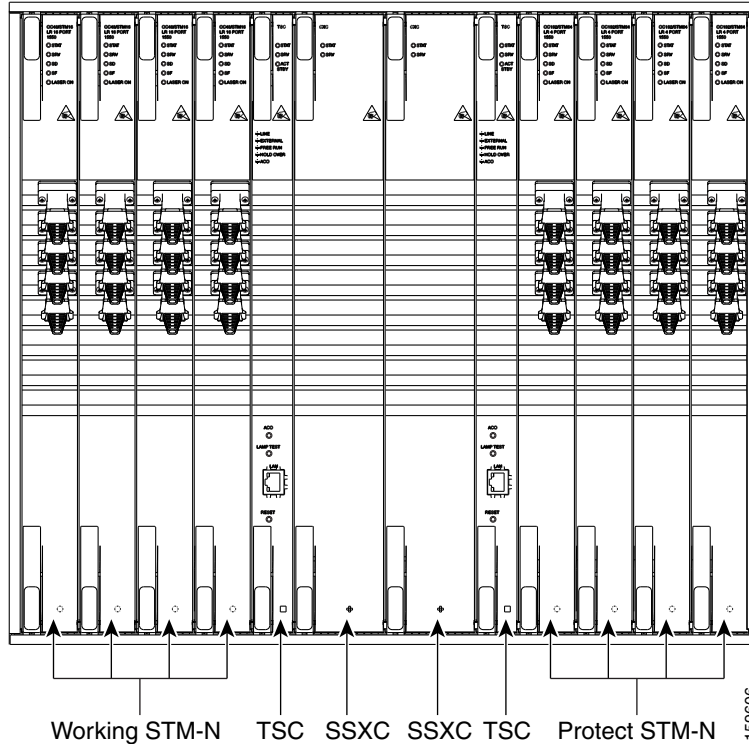
With 1+1 protection, any port can be assigned to protect the traffic of a corresponding working port. A working port must be paired with a protect port of the same type, for example, an STM-16 port must be paired with another STM-16 port.

1+1 span protection can be either revertive or nonrevertive. With nonrevertive 1+1 protection, when a span failure occurs and the signal switches from the working port to the protect port, the signal stays switched to the protect port until it is manually switched back. Revertive 1+1 protection automatically switches the signal back to the working port when the failure condition on the working port is cleared.

For more information about protection schemes and how to create and modify them with Cisco Transport Controller (CTC), refer to the *Cisco ONS 15600 SDH Procedure Guide*.

# 3.2 Unprotected Ports

Unprotected ports are not included in a protection scheme; therefore, a port failure or a signal error can result in data loss if no path level protection (SNCP) exists. Because no bandwidth lies in reserve for protection, unprotected schemes maximize the available ONS 15600 SDH bandwidth. Figure 3-2 shows the ONS 15600 SDH in an unprotected configuration. All ports are in a working state.

*Figure 3-2* ***ONS 15600 SDH in an Unprotected Configuration***



Working STM-N    TSC   SSXC   SSXC   TSC   Working STM-N
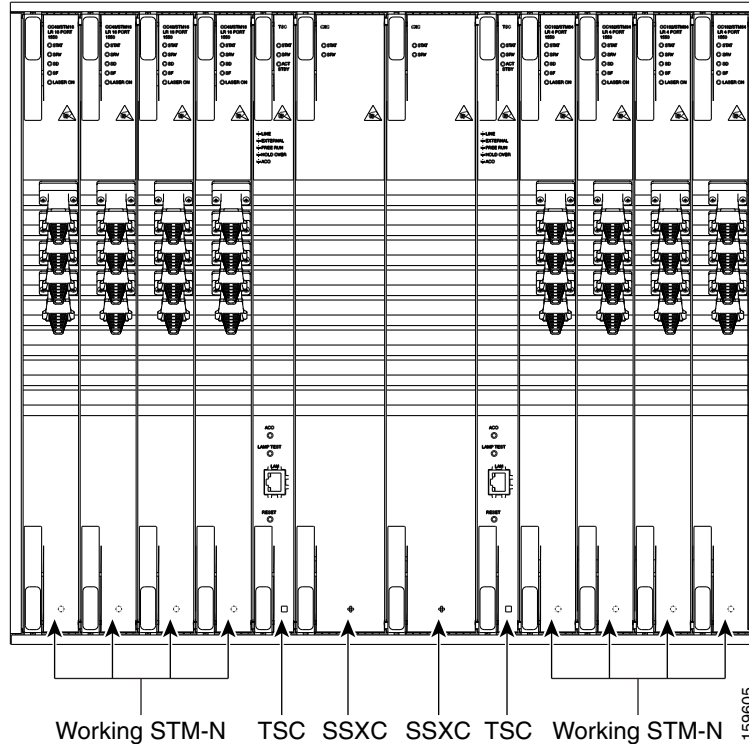
# 3.3 External Switching Commands

The external switching commands on the ONS 15600 SDH are Manual, Force, Lockout, and Lock-on.

A Manual switch will switch traffic if the path has no errors or an error rate less than the signal degrade (SD) threshold. A Force switch will switch traffic even if the path has an SD or signal fail (SF) condition; however, a Force switch will not override an SF condition on a 1+1 protection scheme. A Force switch has a higher priority than a Manual switch.

Lockouts prevent traffic from switching to the protect port under any circumstance, thus they can only be applied to protect cards. Lockouts have the highest priority. Another way to inhibit protection switching in a 1+1 configuration is to apply a lock- on to the working port. A working port with a lock-on applied cannot switch traffic to the protect port in the protection group (pair).

C H A P T E R **4**

# Cisco Transport Controller Operation

This chapter describes Cisco Transport Controller (CTC), the Cisco ONS 15600 SDH software interface that is stored on the TSC card and downloaded to your workstation each time you log into the ONS 15600 SDH. For CTC setup and login information, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Chapter topics include:

# 4.1 CTC Software Delivery Methods

Use CTC to provision and administer the ONS 15600 SDH. CTC is a Java application that is installed in two locations:

- ONS 15600 SDH TSC card
- PCs and UNIX workstations that connect to the ONS 15600 SDH

CTC is stored on the TSC card and is downloaded to your workstation each time you log into an ONS 15600 SDH.

You can also log into CTC using the CTC launcher application (StartCTC.exe). Refer to the "4.6 Using the CTC Launcher Application to Manage Multiple ONS Nodes" section on page 4-15 for more information.

## 4.1.1 CTC Software Installed on the TSC Card

CTC software is preloaded on the ONS 15600 SDH TSC cards; therefore, you do not need to install software on the TSC. To upgrade to a newer CTC software version, refer to the release-specific upgrade document.

You can view the software versions that are installed on one ONS 15600 SDH by clicking the Maintenance > Software tabs in node view. Click the tabs in network view to display the software versions installed on all the network nodes.

## 4.1.2 CTC Software Installed on the PC or UNIX Workstation

When you connect to the ONS 15600 SDH, the TSC card automatically downloads the CTC software to your computer, where it is automatically installed if you have the correct Java Runtime Environment (JRE). The automatic download/installation process ensures that your computer is running the same CTC software version as the TSC you are accessing. The CTC software files are stored in the temporary directory designated by your computer's operating system. You can use the Delete CTC Cache button to remove files stored in the temporary directory. If the files are deleted, they are downloaded the next time you connect to an ONS 15600 SDH. Downloading the Java archive (JAR) files for CTC takes several minutes depending on the bandwidth of the connection between your workstation and the ONS 15600 SDH. For example, JAR files downloaded from a modem or a SONET data communications channel (SDCC) network link requires more time than JAR files downloaded over a LAN connection.

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. 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.

# 4.2 CTC Installation Overview

To connect to an ONS 15600 SDH using CTC, enter the ONS 15600 SDH IP address in the URL field of a web browser, such as Netscape Navigator or Microsoft Internet Explorer. After connecting to an ONS 15600 SDH, the following events occur automatically:

**Note**    Each ONS 15600 SDH has a unique IP address that you use to access the ONS 15600 SDH. The initial IP address, 192.168.1.2, is the default address for ONS 15600 SDH access and configuration.

1. A CTC launcher applet is downloaded from the TSC to your computer's temporary directory. (If these files are deleted, they are automatically reinstalled the next time you connect to the ONS 15600 SDH.)

2. The launcher determines whether your computer has a CTC release matching the release on the ONS 15600 SDH TSC.

**3.** If the computer does not have CTC installed, or if the installed release is older than the TSC version, the launcher downloads the CTC program files from the TSC.

**4.** The launcher starts CTC. The CTC session is separate from the web browser session, so the web browser is no longer needed. If you log into an ONS 15600 SDH that is connected to ONS 15600 SDHs with older versions of CTC, or to Cisco ONS 15454s, CTC element files are downloaded automatically to enable you to interact with those nodes. You cannot interact with nodes on the network that have a newer software version than the node that you are logged into (the nodes will appear gray in network view). Therefore, always log into nodes with the latest software release.

Each ONS 15600 SDH can handle up to 16 simultaneous CTC sessions. CTC performance might vary depending upon the volume of activity in each session.

**Note** You can also use TL1 commands to communicate with the ONS 15600 SDH through VT100 terminals and VT100 emulation software, or you can telnet to an ONS 15600 SDH using TL1 port 3083. Refer to the *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Command Guide* for a comprehensive list of TL1 commands.

# 4.3 PC and UNIX Workstation Requirements

To use CTC with an ONS 15600 SDH, your computer must have a web browser with the correct JRE installed. The correct JRE and Java plug-in for the CTC software release are included on the Cisco ONS 15600 SDH software CD.

**Note** To avoid network performance issues, Cisco recommends managing a maximum of 50 nodes concurrently with CTC. The 50 nodes can be on a single DCC or split across multiple DCCs. Cisco does not recommend running multiple CTC sessions when managing two or more large networks.

To manage more than 50 nodes, Cisco recommends using Cisco Transport Manager (CTM). If you do use CTC to manage more than 50 nodes, you can improve performance by adjusting the heap size; see the "General Troubleshooting" chapter of the *Cisco ONS 15600 SDH Troubleshooting Guide.* You can also create login node groups; see the "Connect the PC and Log Into the GUI" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Table 4-1 provides the minimum requirements for PCs and UNIX workstations.

*Table 4-1      Minimum Computer Requirements for CTC*

| Area | Requirements | Notes |
|---|---|---|
| Processor (PC only) | Pentium 4 processor or equivalent | A faster CPU is recommended if your workstation runs multiple applications or if CTC manages a network with a large number of nodes and circuits. |
| RAM | 512 MB RAM or more | A minimum of 1 GB is recommended if your workstation runs multiple applications or if CTC manages a network with a large number of nodes and circuits. |

*Table 4-1*        ***Minimum Computer Requirements for CTC (continued)***

| Area | Requirements | Notes |
|---|---|---|
| Hard drive | 20 GB hard drive with 100MB of free space required | CTC application files are downloaded from the TCC2/TCC2P to your computer. These files occupy around 100MB (250MB to be safer) or more space depending on the number of versions in the network. |
| Operating System | • PC: Windows 98 (1st and 2nd editions), Windows ME, Windows NT 4.0 with Service Pack 6a, Windows 2000 with Service Pack 3, or Windows XP with Service Pack 1<br><br>• Workstation: Solaris versions 9 or 10 | Check with the vendor for the latest patch/Service Pack level |
| Java Runtime Environment | JRE 5.0 | JRE 5.0 is installed by the CTC Installation Wizard included on the Cisco ONS 15454 software CD. JRE 5.0 provide enhancements to CTC performance, especially for large networks with numerous circuits.<br><br>Cisco recommends that you use JRE 5.0 for networks with Software R8.5 nodes. If CTC must be launched directly from nodes running software R7.0 or R7.2, Cisco recommends JRE 1.4.2 or JRE 5.0. If CTC must be launched directly from nodes running software R5.0 or R6.0, Cisco recommends JRE 1.4.2.If CTC must be launched directly from nodes running software earlier than R5.0, Cisco recommends JRE 1.3.1_02. |

***Table 4-1 Minimum Computer Requirements for CTC (continued)***

| Area | Requirements | Notes |
|------|-------------|-------|
| Web browser | • PC:Internet Explorer 6.x or Netscape 7.x<br>• UNIX Workstation: Mozilla 1.7, Netscape 4.76, Netscape 7.x | For the PC, use JRE 5.0 with any supported web browser. Cisco recommends Internet Explorer 6.x. For UNIX, use JRE 5.0 with Netscape 7.x or JRE 1.3.1_02 with Netscape 4.76.<br><br>Netscape 4.76 or 7.x is available at the following site: http://channels.netscape.com/ns/browsers/default.jsp<br><br>Internet Explorer 6.x is available at the following site: http://www.microsoft.com |
| Cable | Use a crossover or straight-through LAN (CAT-5) cable to connect:<br>• The ONS 15600 SDH to a hub using the backplane RJ-45 ports, or to connect through a LAN.<br>• The ONS 15600 SDH to a PC using the backplane RJ-45 ports.<br>• The active TSC RJ-45 port to a laptop or hub. | A direct PC-to-ONS 15600 SDH connection means your computer is physically connected to the ONS 15600 SDH. This is most commonly done by connecting a LAN (CAT-5) straight-through cable from your PC to the RJ-45 port on the TSC. However, direct connections include connections to switches or hubs where the ONS 15600 SDH is physically connected.<br><br>**Note** Use only the active TSC connector for connectivity. If you connect to the standby or switch TSCs, you will lose connectivity. Cisco recommends that you use the RJ-45 connector on the Customer Access Panel (CAP/CAP2) so that connection to the ONS 15600 SDH will not be lost during a TSC switch. |

# 4.4 CTC Login

After you have installed CTC, you can log in to a node using your browser. To log in, you must type the node IP address in the URL window. The CTC Login window appears.

The CTC Login window provides the following options to accelerate the login process.

- The Disable Network Discovery option omits the discovery of nodes with data communications channel (DCC) connectivity. To access all nodes with DCC connectivity, make sure that Disable Network Discovery is not checked. If you have network discovery disabled, CTC will not poll the network for more recent versions of the software. (For more information about the automatic download of the latest CTC JAR files, see the "4.1.2 CTC Software Installed on the PC or UNIX Workstation" section on page 4-2.)

- The Disable Circuit Management option omits the discovery of circuits. To view circuits immediately after logging in, make sure that Disable Circuit Management is not checked. However, if disabled, after you have logged in you can click the Circuits tab and CTC will give you the option to enable circuit management.

These options are useful if you want to log in to a node to perform a single task, such as placing a card in or out of service, and do not want to wait while CTC discovers DCC connections and circuits.

## 4.4.1 Legal Disclaimer

The CTC Login window currently displays the following warning message: "Warning: This system is restricted to authorized users for business purpose. Unauthorized access is a violation of the law. This service can be monitored for administrative and security reasons. By proceeding, you consent to this monitoring."

The ONS 15600 SDH allows a user with Superuser privileges to modify the default login warning message and save it to a node using the Provisioning > Security > Legal Disclaimer > HTML tab. The login warning message field allows up to 250 characters of text (1600 characters total, including HTML markup).

## 4.4.2 Login Node Group

Login node groups display nodes that have only an IP connection. After you are logged into CTC, you can create a login node group from the Edit > Preferences menu. Login groups appear in the Additional Nodes list on the Login window.

For example, if you logged into Node 1, you would see Node 2 and Node 3 because they have DCC connectivity to Node 1. You would not see Nodes 4, 5, and 6 because DCC connections do not exist. To view all six nodes at once, you create a login node group with the IP addresses of Nodes 1, 4, 5, and 6. Those nodes, and all nodes optically connected to them, appear when you select the login group from the Additional Nodes list on the Login window the next time you log in.

# 4.5 CTC Window

The CTC window appears after you log into an ONS 15600 SDH. The CTC node view is the first view that appears after you log into an ONS 15600 SDH (Figure 4-1). The login node is the first node displayed, and it is the "home view" for the session (accessed by choosing View > Go To Home View).

The CTC window includes a menu bar, a toolbar, and a top and bottom pane. The top pane displays status information about the selected objects and a graphic of the current view. The bottom pane displays tabs and subtabs, which you use to view ONS 15600 SDH information and perform ONS 15600 SDH provisioning and maintenance. From the default node view window you can display the other two ONS 15600 SDH views: network and card.

*Figure 4-1*        *CTC Window Elements in the Node View (Default Login View)*
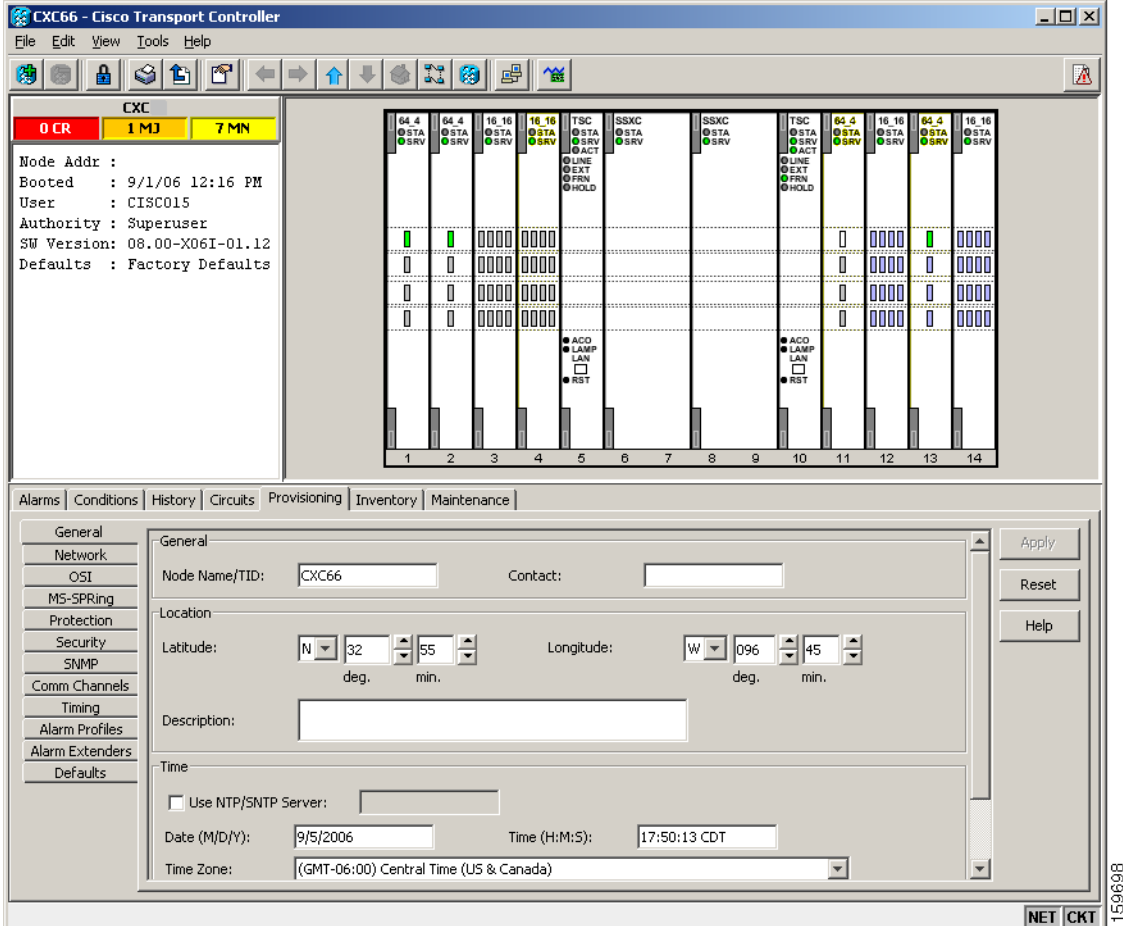


# 4.5.1  Node View

Node view allows you to view and manage one ONS 15600 SDH node (Figure 4-1). The status area shows the node name; number of Critical (CR), Major (MJ), and Minor (MN) alarms; IP address; session boot date and time; name of the current logged-in user; and user security level.

## 4.5.1.1  CTC Card Colors

The graphic area of the CTC window depicts the ONS 15600 SDH shelf assembly. The colors of the cards in the graphic reflect the real-time status of the physical card, slot, and port. Table 4-2 describes the node view card colors.

*Table 4-2        Node View Card Colors*

| Card Color | Status |
|---|---|
| Gray | Slot is not provisioned; no card is installed. |
| Violet | Slot is provisioned; no card is installed (the card immediately changes to yellow because the IMPROPRMVL alarm is raised). |
| White | Slot is provisioned; a functioning card is installed or booting. |
| Yellow | Slot is provisioned; a minor alarm condition exists. |
| Orange | Slot is provisioned; a major alarm condition exists. |
| Red | Slot is provisioned; a critical alarm exists. |

Port color in both card and node view indicates the port service state. Table 4-3 lists the port colors and their service states. For more information about port service states, see Appendix B, "Administrative and Service States."

*Table 4-3        Node View Card Port Colors and Service States*

| Port Color | Service State | Description |
|---|---|---|
| Blue | Locked-enabled,loopback | Port is in a loopback state. On the card in node view, a line between ports indicates that the port is in terminal or facility loopback (see Figure 4-2 and Figure 4-3). Traffic is carried and 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. |
| Blue | Locked-enabled, maintenance | Port is out-of-service for maintenance. Traffic is carried and loopbacks are allowed. 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 Locked-enabled,maintenance for testing or to suppress alarms temporarily. Change the state to Unlocked-enabled; Locked-enabled,disabled; or Unlocked-disabled,automaticInService when testing is complete. |
| Gray | Locked-enabled,disabled | The port is out-of-service and unable to carry traffic. Loopbacks are not allowed in this service state. |

*Table 4-3        Node View Card Port Colors and Service States (continued)*

| Port Color | Service State | Description |
|---|---|---|
| Green | Unlocked-enabled | The port is fully operational and performing as provisioned. The port transmits a signal and displays alarms; loopbacks are not allowed. |
| Violet | Unlocked-disabled, automaticInService | The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in this state for the duration of the soak period. After the soak period ends, the port service state changes to Unlocked-enabled.<br><br>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. The AINS port will automatically transition to Unlocked-enabled when a signal is received for the length of time provisioned in the soak field. |

*Figure 4-2        Terminal Loopback Indicator*



*Figure 4-3        Facility Loopback Indicator*



## 4.5.1.2  Node View Card Shortcuts

If you move your mouse over cards in the graphic, popups display additional information about the card including the card type; card status (active or standby); the type of alarm, such as critical, major, and minor (if any); and the alarm profile used by the card. Right-click a card to reveal a shortcut menu that you can use to open, reset, change, or delete a card. Right-click a slot to preprovision a card (that is, provision a slot before installing the card).

## 4.5.1.3  Node View Tabs

Table 4-4 lists the tabs and subtabs available in the node view.

*Table 4-4        Node View Tabs and Subtabs*

| Tab | Description | Subtabs |
|---|---|---|
| Alarms | Lists current alarms (CR, MJ, MN) for the node and updates them in real time. | — |
| Conditions | Allows you to retrieve a list of standing conditions on the node. | — |

*Table 4-4*        ***Node View Tabs and Subtabs (continued)***

| Tab | Description | Subtabs |
|-----|-------------|---------|
| History | Provides a history of node alarms including date, type, and severity of each alarm. The Session subtab displays alarms and events for the current session. The Shelf subtab displays alarms and events retrieved from a fixed-size log on the node. | Session, Node |
| Circuits | Allows you to create, delete, edit, and reroute circuits. | Circuits, Rolls |
| Provisioning | Allows you to provision the ONS 15600 SDH node. | General, Network, OSI, MS-SPRing, Protection, Security, SNMP, Comm Channels, Timing, Alarm Profiles, Alarm Extenders, Defaults |
| Inventory | Provides inventory information (part number, serial number, Common Language Equipment Identification [CLEI] codes) for cards installed in the node. Allows you to delete and reset cards, and change card service state. For more information on card service states, see Appendix B, "Administrative and Service States." | — |
| Maintenance | Allows you to perform maintenance tasks for the node. | Database, Routing Table, OSI, MS-SPRing, Protection, Software, Diagnostic, Timing, Audit, Test Access, Alarm Extenders, Preferred Copy |

## 4.5.2  Network View

Network view allows you to view and manage ONS 15600 SDHs and ONS 15454 SDHs that have DCC connections to the node that you logged into, and any login node groups you have selected (Figure 4-4).

*Figure 4-4      Network Displayed in CTC Network View*
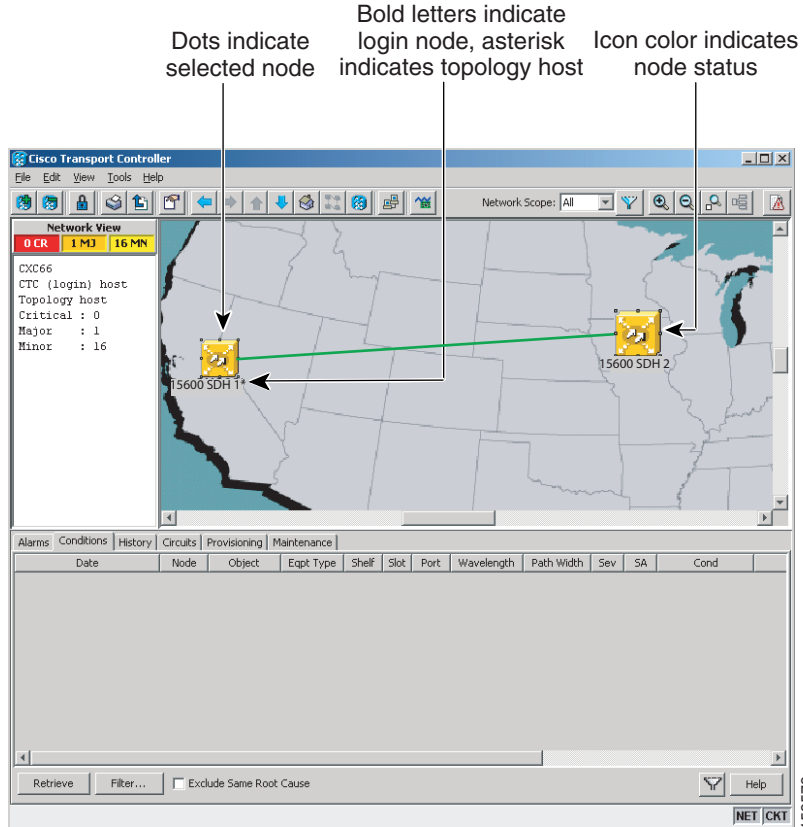


The graphic area displays a background image with colored node icons. A Superuser can set up the logical network view feature, which enables each user to see the same network view.

Lines show DCC connections between the nodes. Selecting a link in the graphic area displays information about the node and span in the status area. See the "4.5.2.3  Link Consolidation" section on page 4-12 for more information.

## 4.5.2.1  CTC Node Colors

The node icon colors indicate the node status (Table 4-5).

*Table 4-5      Node Status*

| Color | Alarm Status |
|---|---|
| Green | No alarms |
| Yellow | Highest-level alarm is a minor alarm |
| Orange | Highest-level alarm is major alarm |
| Red | Highest-level alarm is a critical alarm |
| Gray with node name | Node is initializing |
| Gray with IP address | Node is initializing; a problem exists with IP routing from node to CTC or your login/password is not provisioned on this node |

## 4.5.2.2 Network View Tabs

Table 4-6 lists the tabs and subtabs available in the network view.

*Table 4-6      Network View Tabs and Subtabs*

| Tab | Description | Subtabs |
|-----|-------------|---------|
| Alarms | Lists current alarms (CR, MJ, MN) for the network and updates them in real time | — |
| Conditions | Displays a list of standing conditions on the network | — |
| History | Provides a history of network alarms including date, type, and severity of each alarm | — |
| Circuits | Create, delete, edit, filter and search for network circuits | Circuits, Rolls |
| Provisioning | Provision security, alarm profiles, MS-SPRings, overhead circuits, server trails, and load/manage a VLAN database | Security, Alarm Profiles, MS-SPRing, Overhead Circuits, Provisionable Patchcords (PPC), Server Trails, VLAN DB Profile |
| Maintenance | Displays the working and protect software versions and allows software to be downloaded, retrieves Open Shortest Path First (OSPF) node information, and display the list of automatic power control (APC) domains for a network | Software, Diagnostic, APC |

## 4.5.2.3 Link Consolidation

CTC provides the ability to consolidate multiple data communications channel (DCC), general communications channel (GCC), optical transport section (OTS), provisionable patchcord (PPC), and server trail links into one or more links. Link consolidation allows you to condense multiple inter-nodal links into a single link. The link consolidation sorts links by class, meaning that all DCC links are consolidated together, for example.You can access individual links within consolidated links using the right-click shortcut menu.

Each link has an associated icon (Table 4-7).

*Table 4-7      Link Icons*

| Icon | Description |
|------|-------------|
|  | DCC icon |
|  | GCC icon |
|  | OTS icon |

**Table 4-7       Link Icons (continued)**

| Icon | Description |
|------|-------------|
|  | PPC icon |
|  | Server Trail icon |

✎

**Note**    Link consolidation is only available on non-detailed maps. Non-detailed maps display nodes in icon form instead of detailed form, meaning the nodes appear as rectangles with ports on the sides. Refer to the *Cisco ONS 15600 SDH Procedure Guide* for more information about consolidated links.

## 4.5.3  Card View

The card view provides information about individual ONS 15600 SDH cards. Use this window to perform card-specific maintenance and provisioning (Figure 4-5). A graphic showing the ports on the card is shown in the graphic area. The status area displays the node name, slot, number of alarms, card type, equipment type, and the card status (active or standby), card service state if the card is present, and port service state (described in Table 4-3 on page 4-8). The information that appears and the actions you can perform depend on the card. For more information about card service states, see Appendix B, "Administrative and Service States."

✎

**Note**    CTC displays a card view for all ONS 15600 SDH cards except the TSC and SSXC cards. Provisioning for these common control cards occurs at the node view; therefore, no card view is necessary.

*Figure 4-5        CTC Card View Showing an STM-64 Card*
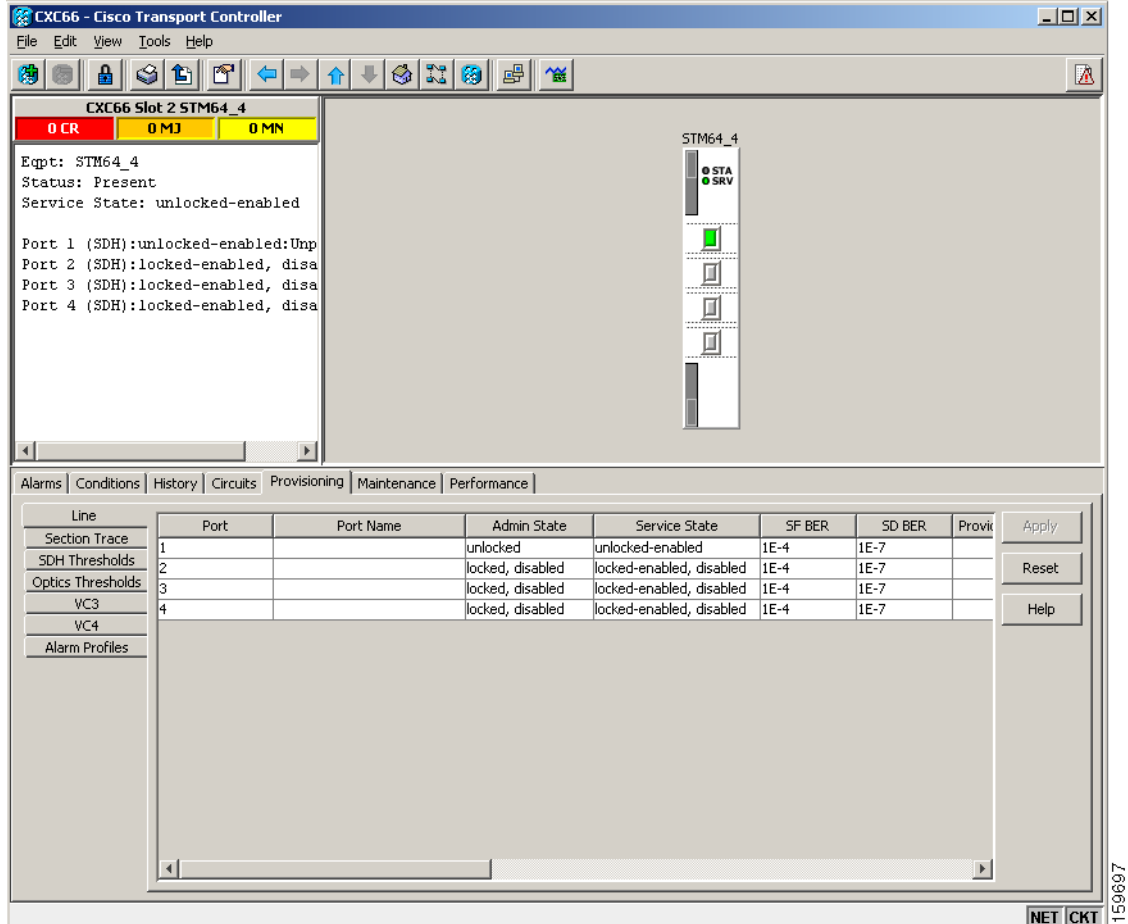


Use the card view tabs and subtabs, shown in Table 4-8, to provision and manage the ONS 15600 SDH. The subtabs, fields, and information displayed under each tab depend on the card type selected.

*Table 4-8        Card View Tabs and Subtabs*

| Tab | Description | Subtabs |
|-----|-------------|---------|
| Alarms | Lists current alarms (CR, MJ, MN) for the card and updates them in real time | — |
| Conditions | Displays a list of standing conditions on the card | — |
| History | Provides a history of card alarms including date, object, port, and severity of each alarm | Session (displays alarms and events for the current session); Card (displays alarms and events retrieved from a fixed-size log on the card) |
| Circuits | Create, delete, edit, filter, and search circuits | Circuits, Rolls |
| Provisioning | Provision an ONS 15600 SDH card | Line, SDH Thresholds, Optics Thresholds, SDH VC, Alarm Profiles Section Trace, Pluggable Port Modules, Optical, Ethernet |

*Table 4-8*        *Card View Tabs and Subtabs (continued)*

| Tab | Description | Subtabs |
|-----|-------------|---------|
| Maintenance | Perform maintenance tasks for the card | Loopback, Transceiver, Protection, Path Trace, ALS, AINS Soak, Optical, Ethernet |
| Performance | Perform performance monitoring for the card | Optical, Ethernet |

## 4.5.4  Export and Print CTC Data

You can use the File > Print or File > Export options to print or export CTC provisioning information for record keeping or troubleshooting. The functions can be performed in card, node, or network views. The File > Print function sends the data to a local or network printer. File > Export exports the data to a file where it can be imported into other computer applications, such as spreadsheets and database management programs.

Whether you choose to print or export data, you can choose from the following options:

- Entire frame—Prints or exports the entire CTC window including the graphical view of the card, node, or network. This option is available for all windows.

- Tabbed view—Prints or exports 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 or exports 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.

  The Table Contents option does not apply to all windows; for a list of windows that do not support print or export, see the *Cisco ONS 15600 SDH Procedure Guide*.

# 4.6  Using the CTC Launcher Application to Manage Multiple ONS Nodes

The CTC Launcher application is an executable file, StartCTC.exe, that is provided on Software Release 8.0 CDs for Cisco ONS products. You can use CTC Launcher to log into multiple ONS nodes that are running CTC Software Release 3.3 or higher, without using a web browser. The CTC launcher application provides an advantage particularly when you have more than one NE version on the network, because it allows you to pick from all available CTC software versions. It also starts more quickly than the browser version of CTC and has a dedicated node history list.

CTC Launcher provides two connection options. The first option is used to connect to ONS NEs that have an IP connection to the CTC computer. The second option is used to connect to ONS NEs that reside behind third party, OSI-based GNEs. For this option, CTC Launcher creates a TL1 tunnel to transport the TCP traffic through the OSI-based GNE.

The TL1 tunnel transports the TCP traffic to and from ONS ENEs through the OSI-based GNE. TL1 tunnels are similar to the existing static IP-over-CLNS tunnels, GRE and Cisco IP, that can be created at ONS NEs using CTC. (Refer to the Cisco ONS product documentation for information about static

IP-over-CLNS tunnels.) However, unlike the static IP-over-CLNS tunnels, TL1 tunnels require no provisioning at the ONS ENE, the third-party GNE, or DCN routers. All provisioning occurs at the CTC computer when the CTC Launcher is started.

Figure 4-6 shows examples of two static IP-over-CLNS tunnels. A static Cisco IP tunnel is created from ENE 1 through other vendor GNE 1 to a DCN router, and a static GRE tunnel is created from ONS ENE 2 to the other vender, GNE 2. For both static tunnels, provisioning is required on the ONS ENEs. In addition, a Cisco IP tunnel must be provisioned on the DCN router and a GRE tunnel provisioned on GNE 2.

*Figure 4-6        Static IP-Over-CLNS Tunnels*
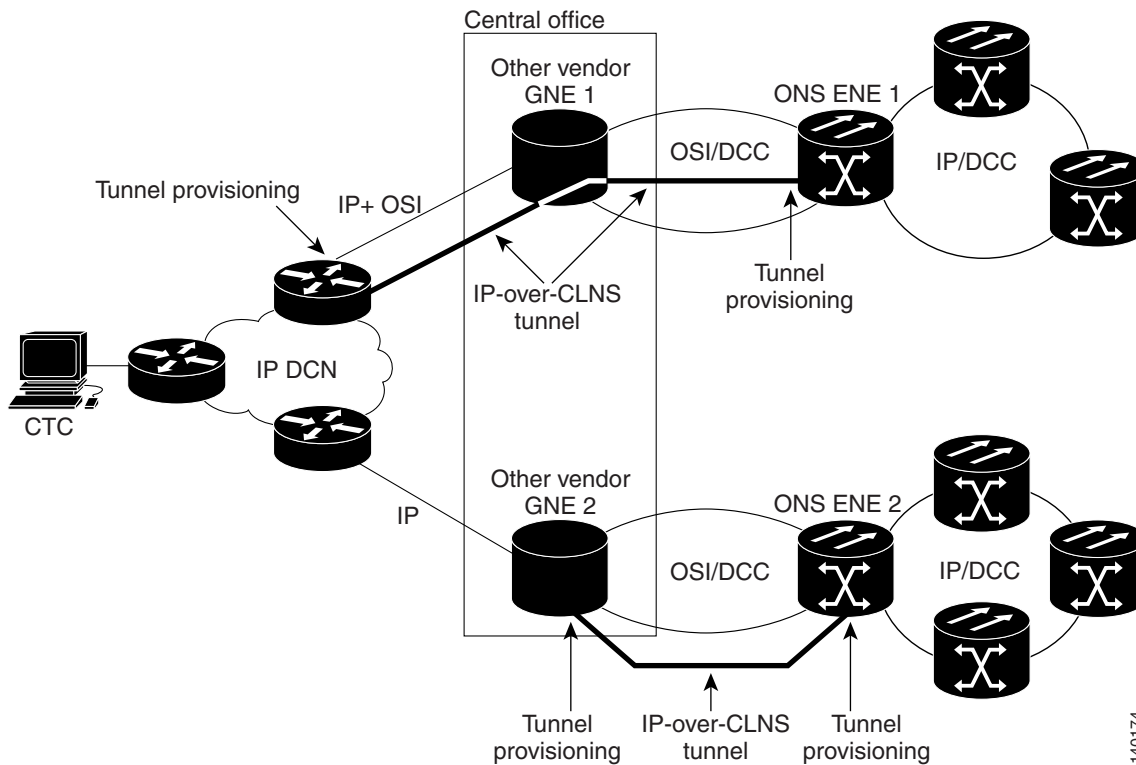


Figure 4-7 shows the same network using TL1 tunnels. Tunnel provisioning occurs at the CTC computer when the tunnel is created with the CTC Launcher. No provisioning is needed at ONS NEs, GNEs or routers.

*Figure 4-7 TL1 Tunnels*
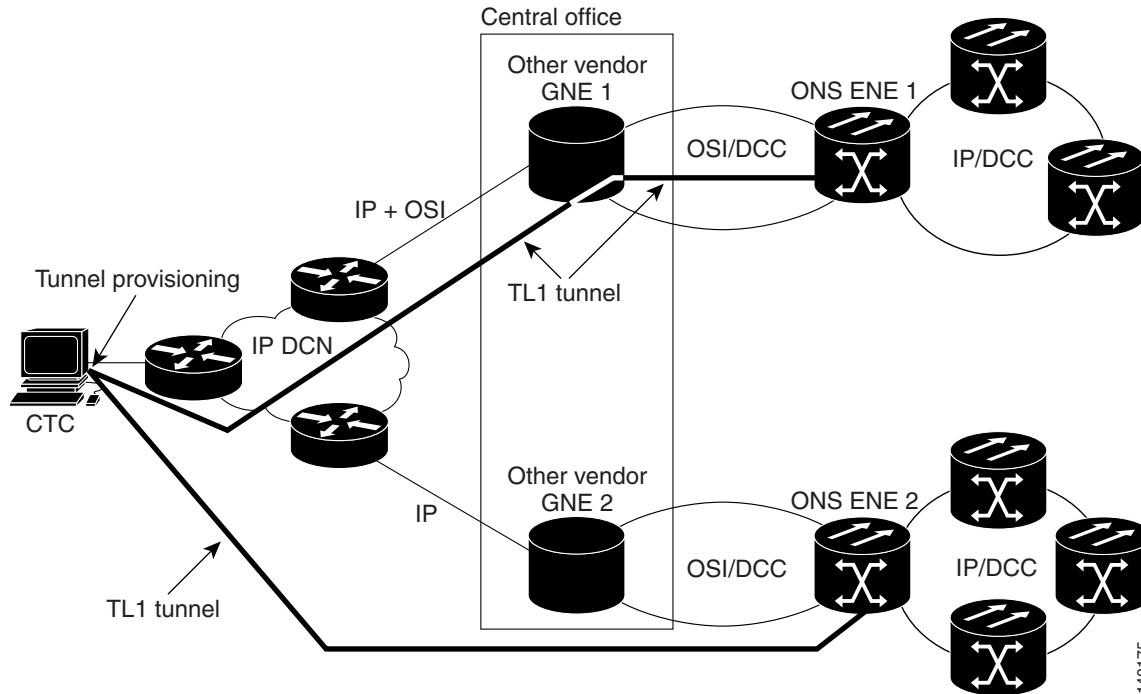


TL1 tunnels provide several advantages over static IP-over-CLNS tunnels. Because tunnel provisioning is needed only at the CTC computer, they are faster to set up. Because they use TL1 for TCP transport, they are more secure. TL1 tunnels also provide better flow control. On the other hand, IP over CLNS tunnels require less overhead and usually provide a slight performance edge over TL1 Tunnels (depending on network conditions). TL1 tunnels do not support all IP applications such as SNMP and RADIUS Authentication. Table 4-9 shows a comparison between the two types of tunnels.

*Table 4-9 TL1 and Static IP-Over-CLNS Tunnels Comparison*

| Category | Static IP-Over-CLNS | TL1 Tunnel | Comments |
|---|---|---|---|
| Setup | Complex | Simple | Requires provisioning at ONS NE, GNE, and DCN routers. For TL1 tunnels, provisioning is needed at the CTC computer. |
| Performance | Best | Average to good | Static tunnels generally provide better performance than TL1 tunnels, depending on TL1 encoding used. LV+Binary provides the best performance. Other encoding will produce slightly slower TL1 tunnel performance. |
| Support all IP applications | Yes | No | TL1 tunnels do not support SNMP or RADIUS Server IP applications. |
| ITU Standard | Yes | No | Only the static IP-over-CLNS tunnels meet ITU standards. TL1 tunnels are new. |
| Tunnel traffic control | Good | Very good | Both tunnel types provide good traffic control |
| Security setup | Complex | No setup needed | Static IP-over-CLNS tunnels require careful planning. Because TL1 tunnels are carried by TL1, no security provisioning is needed. |

*Table 4-9* **TL1 and Static IP-Over-CLNS Tunnels Comparison (continued)**

| Category | Static IP-Over-CLNS | TL1 Tunnel | Comments |
|---|---|---|---|
| Potential to breach DCN from DCC using IP | Possible | Not possible | A potential exists to breach a DCN from a DCC using IP. This potential does not exist for TL1 tunnels. |
| IP route management | Expensive | Automatic | For static IP-over-CLNS tunnels, route changes require manual provisioning at network routers, GNEs, and ENEs. For TL1 tunnels, route changes are automatic. |
| Flow control | Weak | Strong | TL1 tunnels provide the best flow control. |
| Bandwidth sharing among multiple applications | Weak | Best | — |
| Tunnel lifecycle | Fixed | CTC session | TL1 tunnels are terminated when the CTC session ends. Static IP-over-CLNS tunnels exist until they are deleted in CTC. |

TL1 tunnel specifications and general capabilities include:

- Each tunnel generally supports between six to eight ENEs, depending on the number of tunnels at the ENE.
- Each CTC session can support up to 32 tunnels.
- The TL1 tunnel database is stored locally in the CTC Preferences file.
- Automatic tunnel reconnection when the tunnel goes down.
- Each ONS NE can support at least 16 concurrent tunnels.

# 4.7 CTC Card Reset

You can reset the ONS 15600 SDH cards by using CTC (a soft reset) or by physically reseating a TSC card (a hard reset). A soft reset on the TSC reboots the TSC and reloads the operating system and the application software. Additionally, a hard reset temporarily removes power from the TSC card and clears all buffer memory.

You can apply a soft reset from CTC to either an active or standby TSC without affecting traffic. A hard reset temporarily removes power from the TSC and clears all buffer memory. You should only perform a hard reset (or a card pull) on a standby TSC. If you need to perform a CTC hard reset or card pull on an active TSC, put the TSC into standby mode first by performing a soft reset.

A soft reset on an optical card with an active port in a 1+1 protection group will result in a loss of all DCC traffic terminated or tunneled on the active port for the duration of the reset time. A soft reset of an optical card with a standby port in a 1+1 protection group will not affect DCC traffic. A CTC hard reset of an optical card causes a switch to the protect card.

# 4.8 TSC Card Database

Each TSC card hosts a separate database; therefore, the protect card's database is available if the database on the working TSC fails. After a database change, there might be a 30-second interval before the TSC starts writing the data to the Flash drive. If you reset the active TSC immediately after a database change, the change could be lost.

You can also store a backup version of the database on the workstation running CTC. This operation should be part of a regular ONS 15600 SDH maintenance program at approximately weekly intervals and should also be completed when preparing an ONS 15600 SDH for a software upgrade or a pending natural disaster, such as a flood.

**Note**   The Internet Inter-ORB Protocol (IIOP) port is not backed up and restored.

**Note**   The ONS 15600 SDH does not allow you to restore a database from one node to another node. You can install a database from one node on another node by using the Configure Node option on the **Maintenance > Database** tab.

# 4.9 Software Load Revert

Before you upgrade to Software Release 8.0, you must create a database backup. If you later need to restore the original working software load from the protect software load, CTC displays a prompt requesting the location of the backup. Any provisioning performed with Software R8.0 will be lost when the Software R1.1.x backup is restored.

**Note**   After a software load is activated (upgraded to a higher software release), any circuits created and provisioning performed will not reinstate if an older database is restored. The database configuration at the time of activation is reinstated after a revert.

**C H A P T E R 5**

# Security

This chapter provides information about Cisco ONS 15600 SDH user security. To provision security, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Chapter topics include:

## 5.1 Users IDs and Security Levels

When you log in to an ONS 15600 SDH for the first time, you use the CISCO15 user ID, which is provided with every ONS 15600 SDH system. You can use the CISCO15 ID, which has Superuser privileges, to create other ONS 15600 SDH user IDs. For detailed instructions about creating users, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Each ONS 15600 SDH permits up to 500 Cisco Transport Controller (CTC) or TL1 user IDs. A user ID is assigned one of the following security levels:

- Superuser—Users can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users.
- Provisioning—Users can access provisioning and maintenance options.
- Maintenance—Users can access only the ONS 15600 SDH maintenance options.
- Retrieve—Users can retrieve and view CTC information but cannot set or modify parameters.

See Table 5-3 on page 5-6 for idle user timeout information for each security level.

By default, multiple concurrent user ID sessions are permitted on the node, that is, multiple users can log into a node using the same user ID. However, you can provision the node to allow only a single login per user and prevent concurrent logins for all users.

## 5.2 User Privileges and Policies

This section lists user privileges for each CTC action and describes the security policies available to Superusers for provisioning.

# 5.2.1  User Privileges by Security Level

Table 5-1 shows the actions that each security level allows in node view. An "X" indicates that the action is supported on the associated security levels.

***Table 5-1     ONS 15600 SDH Security Levels—Node View***

| CTC Tab | Subtab | Actions | Retrieve | Maintenance | Provisioning | Superuser |
|---------|--------|---------|----------|-------------|--------------|-----------|
| Alarms | — | Synchronize/ Filter/ Delete cleared alarms | X | X | X | X |
| Conditions | — | Retrieve/ Filter | X | X | X | X |
| History | Session | Filter | X | X | X | X |
| | Shelf | Retrieve/ Filter alarms and events | X | X | X | X |
| Circuits | Circuits | Create/Delete | — | — | X | X |
| | | Edit/Filter/Search | X | X | X | X |
| | Rolls | Complete/ Force Valid Signal/ Finish | — | — | X | X |
| Provisioning | General | General: Edit | — | — | Partial[1] | X |
| | Network | General: Edit | — | — | — | X |
| | | Static Routing: Create/Edit/Delete | — | — | X | X |
| | | OSPF: Create/Edit/Delete | — | — | X | X |
| | | Internal Subnet: Edit/Reset | — | — | X | X |
| | | Proxy: Create/Edit/Delete | — | — | — | X |
| | | Firewall: Create/Edit/Delete | — | — | — | X |
| | OSI | Main Setup: Edit | — | — | — | X |
| | | TARP: Config: Edit | — | — | — | X |
| | | TARP: Static TDC: Add/Edit/Delete | — | — | X | X |
| | | TARP: MAT: Add/Edit/Remove | — | — | X | X |
| | | Routers: Setup: Edit | — | — | — | X |
| | | Routers: Subnets: Edit/Enable/Disable | — | — | X | X |
| | | Tunnels: Create/Edit/Delete | — | — | X | X |
| | MS-SPRing | Create/Edit/Delete/Upgrade | — | — | X | X |
| | | Ring Map/Squelch Table/RIP Table | X | X | X | X |
| | Protection | Create/Delete/Edit | — | — | X | X |

*Table 5-1*      ***ONS 15600 SDH Security Levels—Node View (continued)***

| CTC Tab | Subtab | Actions | Retrieve | Maintenance | Provisioning | Superuser |
|---|---|---|---|---|---|---|
| Provisioning (continued) | Security | Users: Create/Delete/Clear Security Intrusion | — | — | — | X |
| | | Users: Edit | Same user | Same user | Same user | All users |
| | | Active Logins: View/Logout/ Retrieve Last Activity Time | — | — | — | X |
| | | Policy: Edit/View | — | — | — | X |
| | | Access: Edit/View | — | — | — | X |
| | | RADIUS Server: Create/Edit/Delete/Move Up/Move Down/View | — | — | — | X |
| | | Legal Disclaimer: Edit | — | — | — | X |
| | SNMP | Create/Edit/Delete | — | — | X | X |
| | | Browse trap destinations | X | X | X | X |
| | Comm Channels | RS-DCC: Create/Edit/Delete | — | — | X | X |
| | | MS-DCC: Create/Edit/Delete | — | — | X | X |
| | Timing | General: Edit | — | — | X | X |
| | | BITS Facilities: Edit | — | — | X | X |
| | Alarm Profiles | Alarm Behaviour: Edit | — | — | X | X |
| | | Alarm Profile Editor: Store/Delete[2] | — | — | X | X |
| | | Alarm Profile Editor: New/Load/Compare/Available/Usage | X | X | X | X |
| | Alarm Extenders | External Alarms: Edit | — | — | X | X |
| | | External Controls: Edit | — | — | X | X |
| | Defaults | Edit/Import | — | — | — | X |
| | | Reset/Export | X | X | X | X |
| Inventory | — | Delete | — | — | X | X |
| | | Hard-reset/Soft-reset | — | X | X | X |
| Maintenance | Database | Backup | — | X | X | X |
| | | Restore | — | — | — | X |
| | Routing Table | Retrieve | X | X | X | X |
| | OSI | IS-IS RIB: Refresh | X | X | X | X |
| | | ES-IS RIB: Refresh | X | X | X | X |
| | | TDC: TID to NSAP/Flush Dynamic Entries | — | X | X | X |
| | | TDC: Refresh | X | X | X | X |
| | MS-SPRing | Edit/Reset | — | X | X | X |

*Table 5-1*     *ONS 15600 SDH Security Levels—Node View (continued)*

| CTC Tab | Subtab | Actions | Retrieve | Maintenance | Provisioning | Superuser |
|---------|--------|---------|----------|-------------|--------------|-----------|
| Maintenance (continued) | Protection | Switch/Lock out/Lockon/Clear/ Unlock | — | X | X | X |
| | Software | Download | — | X | X | X |
| | | Activate/Revert/Accept | — | — | — | X |
| | Diagnostic | Retrieve Diagnostics File | — | — | X | X |
| | | Run Diagnostics Test/Soft-reset | — | X | X | X |
| | Timing | Source: Edit | — | X | X | X |
| | | Report: View/Refresh | X | X | X | X |
| | Audit | Retrieve | — | — | — | X |
| | | Archive | — | — | X | X |
| | Test Access | View | X | X | X | X |
| | Alarm Extenders | External Alarms: View | X | X | X | X |
| | | External Controls: View | X | X | X | X |
| | | Virtual Wires: View/Retrieve | X | X | X | X |
| | | Overhead Termination: View | X | X | X | X |
| | Preferred Copy | Edit/Reset | — | — | — | X |

1. Provisioner user cannot change node name, contact, and location parameters.

2. The action buttons in the subtab are active for all users, but the actions can be completely performed only by the users assigned with the required security levels.

Table 5-2 shows the actions that each user privilege level can perform in network view.

*Table 5-2*     *ONS 15600 SDH Security Levels—Network View*

| CTC Tab | Subtab | Actions | Retrieve | Maintenance | Provisioning | Superuser |
|---------|--------|---------|----------|-------------|--------------|-----------|
| Alarms | — | Synchronize/Filter/Delete cleared alarms | X | X | X | X |
| Conditions | — | Retrieve/Filter | X | X | X | X |
| History | — | Filter | X | X | X | X |
| Circuits | Circuits | Create/Edit/Delete | — | — | X | X |
| | | Filter/Search | X | X | X | X |
| | Rolls | Complete, Force Valid Signal, Finish | — | — | X | X |

*Table 5-2* **ONS 15600 SDH Security Levels—Network View (continued)**

| CTC Tab | Subtab | Actions | Retrieve | Maintenance | Provisioning | Superuser |
|---------|--------|---------|----------|-------------|--------------|-----------|
| Provisioning | Security | Users: Create/Delete | — | — | — | X |
| | | Users: Change | Same User | Same User | Same User | All Users |
| | | Active logins: Logout/Retrieve Last Activity Time/View | — | — | — | X |
| | | Policy: Edit/View | — | — | — | X |
| | Alarm Profiles | Store/Delete[1] | — | — | X | X |
| | | New/Load/Compare/Available/Usage | X | X | X | X |
| | MS-SPRing | Create/Edit/Delete/Upgrade | — | — | X | X |
| | Overhead Circuits | Create/Delete/Edit/Merge | — | — | X | X |
| | | Search | X | X | X | X |
| | Provisionable Patchcords (PPC) | Create/Delete | — | — | X | X |
| | Server Trails | Create/Edit/Delete | — | — | X | X |
| | VLAN DB Profile | Load/Store/Merge/Circuits | X | X | X | X |
| | | Add/Remove Rows | — | — | X | X |
| Maintenance | Software | Download/Cancel | — | X | X | X |
| | Diagnostic | Retrieve/Clear | X | X | X | X |
| | APC | Run APC/Disable APC | — | — | — | X |
| | | Refresh | X | X | X | X |

1. The action buttons in the subtab are active for all users, but the actions can be completely performed only by the users assigned with the required security levels.

# 5.2.2 Security Policies

Users with Superuser security privileges can provision security policies on the ONS 15600 SDH. These security policies include idle user timeouts, password changes, password aging, and user lockout parameters.

## 5.2.2.1 Superuser Privileges for Provisioning Users

Superusers can grant permission to Provisioning users to perform a set of tasks, including retrieving the audit log, restoring a database, clearing performance monitoring (PM) parameters, activating a software load, and reverting a software load. These privileges can only be set using CTC network element (NE) defaults, except the PM clearing privilege, which can be granted using the CTC Provisioning > Security > Access tabs. For more information about setting up Superuser privileges, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

## 5.2.2.2 Idle User Timeout

Each ONS 15600 SDH CTC or TL1 user has a specified amount of time to leave the system idle before the CTC window locks. CTC lockouts prevent unauthorized users from making changes. Higher-level users have shorter idle times and lower-level users have longer or unlimited default idle periods, as shown in Table 5-3. Superusers can change user idle times on the Provisioning > Security > Policy tab.

*Table 5-3       ONS 15600 SDH User Idle Times*

| Security Level | Default Idle Time |
|----------------|-------------------|
| Superuser | 15 minutes |
| Provisioning | 30 minutes |
| Maintenance | 60 minutes |
| Retrieve | Unlimited |

## 5.2.2.3 Superuser Password and Login Privileges

A Superuser can perform ONS 15600 SDH user creation and management tasks from the network or node (default login) view. In network view, a Superuser can add, edit, or delete users from multiple nodes at one time. In node view, a Superuser can only add, edit, or delete users from that node.

Superuser password and login privilege criteria include:

- Privilege level—A Superuser can change the privilege level (such as Maintenance or Provisioning) of a user ID while the user is logged in. The change will become effective the next time the user logs in and will apply to all nodes within the network.

- Login visibility—Superusers can view real-time lists of users who are logged into a node (both CTC and TL1 logins) by retrieving a list of logins by node. A Superuser can also log out an active user.

- Password length, expiration and reuse—Superusers can configure the password length through NE defaults. The password length, by default, is set to a minimum of six and a maximum of 20. You can configure the default values in node view through Provisioning > Defaults > Node > security > passwordComplexity default selector. 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. Superusers provision password reuse periods (the number of days before a user can reuse a password) and reuse intervals (the number of passwords a user must generate before reusing a password).

- User lockout settings—A Superuser can manually lock out or unlock a user ID.

- Invalid login attempts—A Superuser sets the number of invalid login attempts a user can make before the user ID is locked out. Additionally, the Superuser sets the time interval the user ID is locked out after the user reaches the login attempt limit.

- Single Session Per User—If the Superuser provisions a user ID to be active for a single occurrence only, concurrent logins with that user ID are not allowed.

# 5.3 Audit Trail

The ONS 15600 SDH maintains an audit trail log that resides on the TSC card. This record shows who has accessed the system and what operations were performed during a given period of time. The log includes authorized Cisco logins and logouts using the operating system command line interface (CLI), CTC, and TL1; the log also includes FTP actions, circuit creation/deletion, and user/system generated actions.

Event monitoring is also recorded in the audit log. An event is defined as the change in status of an element within the network. External events, internal events, attribute changes, and software upload/download activities are recorded in the audit trail.

Audit trails are useful for maintaining security, recovering lost transactions and enforcing accountability. Accountability is the ability to trace user activities and is done by associating a process or action with a specific user. To view the audit trail log, refer to the "Manage Alarms" chapter in the *Cisco ONS 15600 SDH Procedure Guide*. Users can access the audit trail logs from any management interface (CTC, CTM, TL1).

The audit trail is stored in persistent memory and is not corrupted by processor switches, resets or upgrades. However, if a user pulls both TSC cards, the audit trail log is lost.

## 5.3.1 Audit Trail Log Entries

Audit trail records capture the following activities:

- User—Name of the user performing the action
- Host—Host from where the activity is logged
- Device ID—IP address of the device involved in the activity
- Application—Name of the application involved in the activity
- Task—Name of the task involved in the activity (View a dialog, apply configuration and so on)
- Connection Mode—Telnet, Console, SNMP
- Category—Type of change; Hardware, Software, Configuration
- Status—Status of the user action (Read, Initial, Successful, Timeout, Failed)
- Time—Time of change
- Message Type—Denotes if the event is Success/Failure type
- Message Details—A description of the change

## 5.3.2 Audit Trail Capacities

The system is able to store 640 log entries. When this limit is reached, the oldest entries are overwritten with new events. When the log server is 80 percent full, an AUD-LOG-LOW condition is raised and logged (by way of CORBA/CTC).

When the log server reaches a maximum capacity of 640 entries and begins overwriting records that were not archived, an AUD-LOG-LOSS condition is raised and logged. This event indicates that audit trail records have been lost. Until the user off-loads the file, this event occurs once regardless of the amount of entries that are overwritten by the system. To export the audit trail log, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

# 5.4 RADIUS Security

Users with Superuser security privileges can configure nodes to use Remote Authentication Dial In User Service (RADIUS) authentication. Cisco Systems uses a strategy known as authentication, authorization, and accounting (AAA) for verifying the identity of, granting access to, and tracking the actions of remote users.

## 5.4.1 RADIUS Authentication

RADIUS is a system of distributed security that secures remote access to networks and network services against unauthorized access. RADIUS comprises three components:

- A protocol with a frame format that utilizes User Datagram Protocol (UDP)/IP
- A server
- A client

The server runs on a central computer typically at the customer's site, while the clients reside in the dial-up access servers and can be distributed throughout the network.

An ONS 15600 SDH node operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and returning all configuration information necessary for the client to deliver service to the user. The RADIUS servers can act as proxy clients to other kinds of authentication servers. Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server. This eliminates the possibility that someone snooping on an unsecured network could determine a user's password. Refer to the *Cisco ONS 15600 SDH Procedure Guide* for detailed instructions for implementing RADIUS authentication.

## 5.4.2 Shared Secrets

A shared secret is a text string that serves as a password between:

- A RADIUS client and RADIUS server
- A RADIUS client and a RADIUS proxy
- A RADIUS proxy and a RADIUS server

For a configuration that uses a RADIUS client, a RADIUS proxy, and a RADIUS server, the shared secret that is used between the RADIUS client and the RADIUS proxy can be different than the shared secret used between the RADIUS proxy and the RADIUS server.

Shared secrets are used to verify that RADIUS messages, with the exception of the Access-Request message, are sent by a RADIUS-enabled device that is configured with the same shared secret. Shared secrets also verify that the RADIUS message has not been modified in transit (message integrity). The shared secret is also used to encrypt some RADIUS attributes, such as User-Password and Tunnel-Password.

When creating and using a shared secret:

- Use the same case-sensitive shared secret on both RADIUS devices.
- Use a different shared secret for each RADIUS server-RADIUS client pair.

- To ensure a random shared secret, generate a random sequence at least 22 characters long.

- You can use any standard alphanumeric and special characters.

- You can use a shared secret of up to 128 characters in length. To protect your server and your RADIUS clients from brute force attacks, use long shared secrets (more than 22 characters).

- Make the shared secret a random sequence of letters, numbers, and punctuation and change it often to protect your server and your RADIUS clients from dictionary attacks. Shared secrets should contain characters from each of the three groups listed in Table 5-4.

*Table 5-4        Shared Secret Character Groups*

| Group | Examples |
|---|---|
| Letters (uppercase and lowercase) | A, B, C, D and a, b, c, d |
| Numerals | 0, 1, 2, 3 |
| Symbols (all characters not defined as letters or numerals) | Exclamation point (!), asterisk (*), colon (:) |

The stronger your shared secret, the more secure are the attributes (for example, those used for passwords and encryption keys) that are encrypted with it. An example of a strong shared secret is 8d#>9fq4bV)H7%a3-zE13sW$hIa32M#m<PqAa72(.

CHAPTER **6**

# Timing

This chapter provides information about Cisco ONS 15600 SDH timing. To provision timing, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Chapter topics include:

## 6.1 Timing Parameters

SDH timing parameters must be set for each ONS 15600 SDH node. Each ONS 15600 SDH independently accepts its timing reference from one of three sources:

- The building integrated timing supply(BITS) pins on the Customer Access Panel (CAP/CAP2).
- A port on an STM-N card installed in the ONS 15600 SDH. The timing is traceable to a node that receives timing through a BITS source.
- The internal Stratum 3E clock (ST3E) on the TSC card.

You can set ONS 15600 SDH timing to one of three modes: external, line, or mixed. If the timing comes from BITS, set ONS 15600 SDH timing to external. If the timing comes from an STM-N port, set the timing to line. If the timing comes from both BITS and STM-N port, set ONS 15600 SDH timing to mixed. In typical ONS 15600 SDH networks:

- One node is set to external timing. The external node derives its timing from a BITS source wired to the BITS backplane pins. The BITS source, in turn, derives its timing from a Primary Reference Source (PRS), such as a Stratum 1 clock or global positioning satellite (GPS) signal.
- Other nodes are set to line timing. The line nodes derive timing from the externally timed node through the STM-N trunk cards.

You can set three timing references for each ONS 15600 SDH. The first two references are typically two BITS-level sources, or two line-level sources optically traceable to a node with a BITS source. The third reference is the internal ST3E clock provided on every ONS 15600 SDH TSC card. If an ONS 15600 SDH becomes isolated, the TSC maintains timing at the ST3E level.

# 6.2 Network Timing

Figure 6-1 shows an ONS 15600 SDH network timing example. Node 1 is set to external timing. Two timing references are Stratum 1 timing sources wired to the BITS input pins on the Node 1 backplane. The third reference is set to internal clock. The BITS output pins on the backplane of Node 3 are used to provide timing to outside equipment, such as a digital access line access multiplexer. In the event of a failure of one of the TSC modules, the redundant TSC module provides timing for BITS Out. There are some restrictions on the provisioning of BITS Out:

If the system is BITS timed:

- BITS-1 Out can have one reference if a 1+1 protected pair is chosen, or two references if unprotected line sources are chosen.

- BITS-2 Out can have one reference if a 1+1 protected pair is chosen, or two references if unprotected line sources are chosen.

If system is line timed:

- BITS-1 Out can have one unprotected line source and either or both of the network element (NE) references.

- BITS-2 Out can have one unprotected line source and either or both of the NE references.

If the system is in mixed mode:

- BITS-1 Out can have one unprotected line source and any line source selected as NE reference Ref-1 or Ref-2.

- BITS-2 Out can have one unprotected line source and any line source selected as NE reference Ref-1 or Ref-2.

In the example, Slots 11 and 12 of Node 1 contain the trunk (span) cards. Timing at Nodes 2, 3, and 4 is set to line, and the timing references are set to the trunk cards according to the distance from the BITS source. Reference 1 is set to the trunk card closest to the BITS source. At Node 2, Reference 1 is Slot 11/Port 1 because it is connected to Node 1. At Node 4, Reference 1 is set to Slot 12/Port 1 because it is connected to Node 1. At Node 3, Reference 1 could be either trunk card because they are at an equal distance from Node 1.

*Figure 6-1*      *ONS 15600 SDH Timing Example*
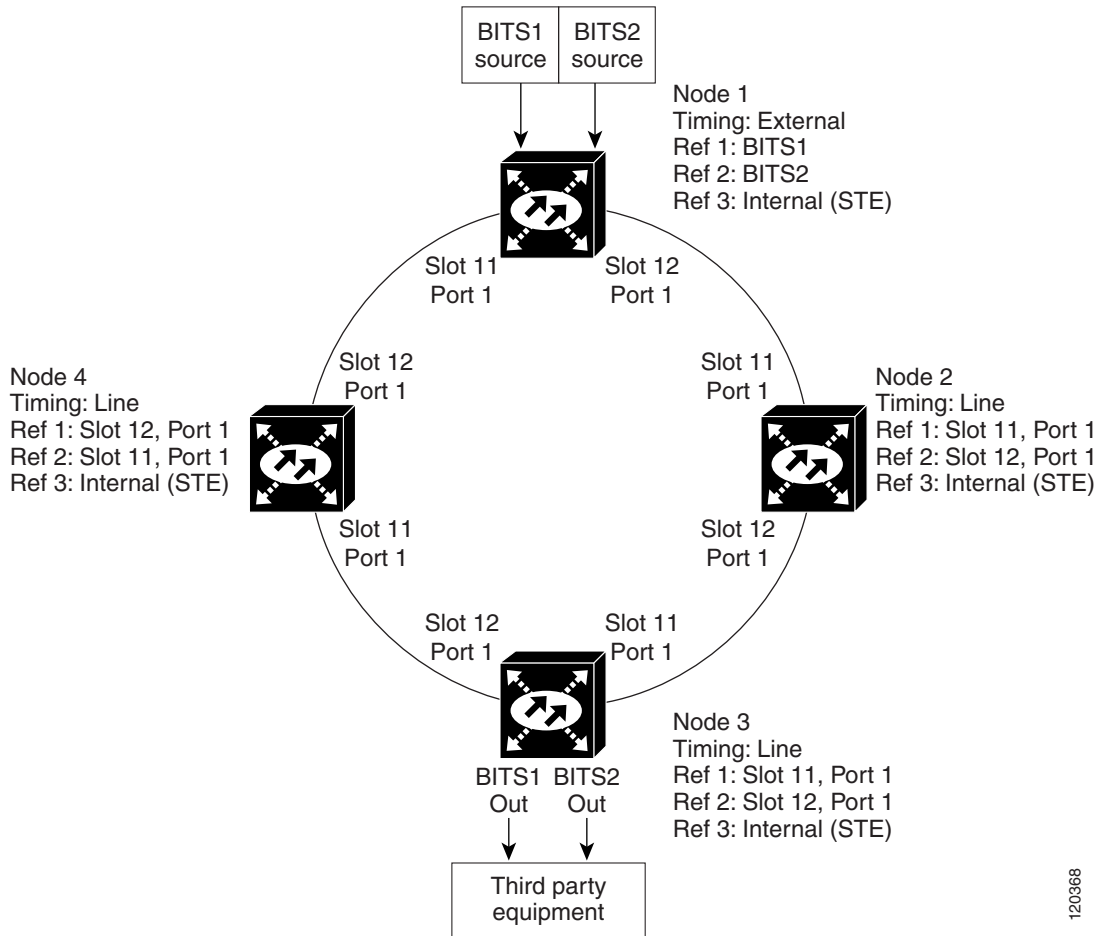


# 6.3 Synchronization Status Messaging

Synchronization status messaging (SSM) is a SONET and SDH protocol that communicates information about the quality of the timing source. SSM messages are transported as follows:

- If SSM is carried over an optical line, for both SONET and SDH the SSM is transported in the S1 byte.

- If SSM is carried over an electrical line:

  - for SDH, the SSM is transported in the Sa bit of E1.

  - for SONET, the SSM is transported in the outband loop code.

The SSM messages enable SONET and SDH devices to select the highest quality timing reference automatically and to avoid timing loops.

# 6.3.1 SONET SSM Messages

SSM messages are either Generation 1 or Generation 2. Generation 1 is the first and most widely deployed SSM message set. Generation 2 is a newer version. If you enable SONET SSM for the ONS 15600 SDH, consult your timing reference documentation to determine which message set to use. Table 6-1 and Table 6-2 show the SONET Generation 1 and Generation 2 message sets.

*Table 6-1*      *SONET SSM Generation 1 Message Set*

| Message | Quality | Description |
|---------|---------|-------------|
| PRS | 1 | Primary reference source—Stratum 1 |
| STU | 2 | Synchronization traceability unknown |
| ST2 | 3 | Stratum 2 |
| ST3 | 4 | Stratum 3 |
| SMC | 5 | SONET minimum clock |
| ST4 | 6 | Stratum 4 |
| DUS | 7 | Do not use for timing synchronization |
| RES | — | Reserved; quality level set by user |

*Table 6-2*      *SONET SSM Generation 2 Message Set*

| Message | Quality | Description |
|---------|---------|-------------|
| PRS | 1 | Primary reference source—Stratum 1 |
| STU | 2 | Synchronization traceability unknown |
| ST2 | 3 | Stratum 2 |
| TNC | 4 | Transit node clock |
| ST3E | 5 | Stratum 3E |
| ST3 | 6 | Stratum 3 |
| SMC | 7 | SONET minimum clock |
| ST4 | 8 | Stratum 4 |
| DUS | 9 | Do not use for timing synchronization |
| RES | — | Reserved; quality level set by user |

# 6.3.2 SDH SSM Messages

If you enable SDH SSM for the ONS 15600 SDH, consult your timing reference documentation to determine which message set to use.

✎ **Note**     Mapping from DS1 SSM to E1 SSM is possible when DS1 timing is used on the 15600 SDH platform.

Table 6-3 shows the SDH SSM messages.

*Table 6-3*        **SDH SSM Messages**

| Message | Quality | Description |
| --- | --- | --- |
| G811 | 1 | Primary reference clock |
| STU | 2 | Sync traceability unknown |
| G812T | 3 | Transit node clock traceable |
| G812L | 4 | Local node clock traceable |
| SETS | 5 | Synchronous equipment |
| DUS | 6 | Do not use for timing synchronization |

**C H A P T E R 7**

# Circuits and Tunnels

This chapter explains Cisco ONS 15600 SDH high-order circuits, data communications channel (DCC), and IP-encapsulated tunnels. To provision circuits and tunnels, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Chapter topics include:

**Note** In this chapter, "cross-connect" and "circuit" have the following meanings: cross-connect refers to the connections that occur within a single ONS 15600 SDH to allow a circuit to enter and exit an ONS 15600 SDH. Circuit refers to the series of connections from a traffic source (where traffic enters the ONS 15600 SDH network) to the destination (where traffic exits an ONS 15600 SDH network).

# 7.1 Overview

You can create circuits across and within ONS 15600 SDH nodes and assign different attributes to circuits. For example, you can:

- Create one-way, two-way (bidirectional), or broadcast circuits.
- Assign user-defined names to circuits.
- Assign different circuit sizes.
- Automatically or manually route circuits.
- Automatically create multiple circuits with autoranging.
- Provide full protection to the circuit path.
- Provide only protected sources and destinations for circuits.
- Define a secondary circuit source or destination that allows you to interoperate an ONS 15600 SDH subnetwork connection protection (SNCP) ring with third-party equipment SNCPs.
- Set SNCP circuits as revertive or nonrevertive.

You can provision circuits at any of the following points:

- Before cards are installed. The ONS 15600 SDH allows you to provision slot and circuits before installing the traffic cards.
- After you preprovision the Small Form-factor Pluggables (SFPs) (also called provisionable port modules [PPMs]).
- After cards and SFPs are installed and ports are enabled. Circuits do not actually carry traffic until the cards and SFPs are installed and the ports are in the Unlocked-enabled state; the Locked-enabled,maintenance state; or the Unlocked-disabled,automaticInService state. Circuits carry traffic as soon as the signal is received.

# 7.2 Circuit Properties

The ONS 15600 SDH Circuits window (Figure 7-1 on page 7-3), which is available from network, node, and card view, is where you can view information about circuits, including:

- Name—The name of the circuit (user-assigned or automatically generated).
- Type—For the ONS 15600 SDH, the circuit type is HOP (high-order circuit).
- Size—The circuit size can be VC3, VC4, VC4-4c, VC4-8c, VC4-16c, or VC4-64c. ASAP optical ports also allow circuit sizes of VC4-2c and VC4-3c. For time slot availability on concatenated VCs, see the "7.2.1 Concatenated VC4 Time Slot Assignments" section on page 7-4.
- Protection—The protection type; see the "7.2.4 Circuit Protection Types" section on page 7-8.
- Direction—The circuit direction, either two-way or one-way.
- Status—The circuit status; for details, see the "7.2.2 Circuit Status" section on page 7-6.
- Source—The circuit source in the format: *node/slot/port/virtual container*. If an ASAP PPM port is the circuit source, the port format is *PIM-PPM-port*, where pluggable interface module (PIM) and PPM values are 1 through 4 (for example, p1-1-1). PPMs have only one port.
- Destination—The circuit destination in the format: *node/slot/port/virtual container*. If an ASAP PPM port is the circuit destination, the port format is *PIM-PPM-port*, where PIM and PPM values are 1 through 4 (for example, p1-1-1). PPMs have only one port.

- # of VLANS—(Future use) The number of VLANs used by an Ethernet circuit.

- # of Spans—The number of internode links that constitute the circuit. Right-clicking the column shows a shortcut menu from which you can choose Span Details to show or hide circuit span detail. For each node in the span, the span detail shows the *node/slot (card type)/port/virtual container*.

- State—The circuit state; for details, see the "7.2.3 Circuit States" section on page 7-7.

The Filter button allows you to filter the circuits in network, node, or card view based on circuit name, size, type, direction, and other attributes. In addition, you can export the Circuit window data in HTML, comma-separated values (CSV), or tab-separated values (TSV) format using the Export command from the File menu.

*Figure 7-1      ONS 15600 SDH Circuit Window in Network View*



The Circuit Filter feature allows you to reduce the number of circuits that appear in the Circuits window. You can specify certain filter criteria, such as name, direction, and state; only the circuits that match the criteria will appear in the Circuits window.

**Note**      You cannot set up low-order circuits to terminate on an ONS 15600 SDH node. However, you can create both high-order and low-order circuits that have an ONS 15454 SDH source and destination with an ONS 15600 SDH as a pass-through node. For information, see the "7.18 Low-Order Traffic Routing over an ONS 15600 SDH Hub Node" section on page 7-27.

## 7.2.1 Concatenated VC4 Time Slot Assignments

Table 7-1 shows the available time slot assignments for concatenated VC4s when using Cisco Transport Controller (CTC) to provision circuits.

*Table 7-1*        *VC4 Mapping Using CTC*

| Starting VC4 | VC4 | VC4-2c | VC4-3c | VC4-4c | VC4-6c | VC4-8c | VC4-12c | VC4-16c | VC4-64c |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| 2 | Yes | Yes | Yes | No | Yes | Yes | Yes | No | No |
| 3 | Yes | Yes | No | No | Yes | Yes | Yes | No | No |
| 4 | Yes | No | Yes | No | Yes | Yes | Yes | No | No |
| 5 | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| 6 | Yes | Yes | Yes | No | Yes | Yes | No | No | No |
| 7 | Yes | Yes | Yes | No | Yes | Yes | No | No | No |
| 8 | Yes | No | No | No | Yes | Yes | No | No | No |
| 9 | Yes | Yes | Yes | Yes | Yes | Yes | No | No | No |
| 10 | Yes | Yes | Yes | No | Yes | No | No | No | No |
| 11 | Yes | Yes | No | No | Yes | No | No | No | No |
| 12 | Yes | No | No | No | No | No | No | No | No |
| 13 | Yes | Yes | Yes | Yes | Yes | No | Yes | No | No |
| 14 | Yes | Yes | Yes | No | No | No | No | No | No |
| 15 | Yes | Yes | No | No | No | No | No | No | No |
| 16 | Yes | No | Yes | No | No | No | No | No | No |
| 17 | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| 18 | Yes | Yes | Yes | No | Yes | Yes | Yes | No | No |
| 19 | Yes | Yes | Yes | No | Yes | Yes | Yes | No | No |
| 20 | Yes | No | No | No | Yes | Yes | Yes | No | No |
| 21 | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| 22 | Yes | Yes | Yes | No | Yes | Yes | No | No | No |
| 23 | Yes | Yes | No | No | Yes | Yes | No | No | No |
| 24 | Yes | No | No | No | Yes | Yes | No | No | No |
| 25 | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| 26 | Yes | Yes | Yes | No | Yes | No | No | No | No |
| 27 | Yes | Yes | No | No | Yes | No | No | No | No |
| 28 | Yes | No | Yes | No | No | No | No | No | No |
| 29 | Yes | Yes | Yes | Yes | No | No | No | No | No |
| 30 | Yes | Yes | Yes | No | No | No | No | No | No |
| 31 | Yes | Yes | Yes | No | Yes | No | No | No | No |

*Table 7-1      VC4 Mapping Using CTC (continued)*

| Starting VC4 | VC4 | VC4-2c | VC4-3c | VC4-4c | VC4-6c | VC4-8c | VC4-12c | VC4-16c | VC4-64c |
|---|---|---|---|---|---|---|---|---|---|
| 32 | Yes | No | No | No | No | No | No | No | No |
| 33 | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| 34 | Yes | Yes | Yes | No | Yes | Yes | Yes | No | No |
| 35 | Yes | Yes | No | No | Yes | Yes | Yes | No | No |
| 36 | Yes | No | No | No | Yes | Yes | Yes | No | No |
| 37 | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| 38 | Yes | Yes | Yes | No | Yes | Yes | No | No | No |
| 39 | Yes | Yes | No | No | Yes | Yes | No | No | No |
| 40 | Yes | No | Yes | No | Yes | Yes | No | No | No |
| 41 | Yes | Yes | Yes | Yes | Yes | Yes | No | No | No |
| 42 | Yes | Yes | Yes | No | Yes | No | No | No | No |
| 43 | Yes | Yes | Yes | No | Yes | No | No | No | No |
| 44 | Yes | No | No | No | No | No | No | No | No |
| 45 | Yes | Yes | Yes | Yes | No | No | No | No | No |
| 46 | Yes | Yes | Yes | No | No | No | No | No | No |
| 47 | Yes | Yes | No | No | No | No | No | No | No |
| 48 | Yes | No | No | No | No | No | No | No | No |
| 49 | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| 50 | Yes | Yes | Yes | No | Yes | Yes | Yes | No | No |
| 51 | Yes | Yes | No | No | Yes | Yes | Yes | No | No |
| 52 | Yes | No | Yes | No | Yes | Yes | Yes | No | No |
| 53 | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| 54 | Yes | Yes | Yes | No | Yes | Yes | No | No | No |
| 55 | Yes | Yes | Yes | No | Yes | Yes | No | No | No |
| 56 | Yes | No | No | No | Yes | Yes | No | No | No |
| 57 | Yes | Yes | Yes | Yes | Yes | Yes | No | No | No |
| 58 | Yes | Yes | Yes | No | Yes | No | No | No | No |
| 59 | Yes | Yes | No | No | Yes | No | No | No | No |
| 60 | Yes | No | No | No | No | No | No | No | No |
| 61 | Yes | Yes | Yes | Yes | Yes | No | No | No | No |
| 62 | Yes | Yes | Yes | No | Yes | No | No | No | No |
| 63 | Yes | Yes | No | No | Yes | No | No | No | No |
| 64 | Yes | No | No | No | Yes | No | No | No | No |

## 7.2.2 Circuit Status

The circuit statuses that appear in the Circuit window Status column are generated by CTC based on an assessment of conditions along the circuit path. Table 7-2 shows the statuses that can appear in the Status column.

*Table 7-2* **ONS 15600 SDH 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 connection or circuit span (network link), or a complete path from source to destination(s) 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, a PARTIAL status does not necessarily mean a circuit traffic failure has occurred, because traffic might flow on a protect path. |
| | Network spans are in one of two states: up or down. On CTC circuit and network maps, up spans 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 Transaction Language One (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 destination(s) does not exist. |
| CONVERSION_PENDING | An existing circuit in a topology upgrade is set to this state. The circuit returns to the DISCOVERED state when the topology upgrade is complete. For more information about topology upgrades, see Chapter 8, "SDH Topologies and Upgrades." |

*Table 7-2* *ONS 15600 SDH 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 it is a temporary circuit. These circuits can be deleted if a topology upgrade fails. For more information about topology upgrades, see Chapter 8, "SDH Topologies and Upgrades." |
| DROP_PENDING | A circuit is set to this status when a new circuit drop is being added. |

# 7.2.3 Circuit States

The circuit service state is an aggregate of the cross-connect states within the circuit.

- If all cross-connects in a circuit are in the Unlocked-enabled service state, the circuit service state is Unlocked.

- If all cross-connects in a circuit are in the Locked-enabled,maintenance, Locked-enabled,disabled service state, or the Unlocked-disabled,automaticInService state, the circuit service state is Locked.

- Partial is appended to the Locked circuit service state when circuit cross-connect state are mixed and not all in the Unlocked-enabled service state. The Locked-partial state can occur during automatic or manual transitions between states. The Locked-partial service state can appear during a manual transition caused by an abnormal event such as a CTC crash or communication error, or if one of the cross-connects could not be changed. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for troubleshooting procedures. The Locked-partial circuit state does not apply to optical channel network connection (OCHNC) circuit types.

You can assign a service state to circuit cross-connects at two points:

- During circuit creation, you can set the state on the Create Circuit wizard.

- After circuit creation, you can change a circuit state in the Edit Circuit window or from the Tools > Circuits > Set Circuit State menu.

**Note** After you have created an initial circuit in a CTC session, the subsequent circuit states default to the circuit state of the initial circuit, regardless of which nodes in the network the circuits traverse or the node.ckt.state default setting.

During circuit creation, you can apply a service state to the drop ports in a circuit. You cannot transition a port from the Unlocked-enabled service state to the Locked-enabled,disabled state. You must first transition the port to the Locked-enabled,maintenance state before changing it to the Locked-enabled,disabled state. For more information about port service state transitions, see Appendix B, "Administrative and Service States."

Circuits do not use the soak timer, but ports do. The soak period is the amount of time that the port remains in the Unlocked-disabled,automaticInService service state after a signal is continuously received. When the cross-connects in a circuit are in the Unlocked-disabled,automaticInService service state, the ONS 15600 SDH monitors the cross-connects for an error-free signal. It changes the state of the circuit from Locked to Unlocked or to Locked-partial as each cross-connect assigned to the circuit path is completed. This allows you to provision a circuit using TL1, verify its path continuity, and prepare the port to go into service when it receives an error-free signal for the time specified in the port soak timer.

To find the remaining port soak time, choose the Maintenance > AINS Soak tabs in card view and click the Retrieve button. If the port is in the Unlocked-disabled,automaticInService state and has a good signal, the Time Until IS column shows the soak count-down status. If the port is Unlocked-disabled,automaticInService and has a bad signal, the Time Until IS column indicates that the signal is bad. You must click the Retrieve button to obtain the latest time value.

For more information about cross-connect states, see Appendix B, "Administrative and Service States."

## 7.2.4 Circuit Protection Types

The Protection column in the Circuit window shows the card (line) and SDH topology (path) protection used for the entire circuit path. Table 7-3 lists the protection type indicators that you will see in this column.

*Table 7-3      Circuit Protection Types*

| Protection Type | Description |
| --- | --- |
| 1+1 | The circuit is protected by a 1+1 protection group. |
| 2F MS-SPRing | The circuit is protected by a two-fiber MS-SPRing. |
| 2F-PCA | The circuit is routed on a protection channel access (PCA) path on a two-fiber MS-SPRing. PCA circuits are unprotected. |
| DRI | The circuit is protected by dual-ring interconnect (DRI). |
| N/A | A circuit with connections on the same node is not protected. |
| Protected | The circuit is protected by diverse SDH topologies, for example, an MS-SPRing and an SNCP, or an SNCP and 1+1. |
| Unknown | A circuit has a source and destination on different nodes and communication is down between the nodes. This protection type appears if not all circuit components are known. |
| Unprot (black) | A circuit with a source and destination on different nodes is not protected. |
| Unprot (red) | A circuit created as a fully protected circuit is no longer protected due to a system change, such as removal of an MS-SPRing or 1+1 protection group. |
| SNCP | The circuit is protected by an SNCP. |

## 7.2.5 Circuit Information in the Edit Circuit Window

You can edit a selected circuit using the Edit button on the Circuits window. The tabs that appear depend on the circuit chosen:

- General—Displays general circuit information and allows you to edit the circuit name.
- Drops—Allows you to add a drop to a unidirectional circuit. For more information, see the "7.5 Multiple Destinations for Unidirectional Circuits" section on page 7-12.
- SNCP Selectors—Allows you to change SNCP selectors. For more information, see the "7.6 SNCP Circuits" section on page 7-12.
- SNCP Switch Counts—Allows you to change SNCP switch protection paths. For more information, see the "7.6 SNCP Circuits" section on page 7-12.

- State—Allows you to edit cross-connect service states.
- Merge—Allows you to merge aligned circuits. For more information, see the "7.14 Merged Circuits" section on page 7-24.

Using the Export command from the File menu, you can export data from the SNCP Selectors, SNCP Switch Counts, State, and Merge tabs in HTML, comma-separated values (CSV), or tab-separated values (TSV) format.

The Show Detailed Map check box in the Edit Circuit window updates the graphical view of the circuit to show more detailed routing information in the map area, such as:

- The circuit direction (unidirectional or bidirectional)
- The node names
- The slot and port numbers
- The circuit source and drop

The pane area shows:

- The circuit name, type, and size
- The protection type (SNCP, unprotected, MS-SPRing, 1+1) and routing preferences such as fully protected path
- Open Shortest Path First (OSPF) area IDs

For MS-SPRings, the detailed map shows the number of MS-SPRing fibers and the MS-SPRing ring ID. For SNCPs, the map shows the active and standby paths from circuit source to destination, and it also shows the working and protect paths. Selectors appear as pentagons on the detailed circuit map.

Alarms and states can also be viewed on the circuit map, including:

- Alarm states of nodes on the circuit route
- Number of alarms on each node organized by severity
- Port service states on the circuit route
- Alarm state/color of most severe alarm on port
- Loopbacks
- Path trace states
- Path selector states

By default, the working path is indicated by a green, bidirectional arrow, and the protect path is indicated by a purple, bidirectional arrow. Source and destination ports are shown as circles with an S and D, respectively. Port states are indicated by colors, shown in Table 7-4.

*Table 7-4        Port State Color Indicators*

| Port Color | Service State |
|---|---|
| Green | Unlocked-enabled |
| Gray | Locked-enabled,disabled |
| Violet | Unlocked-disabled,automaticInService |
| Blue (Cyan) | Locked-enabled,maintenance |

A notation within or by the squares or selector pentagons in detailed view indicates switches and loopbacks, including:

- F = Force switch
- M = Manual switch
- L = Lockout switch
- Arrow = Facility (outward) or terminal (inward) loopback

Figure 7-2 shows an example of the Edit Circuit window with a terminal loopback.

*Figure 7-2        Detailed Circuit Map Showing a Terminal Loopback*
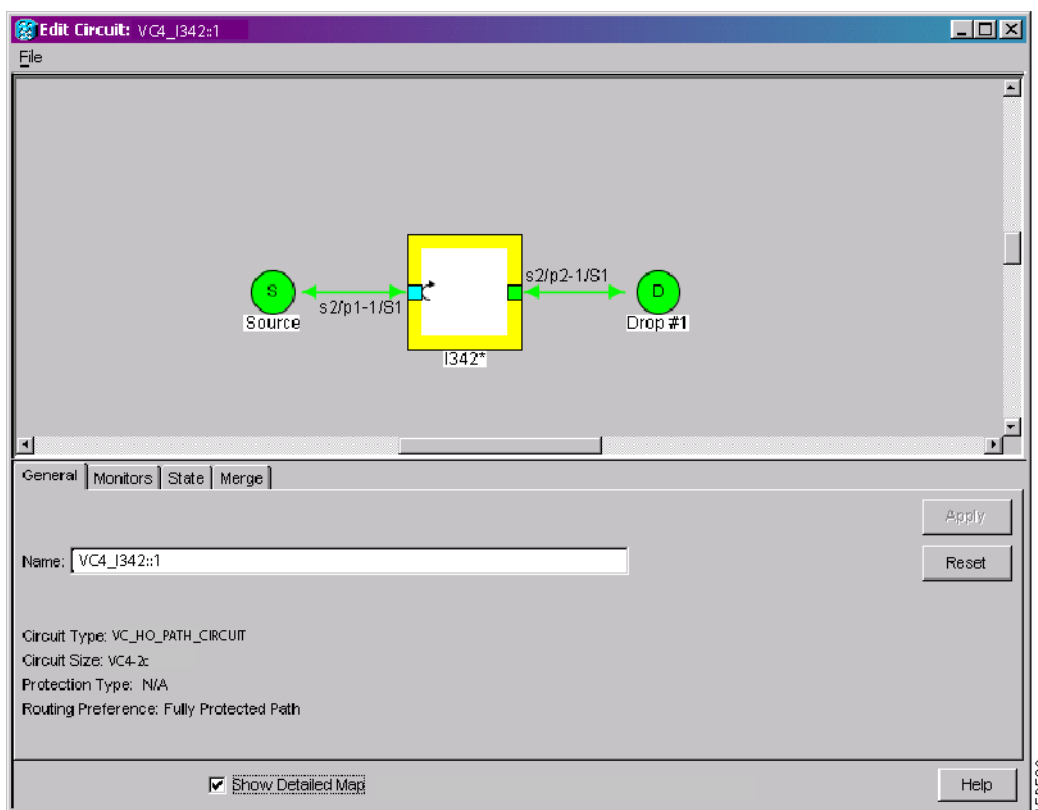
Move the mouse cursor over nodes, ports, and spans to see tooltips with information including the number of alarms on a node (organized by severity), a port's service state, and the protection topology.

Right-click a node, port, or span on the detailed circuit map to initiate certain circuit actions:

- Right-click a unidirectional circuit destination node to add a drop to the circuit.
- Right-click a port containing a path-trace-capable card to initiate the path trace.
- Right-click an SNCP span to change the state of the path selectors in the SNCP circuit.

# 7.3 Cross-Connect Card Bandwidth

The single shelf cross-connect card (SSXC) performs port-to-port time-division multiplexing (TDM). The VC matrix has the capacity for 2048 VC4 and/or 6144 VC3 terminations. Because each VC4/VC3 circuit requires a minimum of two terminations, one for ingress and one for egress, the SSXC has a capacity for 1024 VC4 and 3072 VC3 circuits respectively. However, this capacity is reduced at SNCP and 1+1 nodes because three VC4/VC3 terminations are required at circuit source and destination nodes and four terminations are required at 1+1 circuit pass-through nodes. SNCP pass-through nodes only require two VC4/VC3 terminations.

# 7.4 DCC Tunnels

SDH provides four data communications channels (DCCs) for network element operations, administration, maintenance, and provisioning (OAM&P): one on the SDH Section layer (DCC1) and three on the SDH Line layer (DCC2, DCC3, DCC4). The ONS 15600 SDH uses the regenerator-section DCC (RS-DCC) for ONS 15600 SDH management and provisioning. An RS-DCC and multiplex-section (MS-DCC) each provide 192 Kbps of bandwidth per channel. The aggregate bandwidth of the three MS-DCCs is 576 Kbps. You can tunnel third-party SDH equipment across ONS 15600 SDH networks using one of two tunneling methods, a traditional DCC tunnel or an IP-encapsulated tunnel.

## 7.4.1 Traditional DCC Tunnels

In traditional DCC tunnels, you can use the three MS-DCCs and the RS-DCC (when not used for ONS 15600 SDH DCC terminations). A DCC tunnel endpoint is defined by slot, port, and DCC, where DCC can be either the RS-DCC or one of the MS-DCCs. You can link MS-DCCs to MS-DCCs and link RS-DCCs to RS-DCCs. You can also link an RS-DCC to an MS-DCC and an MS-DCC to an RS-DCC. To create a DCC tunnel, connect the tunnel endpoints from one ONS 15600 SDH optical port to another. Table 7-5 lists the DCC tunnels that you can create.

*Table 7-5        DCC Tunnels*

| DCC | SDH Layer | SDH Bytes |
|------|-----------|-----------|
| DCC1 | RS-DCC | D1 to D3 |
| DCC2 | MS-DCC | D4 to D6 |
| DCC3 | MS-DCC | D7 to D9 |
| DCC4 | MS-DCC | D10 to D12 |

When you create DCC tunnels, keep the following guidelines in mind:

- Each ONS 15600 SDH can have up to 64 DCC tunnel connections.
- An RS-DCC that is terminated cannot be used as a DCC tunnel endpoint.
- An RS-DCC that is used as an DCC tunnel endpoint cannot be terminated.
- All DCC tunnel connections are bidirectional.

## 7.4.2 IP-Encapsulated Tunnels

An IP-encapsulated tunnel puts an RS-DCC in an IP packet at a source node and dynamically routes the packet to a destination node. To compare traditional DCC tunnels with IP-encapsulated tunnels, a traditional DCC tunnel is configured as one dedicated path across a network and does not provide a failure recovery mechanism if the path is down. An IP-encapsulated tunnel is a virtual path, which adds protection when traffic travels between different networks.

IP-encapsulated tunneling has the potential of flooding the DCC network with traffic resulting in a degradation of performance for CTC. The data originating from an IP tunnel can be throttled to a user-specified rate, which is a percentage of the total RS-DCC bandwidth.

Each ONS 15600 SDH supports up to 128 IP-encapsulated tunnels. You can convert a traditional DCC tunnel to an IP-encapsulated tunnel or an IP-encapsulated tunnel to a traditional DCC tunnel. Only tunnels in the DISCOVERED status can be converted.

⚠

**Caution**    Converting from one tunnel type to the other is service-affecting.

# 7.5  Multiple Destinations for Unidirectional Circuits

Unidirectional circuits can have multiple destinations (drops) for use in broadcast circuit schemes. In broadcast scenarios, one source transmits traffic to multiple destinations, but traffic is not returned to the source. The ONS 15600 SDH supports one of the following:

- Up to 2048 1:2 nonblocking broadcast connections
- Up to 682 1:*n* nonblocking broadcast connections (where *n* is less than or equal to 8)

When you create a unidirectional circuit, the card that does not have its backplane receive (Rx) input terminated with a valid input signal generates a Loss of Signal (LOS) alarm. To mask the alarm, create an alarm profile suppressing the LOS alarm and apply the profile to the port that does not have its Rx input terminated. To create an alarm profile, refer to the "Manage Alarms" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

# 7.6  SNCP Circuits

Use the Edit Circuit window to change SNCP selectors and switch protection paths (Figure 7-3). In the SNCP Selectors subtab in the Edit Circuits window, you can:

- View the SNCP circuit's working and protection paths.
- Edit the reversion time.
- Set the hold-off timer.
- Edit the Signal Fail (SF) and Signal Degrade (SD) thresholds.

✎

**Note**    In the SNCP Selectors tab, the SF Ber Level and SD Ber Level columns display "N/A" for those nodes that do not support low-order path signal bit error rate (BER) monitoring.

From the SNCP Switch Counts subtab, you can:

- Perform maintenance switches on the circuit selector.

• View switch counts for the selectors.

*Figure 7-3 Editing SNCP Selectors*
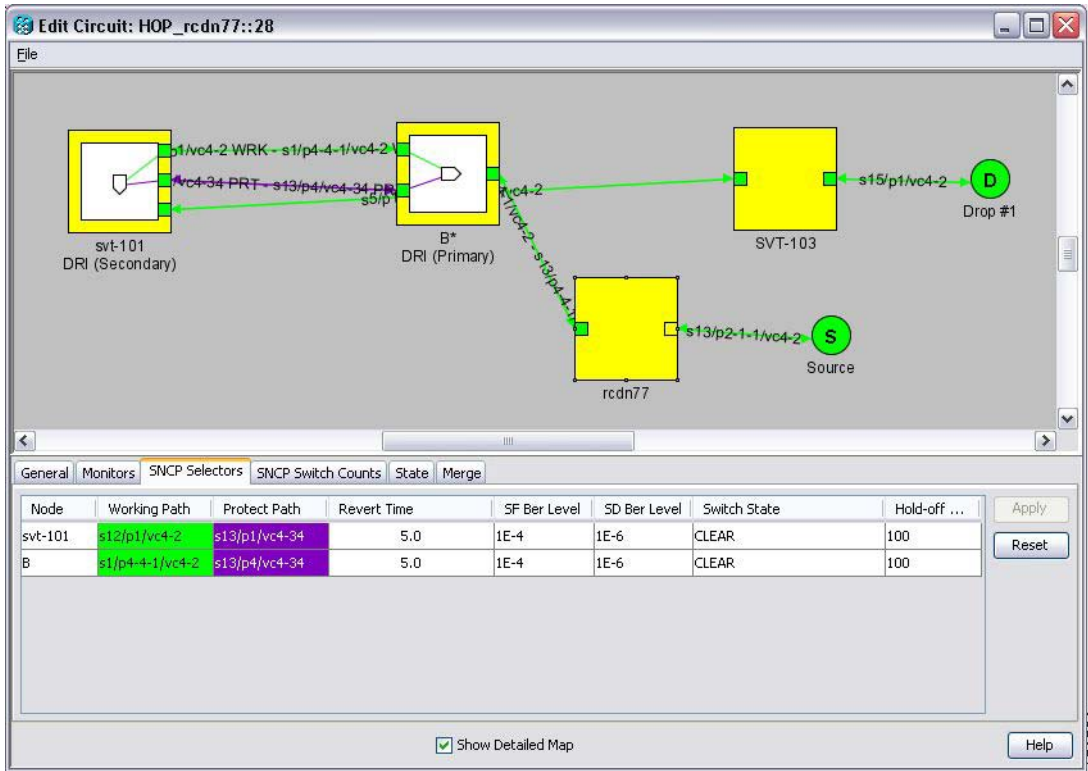


On the SNCP Switch Counts tab, you can view switch counts for the selectors (Figure 7-4).

*Figure 7-4 Viewing SNCP Switch Counts*
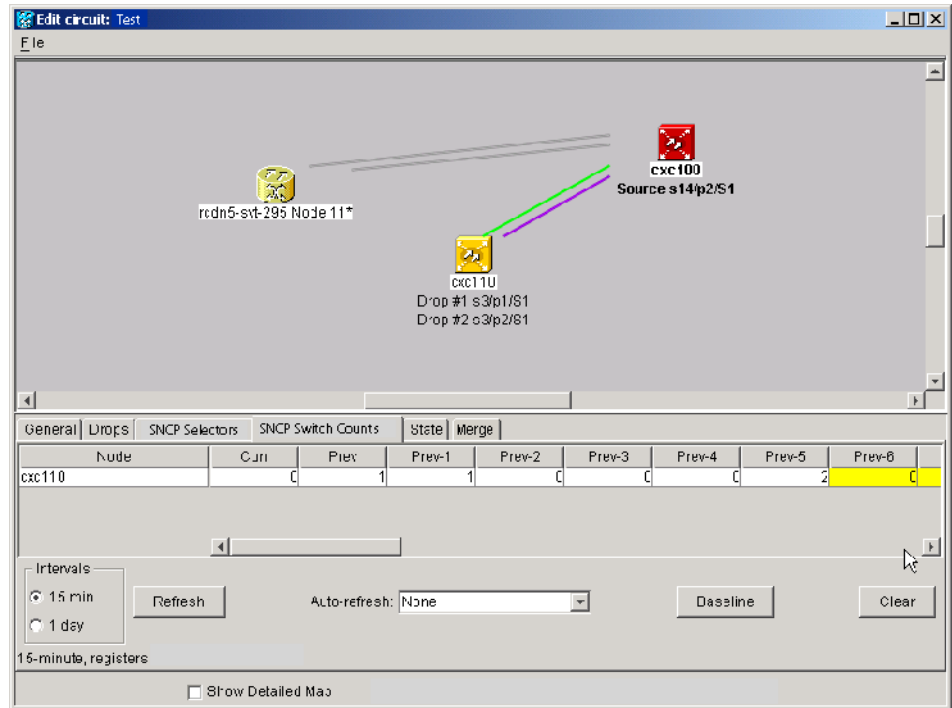


In network view, you can right-click on a span and choose the Circuits command to open the Circuits on Span dialog box. Use the Circuits on Span dialog box to view circuit span usage information and, for SNCP spans, to perform span switches and lockouts.

# 7.7 Protection Channel Access Circuits

You can provision circuits to carry traffic on MS-SPRing protection channels when conditions are fault-free and set up MS-SPRing diagnostic test circuits. Traffic routed on MS-SPRing PCA circuits, called extra traffic, has lower priority than the traffic on the working channels and has no means for protection. During ring or span switches, PCA circuits are preempted and squelched. For example, in a two-fiber STM-16 MS-SPRing, STMs 9 to 16 can carry extra traffic when no ring switches are active, but PCA circuits on these STMs are preempted when a ring switch occurs. When the conditions that caused the ring switch are resolved and the ring switch is removed, PCA circuits are restored. If the MS-SPRing is provisioned as revertive, this occurs automatically after the fault conditions are cleared and the reversion timer has expired.

Traffic provisioning on MS-SPRing protection channels is performed during circuit provisioning. The Protection Channel Access check box appears whenever Fully Protected Path is unchecked in the circuit creation wizard. Refer to the *Cisco ONS 15600 SDH Procedure Guide* for more information. When provisioning PCA circuits, two considerations are important to keep in mind:

- If MS-SPRings are provisioned as nonrevertive, PCA circuits are not restored automatically after a ring or span switch. You must switch the MS-SPRing manually.

- PCA circuits are routed on working channels when you upgrade a MS-SPRing from one optical speed to a higher optical speed. For example, if you upgrade a two-fiber STM-16 MS-SPRing to an STM-64, STMs 9 to 16 on the STM-16 MS-SPRing become working channels on the STM-64 MS-SPRing.

# 7.8  MS-SPRing VC4/VC3 Squelch Table

The ONS 15600 SDH platform does not support low-order path squelching; however, when an ONS 15454 SDH and an ONS 15600 SDH are in the same network, the ONS 15600 SDH node allows the ONS 15454 SDH node to carry low-order path circuits in a VC_LO_PATH_TUNNEL. The ONS 15600 SDH performs 100-ms VC4-level squelching for each low-order-access VC at the switching node in case of a node failure.

- SDH-AU4—Displays all circuits with SDH-AU4 format (VC4 or VC4-*n*c high-order circuits). For example, if "Circuit1" is a high-order VC4 circuit using ring bandwidth VC4-2c, then "Circuit1" appears in the SDH-AU4 pane in the column "vc4=2."

- SDH-AU3—Displays all circuits with SDH-AU3 format (VC3 high-order circuits).

- VC4/VC3 Number—The SDH-AU4 pane shows VC4 number only, and the SDH-AU3 pane shows VC3 number only.

- West Source—If traffic is received by the node on its west span, the MS-SPRing node ID of the source appears. (To view the MS-SPRing node IDs for all nodes in the ring, click the Ring Map button.)

- West Dest—If traffic is sent on the node's west span, the MS-SPRing node ID of the destination appears.

- East Source—If traffic is received by the node on its east span, the MS-SPRing node ID of the source appears.

- East Dest—If traffic is sent on the node's east span, the MS-SPRing node ID of the destination appears.

- Retrieve—Retrieves the most current squelch table display.

**Note**  MS-SPRing squelching is performed on VC4s that carry VC4 circuits only or on VC3s that carry VC3 circuits only.

# 7.9  Section and Path Trace

SDH J0 section and J1 path trace are repeated, fixed-length strings used to monitor interruptions or changes to circuit traffic. J0 section trace inlcudes 1 or 16 consecutive J0 bytes. All ONS 15600 SDH optical cards and ports support J0 path trace. J1 path trace includes 16 consecutive J1 bytes. If the string received at a circuit drop port does not match the string the port expects to receive, the Trace Identifier Mismatch Path (TIM-P) alarm is raised.

Table 7-6 lists the ONS 15600 SDH cards that support J1 path trace.

*Table 7-6*        ***ONS 15600 SDH Cards Supporting J1 Path Trace***

| Card | Receive | Transmit |
|------|---------|----------|
| OC48/STM16 SR/SH 16 Port 1310 | Yes | No |
| OC48/STM16 LR/LH 16 Port 1550 | Yes | No |
| OC192/STM64 SR/SH 4 Port 1310 | Yes | No |
| OC192/STM64 LR/LH 4 Port 1550 | Yes | No |
| OC192LR/STM64 4 Port ITU C-Band | Yes | No |

**Table 7-6** *ONS 15600 SDH Cards Supporting J1 Path Trace (continued)*

| Card | Receive | Transmit |
|------|---------|----------|
| ASAP STM-N ports | Yes | No |
| ASAP Ethernet ports | Yes | Yes |

The ONS 15600 SDH supports both automatic and manual J1 path trace monitoring to detect and report the contents of the 16-byte path trace message (nonterminated) for the designated path.

- Automatic—The receiving port assumes that the first J1 string it receives is the baseline J1 string.

- Manual—The receiving port uses a string that you manually enter as the baseline J1 string.

**Note** When J1 path trace is enabled on a two-fiber MS-SPRing circuit, CTC will not retrieve the path trace information from the card view Maintenance > Path Trace tab.

# 7.10 Automatic Circuit Routing

If you select automatic routing during circuit creation, CTC routes the circuit by dividing the entire circuit route into segments based on protection domains. For unprotected segments of circuits provisioned as fully protected, CTC finds an alternate route to protect the segment, creating a virtual SNCP. Each segment of a circuit path is a separate protection domain. Each protection domain is protected in a specific protection scheme including 1+1, SNCP, or MS-SPRing.

The following list provides principles and characteristics of automatic circuit routing:

- Circuit routing tries to use the shortest path within the user-specified or network-specified constraints.

- If you do not choose fully path protected during circuit creation, circuits can still contain protected segments. Because circuit routing always selects the shortest path, one or more links and/or segments can have some protection. CTC does not look at link protection while computing a path for unprotected circuits.

- Circuit routing does not use links that are down. If you want all links to be considered for routing, do not create circuits when a link is down.

- Circuit routing computes the shortest path when you add a new drop to an existing circuit. It tries to find the shortest path from the new drop to any nodes on the existing circuit.

## 7.10.1 Bandwidth Allocation and Routing

Within a given network, CTC routes circuits on the shortest possible path between source and destination based on the circuit attributes, such as protection and type. CTC considers using a link for the circuit only if the link meets the following requirements:

- The link has sufficient bandwidth to support the circuit.

- The link does not change the protection characteristics of the path.

- The link has the required time slots to enforce the same time slot restrictions for MS-SPRing.

If CTC cannot find a link that meets these requirements, an error appears.

## 7.10.2 Secondary Sources and Destination

CTC supports secondary sources and destinations (drops). Secondary sources and destinations typically interconnect two third-party networks, as shown in Figure 7-5. Traffic is protected while it traverses a network of ONS 15600 SDHs.

*Figure 7-5        Secondary Sources and Drops*
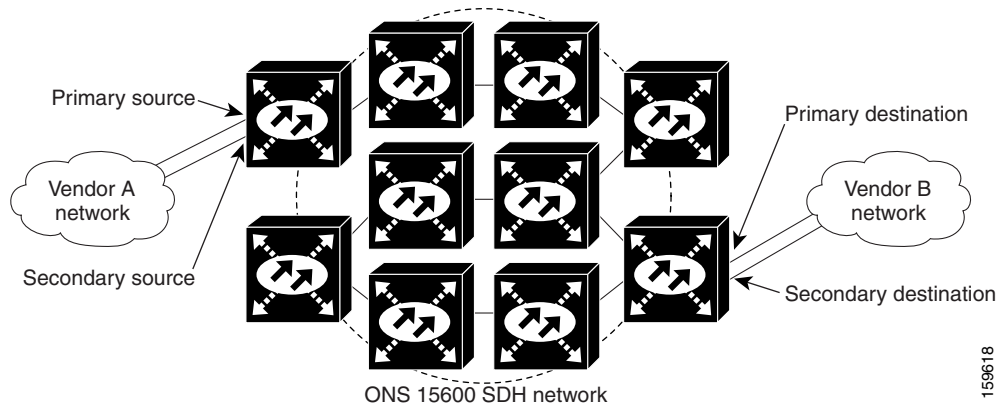


Several rules apply to secondary sources and destinations:

- CTC does not allow a secondary destination for unidirectional circuits because you can specify additional destinations after you create the circuit.

- Primary and secondary sources should be on the same node.

- Primary and secondary destinations should be on the same node.

- Secondary sources and destinations are permitted only for regular VC4 connections.

For bidirectional circuits, CTC creates an SNCP connection at the source node that allows traffic to be selected from one of the two sources on the ONS 15600 SDH network. If you check the Fully Path Protected option during circuit creation, traffic is protected within the ONS 15600 SDH network. At the destination, another SNCP connection is created to bridge traffic from the ONS 15600 SDH network to the two destinations. A similar but opposite path exists for the reverse traffic flowing from the destinations to the sources.

For unidirectional circuits, an SNCP drop-and-continue connection is created at the source node.

**Note** Automatic routing and its associated subfields are not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see Appendix C, "Network Element Defaults."

# 7.11 Manual Circuit Routing

Routing circuits manually allows you to:

- Choose a specific path, not just the shortest path chosen by automatic routing.

- Choose a specific VC4 on each link along the route.

CTC imposes the following rules on manual routes:

- All circuits in a shared packet ring should have links with a direction that flows from source to destination.

- If you enabled Fully Protected Path, choose a diverse protect (alternate) path for every unprotected segment.

- For a node that has an SNCP selector based on the links chosen, the input links to the SNCP selectors cannot be 1+1 protected. The same rule applies at the SNCP bridge.

If you enabled Fully Protected Path, CTC verifies that the route selection is protected at all segments. A route can have multiple protection domains with each domain protected by a different scheme.

Table 7-7 summarizes the available bidirectional connections. Any other combination is invalid and generates an error.

*Table 7-7      Bidirectional VC4 Circuits*

| No. of Inbound Links | No. of Outbound Links | No. of Sources | No. of Drops | Connection Type |
|---|---|---|---|---|
| — | 2 | 1 | — | SNCP |
| 2 | — | — | 1 | SNCP |
| 2 | 1 | — | — | SNCP |
| 1 | 2 | — | — | SNCP |
| 1 | — | — | 2 | SNCP |
| — | 1 | 2 | — | SNCP |
| 2 | 2 | — | — | Double SNCP |
| 2 | — | — | 2 | Double SNCP |
| — | 2 | 2 | — | Double SNCP |
| 1 | 1 | — | — | Two-way |

Table 7-8 summarizes the available unidirectional connections. Any other combination is invalid and generates an error.

*Table 7-8      Unidirectional VC4 Circuits*

| No. of Inbound Links | No. of Outbound Links | No. of Sources | No. of Drops | Connection Type |
|---|---|---|---|---|
| 1 | 1 | — | — | One-way |
| 1 | 2 | — | — | SNCP head end |
| — | 2 | 1 | — | SNCP head end |
| 2 | — | — | 1+ | SNCP drop and continue |

# 7.12 Constraint-Based Circuit Routing

When you create circuits, you can choose Fully Protected Path to protect the circuit from source to destination. The protection mechanism used depends on the path that CTC calculates for the circuit. If the network is comprised entirely of MS-SPRing or 1+1 links, or the path between source and destination can be entirely protected using 1+1 or MS-SPRing links, no extended SNCP, or virtual SNCP, protection is used.

If extended SNCP protection is needed to protect the path, set the level of node diversity for the extended SNCP portions of the complete path on the Circuit Routing Preferences area of the Circuit Creation dialog box:

- Nodal Diversity Required—Ensures that the primary and alternate paths of each extended SNCP domain in the complete path have a diverse set of nodes.

- Nodal Diversity Desired—CTC looks for a node-diverse path; if a node-diverse path is not available, CTC finds a link-diverse path for each extended SNCP domain in the complete path.

- Link Diversity Only—Creates only a link diverse path for each extended SNCP domain.

When you choose automatic circuit routing during circuit creation, you have the option to require or exclude nodes and links in the calculated route. You can use this option to achieve the following results:

- Simplify manual routing, especially if the network is large and selecting every span is tedious. You can select a general route from source to destination and allow CTC to fill in the route details.

- Balance network traffic; by default CTC chooses the shortest path, which can load traffic on certain links while other links are either free or use less bandwidth. By selecting a required node and/or a link, you force CTC to use (or not use) an element, resulting in more efficient use of network resources.

CTC considers required nodes and links to be an ordered set of elements. CTC treats the source nodes of every required link as required nodes. When CTC calculates the path, it makes sure the computed path traverses the required set of nodes and links and does not traverse excluded nodes and links.

The required nodes and links constraint is used only during the primary path computation and only for extended SNCP domains/segments. The alternate path is computed normally; CTC uses excluded nodes/links when finding all primary and alternate paths on extended SNCPs.

# 7.13 Bridge and Roll

The CTC Bridge and Roll wizard reroutes live traffic without interrupting service. The bridge process takes traffic from a designated "roll from" facility and establishes a cross-connect to the designated "roll to" facility. When the bridged signal at the receiving end point is verified, the roll process creates a new cross-connect to receive the new signal. When the roll completes, the original cross-connects are released. You can use the bridge and roll feature for maintenance functions such as card or facility replacement, or for load balancing. You can perform a bridge and roll on the following ONS platforms: ONS 15600 SDH, ONS 15600, ONS 15454, ONS 15454 SDH, ONS 15310-MA, and ONS 15310-CL.

## 7.13.1 Rolls Window

The Rolls window lists information about a rolled circuit before the roll process is complete. You can access the Rolls window by clicking the Circuits > Rolls tabs in either network or node view. Figure 7-6 shows the Rolls window.

**Figure 7-6 Rolls Window**
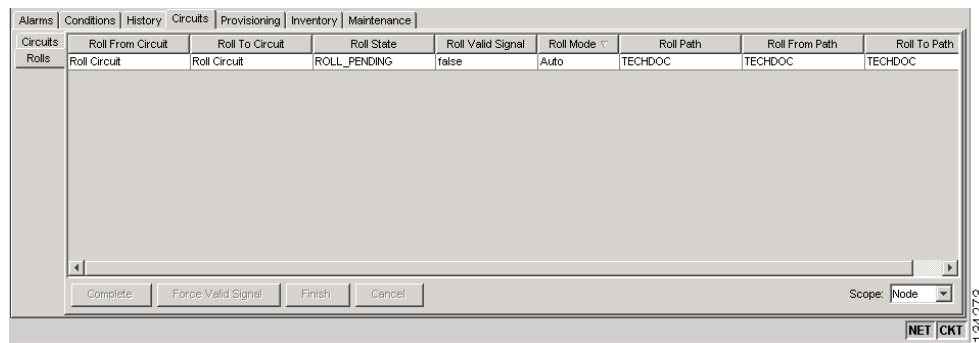


The Rolls window information includes:

- Roll From Circuit—The circuit with connections that will no longer be used when the roll process is complete.

- Roll To Circuit—The circuit that will carry the traffic when the roll process is complete. The Roll To Circuit is the same as the Roll From Circuit if a single circuit is involved in a roll.

- Roll State—The roll status; see the "7.13.2 Roll Status" section on page 7-21 for information.

- Roll Valid Signal—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. It is not possible to get a true Roll Valid Signal status for a one-way destination roll.

- Roll Mode—The mode indicates whether the roll is automatic or manual.

  CTC implements a roll mode at the circuit level. TL1 implements a roll mode at the cross-connect level. If a single roll is performed, CTC and TL1 behave the same. If a dual roll is performed, the roll mode specified in CTC might be different than the roll mode retrieved in TL1. For example, if you select Automatic, CTC coordinates the two rolls to minimize possible traffic hits by using the Manual mode behind the scenes. When both rolls have a good signal, CTC signals the nodes to complete the roll.

  - Automatic—When a valid signal is received on the new path, CTC completes the roll on the node automatically. One-way source rolls are always automatic.

  - Manual—You must complete a manual roll after a valid signal is received. One-way destination rolls are always manual.

- Roll Path—The fixed point of the roll object.

- Roll From Path— The old path that is being rerouted.

- Roll To Path—The new path where the Roll From Path is rerouted.

- Complete—Completes a manual roll after a valid signal is received. You can complete a manual roll if it is in a ROLL_PENDING status and you have not yet completed the roll or have not cancelled its sibling roll.

- Force Valid Signal—Forces a roll onto the Roll To Circuit destination without a valid signal. If you choose Force Valid Signal, traffic on the circuit that is involved in the roll will be dropped once the roll is completed.

- Finish—Completes the circuit processing of both manual and automatic rolls and changes the circuit status from ROLL_PENDING to DISCOVERED. After a roll, the Finish button also removes any cross-connects that are no longer used from the Roll From Circuit field.

- Cancel—Cancels the roll process. When the roll mode is Manual, cancel roll is only allowed 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 you click the Force Valid Signal button.

## 7.13.2  Roll Status

Table 7-9 lists the roll statuses. You can only reroute circuits that have a DISCOVERED status. (See Table 7-2 on page 7-6 for a list of circuit statuses.) You cannot reroute circuits that are in the ROLL_PENDING status.

*Table 7-9      Roll Statuses*

| State | Description |
|-------|-------------|
| ROLL_PENDING | The roll is awaiting completion or cancellation. |
| ROLL_COMPLETED | The roll is complete. Click the Finish button. |
| ROLL_CANCELLED | The roll has been canceled. |
| TL1_ROLL | A TL1 roll was initiated. |
| | **Note**   If a roll is created using TL1, a CTC user cannot complete or cancel the roll. Also, if a roll is created using CTC, a TL1 user cannot complete or cancel the roll. You must use the same interface to complete or change a roll. |
| INCOMPLETE | This state appears when the underlying circuit becomes incomplete. To correct this state, you must fix the underlying circuit problem before the roll state will change. |
| | For example, a circuit traveling on Nodes A, B, and C can become INCOMPLETE if Node B is rebooted. The cross connect information is lost on Node B during a reboot. The Roll State on Nodes A and C will change to INCOMPLETE. |

## 7.13.3  Single and Dual Rolls

Circuits have an additional layer of roll types: single and dual. A single roll on a circuit is a roll on one of its cross-connects. Use a single roll to:

- Change either the source or destination of a selected circuit (Figure 7-7 on page 7-22 and Figure 7-8 on page 7-22, respectively).
- Roll a segment of the circuit onto another chosen circuit (Figure 7-9 on page 7-22). This roll also results in a new destination or a new source.

In Figure 7-7, you can select any available VC4 on Node 1 for a new source.

**Figure 7-7**       *Single Source Roll*
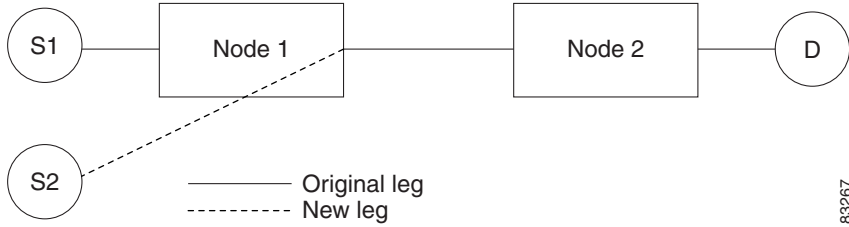


In Figure 7-8, you can select any available VC4 on Node 2 for a new destination.

**Figure 7-8**       *Single Destination Roll*
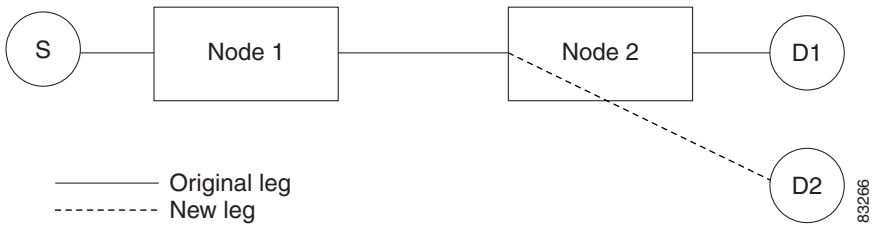


Figure 7-9 shows one circuit rolling onto another circuit at the destination. The new circuit has cross-connects on Node 1, Node 3, and Node 4. CTC deletes the cross-connect on Node 2 after the roll.

**Figure 7-9**       *Single Roll from One Circuit to Another Circuit (Destination Changes)*
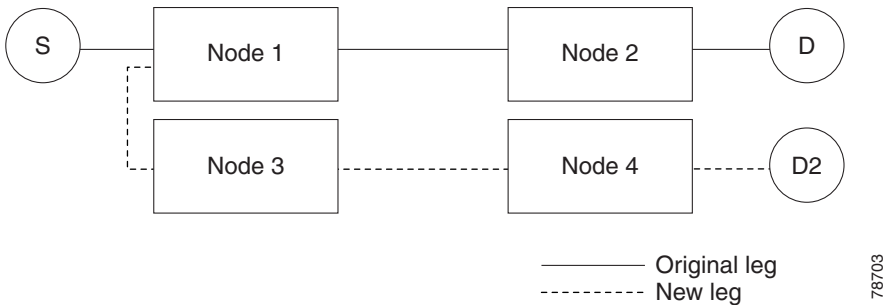


Figure 7-10 shows one circuit rolling onto another circuit at the source.

**Figure 7-10**       *Single Roll from One Circuit to Another Circuit (Source Changes)*
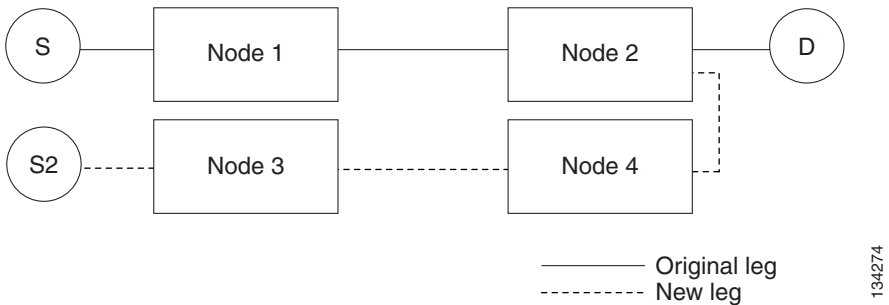
**Note** Create a Roll To Circuit before rolling a circuit with the source on Node 3 and the destination on Node 4.

A dual roll involves two cross-connects. It allows you to reroute intermediate segments of a circuit, but keep the original source and destination. If the new segments require new cross-connects, use the Bridge and Roll wizard or create a new circuit and then perform a roll.

**Caution** Only single rolls can be performed using TL1. Dual rolls require the network-level view that only CTC or CTM provide.

Dual rolls have several constraints:

- You must complete or cancel both cross-connects rolled in a dual roll. You cannot complete one roll and cancel the other roll.

- When a Roll To circuit is involved in the dual roll, the first roll must roll onto the source of the Roll To circuit and the second roll must roll onto the destination of the Roll To circuit.

Figure 7-11 illustrates a dual roll on the same circuit.

*Figure 7-11*     *Dual Roll to Reroute a Link*
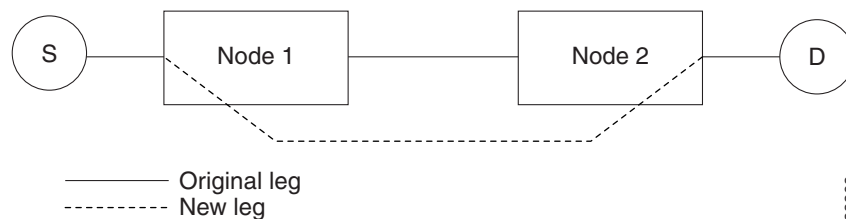


Figure 7-12 illustrates a dual roll involving two circuits.

*Figure 7-12*     *Dual Roll to Reroute to a Different Node*
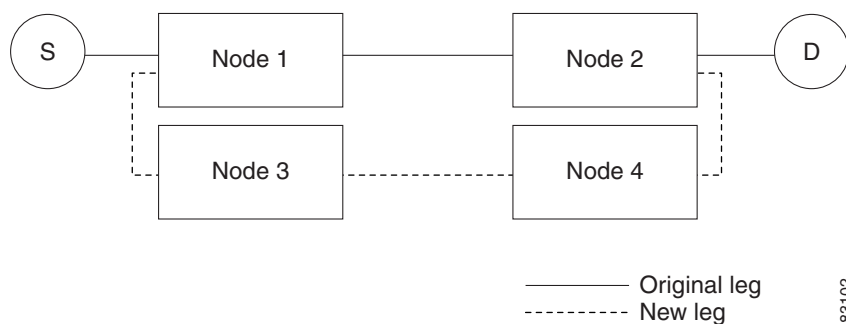


**Note** If a new segment is created on Nodes 3 and 4 using the Bridge and Roll wizard, the created circuit has the same name as the original circuit with the suffix _ROLL**. The circuit source is on Node 3 and the circuit destination is on Node 4.

## 7.13.4  Two Circuit Bridge and Roll

When using the bridge and roll feature to reroute traffic using two circuits, the following constraints apply:

- DCC must be enabled on the circuits involved in a roll before roll creation.

- A maximum of two rolls can exist between any two circuits.

- If two rolls are involved between two circuits, both rolls must be on the original circuit. The second circuit should not carry live traffic. The two rolls loop from the second circuit back to the original circuit. The roll mode of the two rolls must be identical (either automatic or manual).

- If a single roll exists on a circuit, you must roll the connection onto the source or the destination of the second circuit and not an intermediate node in the circuit.

## 7.13.5  Protected Circuits

CTC allows you to roll the working or protect path regardless of which path is active. You can upgrade an unprotected circuit to a fully protected circuit or downgrade a fully protected circuit to an unprotected circuit with the exception of an SNCP circuit. When using bridge and roll on SNCP circuits, you can roll the source or destination or both path selectors in a dual roll. However, you cannot roll a single path selector.

# 7.14  Merged Circuits

A circuit merge combines a single selected circuit with one or more circuits. You can merge CTC-created circuits and TL1-created circuits. To merge circuits, you choose a circuit in the CTC Circuits window and the circuits that you want to merge with the chosen (master) circuit on the Merge tab in the Edit Circuit window. The Merge tab shows only the circuits that are available for merging with the master circuit:

- Circuit cross-connects must create a single, contiguous path.

- Circuits types must be a compatible.

- Circuit directions must be compatible. You can merge a one-way and a two-way circuit, but not two one-way circuits in opposing directions.

- Circuit sizes must be identical.

- Circuit end points must send or receive the same framing format.

- The merged circuits must become a DISCOVERED circuit.

If all connections from the master circuit and all connections from the merged circuits align to form one complete circuit, the merge is successful. If all connections from the master circuit and some, but not all, connections from the other circuits align to form a single complete circuit, CTC notifies you and gives you the chance to cancel the merge process. If you choose to continue, the aligned connections merge successfully into the master circuit, and unaligned connections remain in the original circuits. All connections in the completed master circuit use the original master circuit name.

All connections from the master circuit and at least one connection from the other selected circuits must be used in the resulting circuit for the merge to succeed. If a merge fails, the master circuit and all other circuits remain unchanged. When the circuit merge completes successfully, the resulting circuit retains the name of the master circuit.

# 7.15 Reconfigured Circuits

You can reconfigure multiple circuits, which is typically necessary when a large number of circuits are in the PARTIAL status. When you reconfigure multiple circuits, the selected circuits can be any combination of DISCOVERED, PARTIAL, DISCOVERED_TL1, and PARTIAL_TL1 circuits. You can reconfigure tunnels, CTC-created circuits, and TL1-created circuits. The Reconfigure command maintains the names of the original cross-connects.

Use the CTC Tools > Circuits > Reconfigure Circuits command to reconfigure selected circuits. During reconfiguration, CTC reassembles all connections of the selected circuits into circuits based on path size, direction, and alignment. Some circuits might merge and others might split into multiple circuits. If the resulting circuit is a valid circuit, it appears as a DISCOVERED circuit. Otherwise, the circuit appears as a PARTIAL or PARTIAL_TL1 circuit.

**Note** PARTIAL tunnel circuits do not split into multiple circuits during reconfiguration.

# 7.16 Server Trails

A server trail is a non-DCC (logical or virtual) link across a third-party network that connects two CTC network domains. A server trail allows A-Z circuit provisioning when no DCC is available. You can create server trails between two distant optical or STM-1E ports. The end ports on a server trail can be different types (for example, an STM-4 port can be linked to an STM-1 port). Server trails are not allowed on DCC-enabled ports.

The server trail link is bidirectional and can be VC3, VC11, VC12, VC4, VC4-2c, VC4-3c, VC4-4c, VC4-6c, VC4-8c, VC4-12c, VC4-16c, VC4-32c, and VC4-64c; you cannot change an existing server trail to another size. It must be deleted and recreated. A circuit provisioned over a server trail must match the type and size of the server trail it uses. For example, an VC4-3c server trail can carry only VC4-3c circuits and not three VC4 circuits.

**Note** There is no OSPF or any other management information exchange between NEs over a server trail.

## 7.16.1 Server Trail Protection Types

The server trail protection type determines the protection type for any circuits that traverse it. A server trail link can be one of the following protection types:

- 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.

**Note** Only SNCP protection is available on server trails. MS-SPRing procection is not available on server trail.

## 7.16.2  VCAT Circuit Routing over Server Trails

An VC4-3c server trail can be used to route VC4-3c circuits and an VC4 server trail can be used to route VC4 circuits. Similarly, a VC3 server trail can be used to route VC3 circuits.

For example, to route a VC4-3c-2v circuit over a server trail, you must enable split fiber routing and create two VC4-3c server trails and route each member manually or automatically over each server trail. To route a VC4-12c-2v circuit over a server trail, you must enable split fiber routing and create two VC4 server trails and route each member manually or automatically over each server trail.

**Note**    Server trails can only be created between any two optical ports or STM-1E ports.

VCAT circusits can be created over server trails in the following ways:

- Manual routing
- Automatic routing
    - Diverse routing: This method enables VCAT circuit routing over diverse server trail links.

**Note**    When creating circuits or VCATs, you can choose a server trail link during manual circuit routing. CTC may also route circuits over server trail links during automatic routing. VCAT common-fiber automatic routing is not supported.

For a detailed procedure on how to route a VCAT circuit over a server trail, refer "Chapter 6, Create Circuits and VT Tunnels, Section NTP-A264, Create an Automatically Routed VCAT Circuit and Section NTP-A265, Create a Manually Routed VCAT Circuit" in the *Cisco ONS 15454 Procedure Guide*.

### 7.16.2.1  Shared Resource Link Group

The Shared Resource Link Group (SRLG) attribute can be assigned to a server trail link using a commonly shared resource such as port, fiber or span. For example, if two server trail links are routed over the same fiber, an SRLG attribute can be assigned to these links. SRLG is used by Cisco Transport Manager (CTM) to specify link diversity. 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.

# 7.17  Traffic Routing over a Third-Party Network

If ONS 15600 SDHs are connected to a third-party network, you can create an open-ended SNCP circuit to route a circuit through it. To do this, you create three circuits. One circuit is created on the source ONS 15600 SDH network. This circuit has one source and two destinations, one at each ONS 15600 SDH that is connected to the third-party network. The second circuit is created on the third-party network so that the circuit travels across the network on two paths to the ONS 15600 SDHs. That circuit routes the two circuit signals across the network to ONS 15600 SDHs that are connected to the network on other side. At the destination node network, the third circuit is created with two sources, one at each node connected to the third-party network. A selector at the destination node chooses between the two signals that arrive at the node, similar to a regular SNCP circuit.

# 7.18 Low-Order Traffic Routing over an ONS 15600 SDH Hub Node

When an ONS 15600 SDH node is configured as a hub between compatible protection domains, it is possible to use CTC to automatically create circuits, including low-order circuits from an ONS 15454 SDH node, across the domains. Low-order circuits cannot terminate on an ONS 15600 SDH node. All combinations of protection domains are compatible for high-order circuits, including combinations of SNCP and line-protected domains.

When you must route low-order traffic over an ONS 15600 SDH hub node connecting SNCP, line-protected, and unprotected domains, you must manually create the circuits for this traffic. For specific information on ONS 15454 SDH low-order circuit creation and tunneling, refer to the circuit chapters in the *Cisco ONS 15454 SDH Reference Manual*.

Figure 7-13 shows an ONS 15600 SDH as a protection domain hub between a ONS 15454 SDH SNCP network, an ONS 15454 SDH MS-SPRing network, and a 1+1 protected ONS 15454 SDH node.

*Figure 7-13        ONS 15600 SDH as Hub Node between Protection Domains*
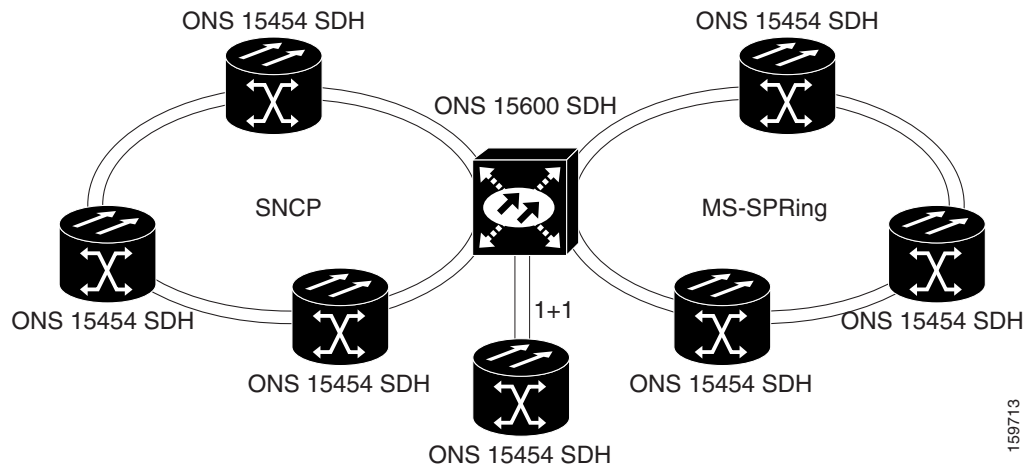


## 7.18.1 Automatic Low-Order Circuit Creation

To route low-order traffic across an ONS 15600 SDH for compatible protection domains, you must create a low-order tunnels on an ONS 15454 SDH node or create an end-to-end circuit. If you create an end-to-end circuit, CTC automatically creates a tunnel to route the low-order traffic. You can create circuits or tunnels with an ONS 15600 SDH as a hub node for the following domain combinations:

- SNCP to SNCP
- 1+1 to 1+1
- MS-SPRing to MS-SPRing
- 1+1 to MS-SPRing
- Unprotected to MS-SPRing

Once the tunnel or end-to-end circuit exists, additional low-order circuits can be routed until all of the bandwidth is used. The tunnel source and destination are the low-order circuit source and destination, and when created results in the creation of high-order pass-through circuits on each node in the path. For any of the listed topology combinations except SNCP to SNCP, one tunnel is required; an SNCP-to-SNCP topology requires two tunnels.

## 7.18.2 Manual Low-order Circuit Creation

When you must route low-order traffic from an ONS 15454 SDH SNCP across an ONS 15600 SDH hub to a line-protected domain, CTC cannot automatically create the end-to-end low-order circuit. The configuration requires three TL1-like circuits. You must create all three circuits separately:

1. Low-order open-ended circuit on the ONS 15454 SDH SNCP

2. STS open-ended circuit on the ONS 15600 SDH hub node

3. Low-order two-way circuit on the ONS 15454 SDH line-protected node

The three TL1-like circuits must physically align for CTC to automatically merge the circuits. Figure 7-14 is an example of an ONS 15600 SDH node bridging an ONS 15454 SDH SNCP and an ONS 15454 SDH line-protected domain. In Figure 7-14, the following circuits are present:

- An open-ended low-order circuit exists on Node 1. Slot 1 is the source, and Slots 2 and 3 are the destinations.

- An open-ended high-order circuit exists on Node 2 (the hub ONS 15600 SDH node). Slot 1 and Slot 2 are the sources, and Slot 3 is the destination.

- A two-way low-order circuit exists on Node 3 between Slot 1 and Slot 2.

*Figure 7-14     Low-order Traffic Routing over an ONS 15600 SDH Hub Node*
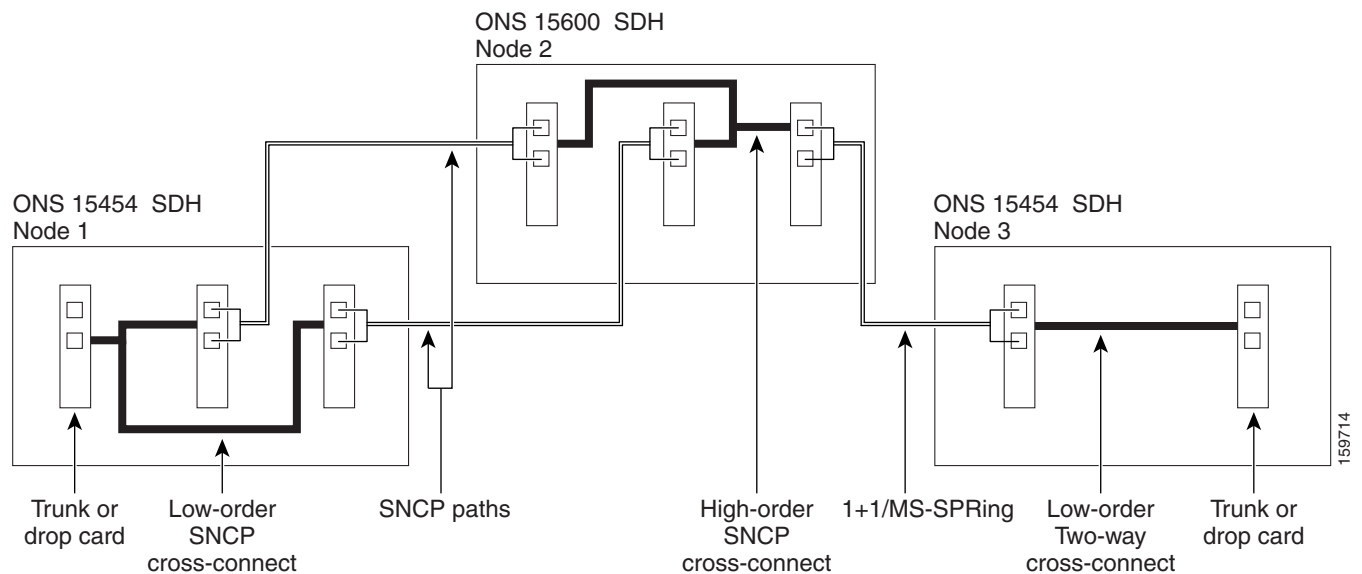


For information on creating an open-ended circuit on the ONS 15600 SDH to bridge protection domains, refer to the "Turn Up Network" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

## 7.19 High-Order VC3 Traffic Routing

High-order VC3 circuits are supported on the ONS 15600 SDH for connecting an ONS 15600 SDH node to another ONS 15600 SDH node, or for connecting an ONS 15600 SDH node to third-party SDH network elements. You can create VC3 circuits that use STM-1, STM-4, STM-16, and STM-64 interfaces.

C H A P T E R **8**

# SDH Topologies and Upgrades

This chapter explains Cisco ONS 15600 SDH topologies and upgrades. To provision topologies, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Chapter topics include:

## 8.1 Overview

The ONS 15600 SDH usually operates as a hub node in networks that include ONS 15454 SDHs. Single nodes are installed at geographic locations where several ONS SDH topologies converge. A single ONS 15600 SDH node might be a part of several ONS SDH rings/networks.

To avoid errors during network configuration, Cisco recommends that you draw the complete ONS SDH network topology on paper (or electronically) before you begin the physical implementation. A sketch ensures that you have adequate slots, cards, and fibers to complete the topology.

## 8.2 Point-to-Point and Linear ADM Configurations

You can configure ONS 15600 SDHs as a line of add/drop multiplexers (ADMs) by configuring one STM-N port as the working path and a second port as the protect path. Unlike rings, point-to-point (two node configurations) and linear (three node configurations) ADMs require that the STM-N ports at each node be in 1+1 protection to ensure that a break to the working line automatically routes traffic to the protect line.

Figure 8-1 shows two ONS 15600 SDH nodes in a point-to-point ADM configuration. Working traffic flows from Slot 1/Port 1 at Node 1 to Slot 1/Port 1 at Node 2. You create the protect path by creating a 1+1 configuration with Slot 2/Port 1 and Slot 2/Port 1 at Nodes 1 and 2.

*Figure 8-1* **Point-to-Point ADM Configuration**
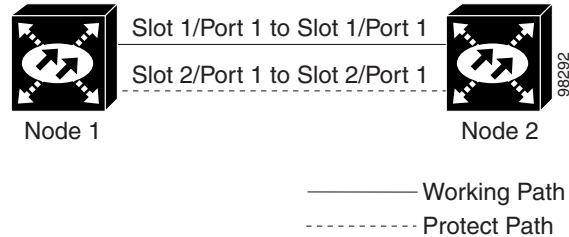


**8.3 Multiplex-Section Shared Protection Rings**

The ONS 15600 SDH can support up to 32 multiplex section-shared protection rings (MS-SPRings). Because the working and protect bandwidths must be equal, you can create only STM-16 or STM-64 MS-SPRings (that is, you cannot create an MS-SPRing with a mixture of STM-16 and STM-64 line rates). For information about MS-SPRing protection channels, see the "7.7 Protection Channel Access Circuits" section on page 7-14.

**Note** For best performance, MS-SPRings should have one LAN connection for every ten nodes in the MS-SPRing.

**8.3.1 Two-Fiber MS-SPRings**

In two-fiber MS-SPRings, each fiber is divided into working and protect bandwidths. For example, in an STM-16 MS-SPRing, VC4s 1 to 8 carry the working traffic, and VC4s 9 to 16 are reserved for protection (Figure 8-2). Working traffic (VC4s 1 to 8) travels in one direction on one fiber and in the opposite direction on the second fiber. Cisco Transport Controller (CTC) circuit routing routines calculate the shortest path for circuits based on many factors, including user requirements, traffic patterns, and distance. For example, in Figure 8-2, circuits going from Node 0 to Node 1 will typically travel on Fiber 1, unless that fiber is full, in which case circuits will be routed to Fiber 2 through Node 3 and Node 2. Traffic from Node 0 to Node 2 (or Node 1 to Node 3) can be routed on either fiber, depending on circuit provisioning requirements and traffic loads.

*Figure 8-2        Four-Node, Two-Fiber MS-SPRing*
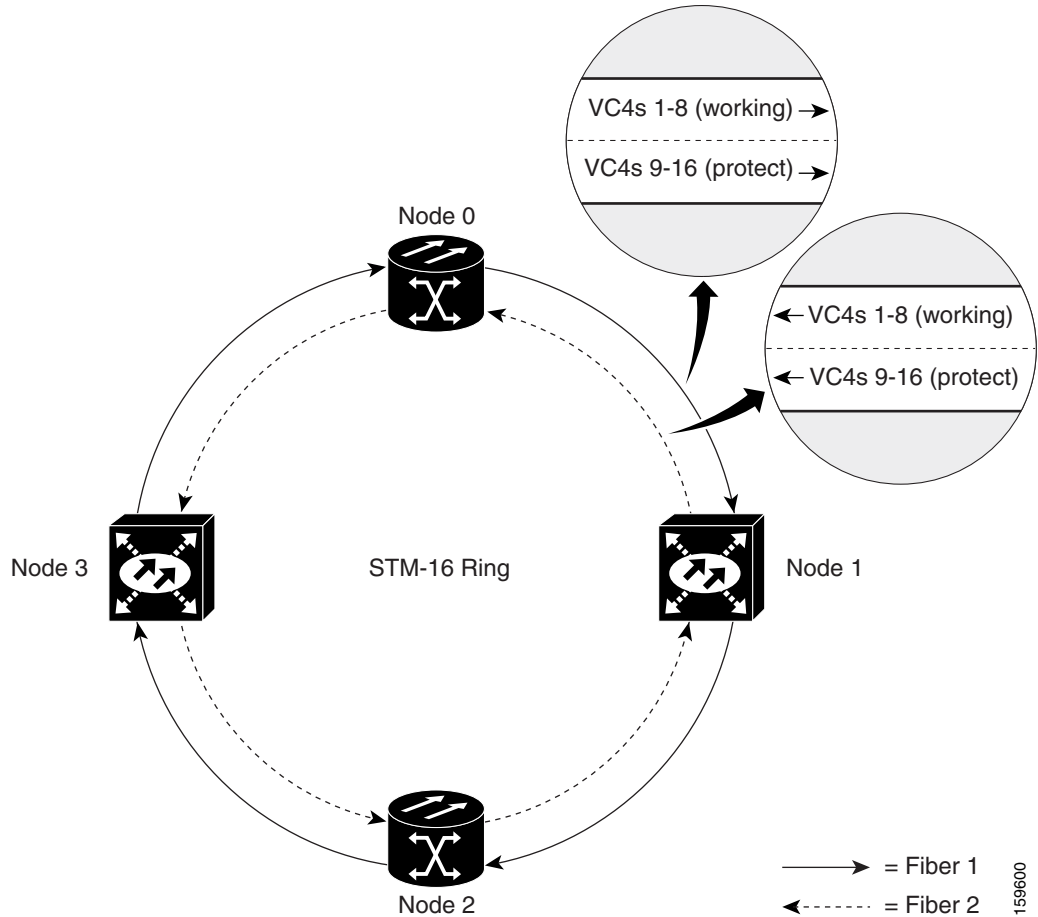


The SDH K1, K2, and K3 bytes carry the information that governs MS-SPRing protection switches. Each MS-SPRing node monitors the K bytes to determine when to switch the SDH signal to an alternate physical path. The K bytes communicate failure conditions and actions taken between nodes in the ring.

If a break occurs on one fiber, working traffic targeted for a node beyond the break switches to the protect bandwidth on the second fiber. The traffic travels in a reverse direction on the protect bandwidth until it reaches its destination node. At that point, traffic is switched back to the working bandwidth.

Figure 8-3 shows a traffic pattern sample on a four-node, two-fiber MS-SPRing.

*Figure 8-3    Four-Node, Two-Fiber MS-SPRing Traffic Pattern Sample*
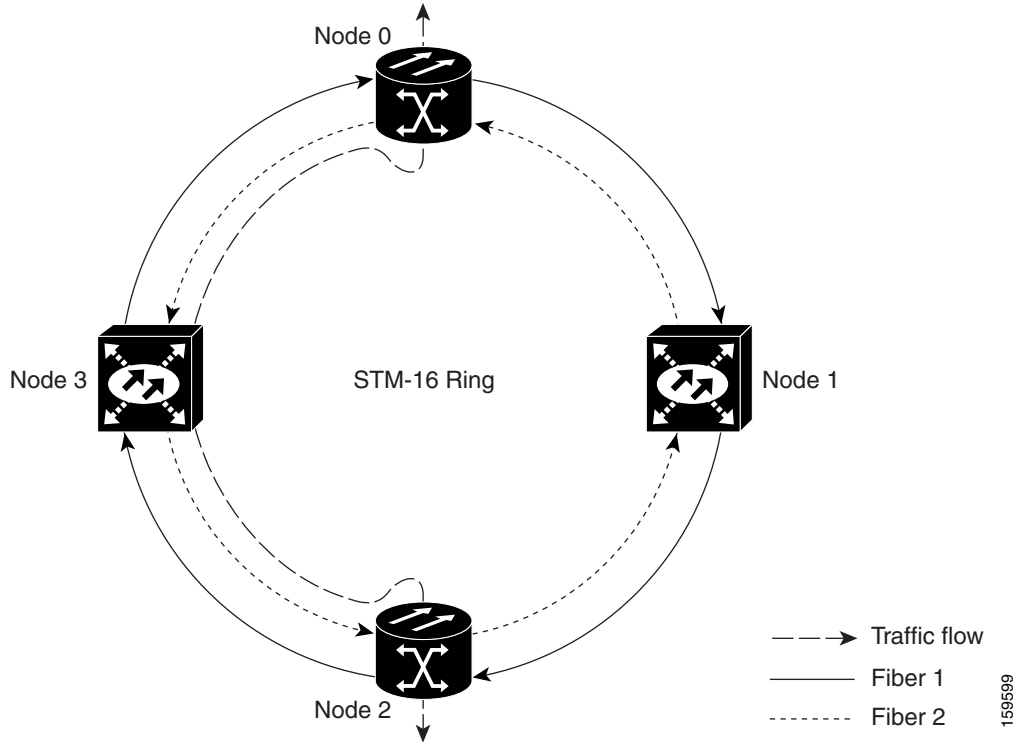


Figure 8-4 shows how traffic is rerouted following a line break between Node 0 and Node 3.

- All circuits originating on Node 0 that carried traffic to Node 2 on Fiber 2 are switched to the protect bandwidth of Fiber 1. For example, a circuit carried on VC4-1 on Fiber 2 is switched to VC4-9 on Fiber 1. A circuit carried on VC4-2 on Fiber 2 is switched to VC4-10 on Fiber 1. Fiber 1 carries the circuit to Node 3 (the original routing destination). Node 3 switches the circuit back to VC4-1 on Fiber 2 where it is routed to Node 2 on VC4-1.

- Circuits originating on Node 2 that normally carry traffic to Node 0 on Fiber 1 switch to the protect bandwidth of Fiber 2 at Node 3. For example, a circuit carried on VC4-2 on Fiber 1 is switched to VC4-10 on Fiber 2. Fiber 2 carries the circuit to Node 0 where the circuit is switched back to VC4-2 on Fiber 1 and then dropped to its destination.

*Figure 8-4*      *Four-Node, Two-Fiber MS-SPRing Traffic Pattern Following Line Break*
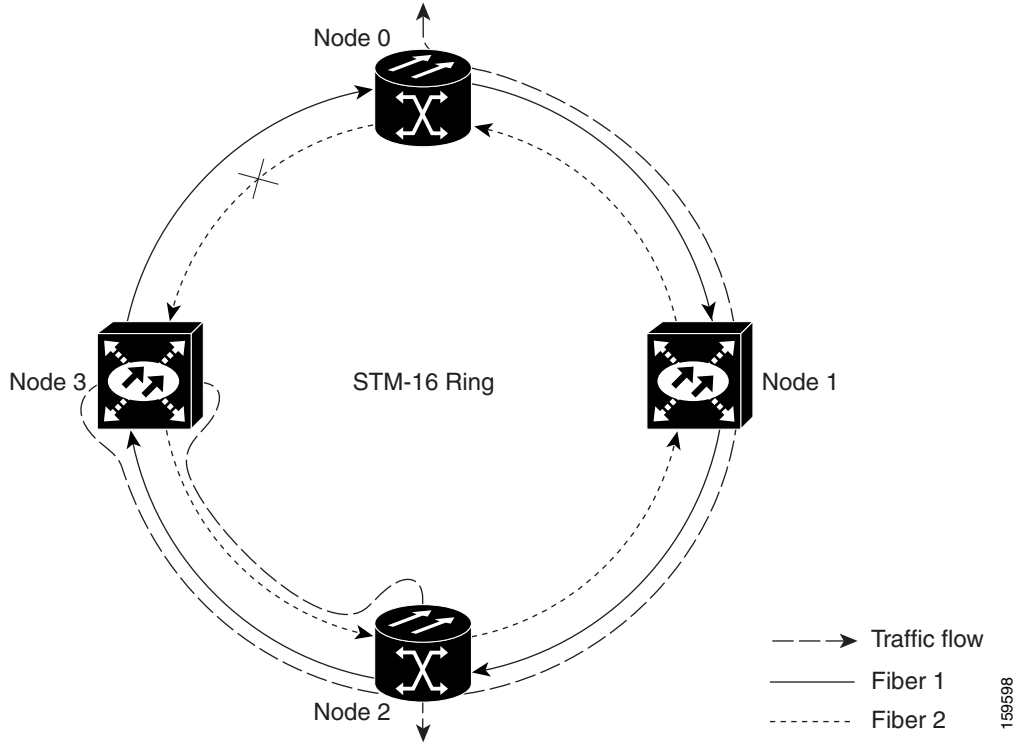


## 8.3.2 MS-SPRing Bandwidth

MS-SPRing nodes can terminate traffic coming from either side of the ring. Therefore, MS-SPRings are suited for distributed node-to-node traffic applications such as interoffice networks and access networks.

MS-SPRings allow bandwidth to be reused around the ring and can carry more traffic than a network with traffic flowing through one central hub. MS-SPRings can also carry more traffic than a subnetwork connection protection (SNCP) ring operating at the same STM-N rate. Table 8-1 shows the bidirectional bandwidth capacities of two-fiber MS-SPRings. The capacity is the STM-N rate divided by two, multiplied by the number of nodes in the ring minus the number of pass-through VC circuits.

*Table 8-1*      *Two-Fiber MS-SPRing Capacity*

| OC Rate | Working Bandwidth | Protection Bandwidth | Ring Capacity |
|---------|-------------------|----------------------|---------------|
| STM-16  | VC4 1-8           | VC4 9-16             | $8 \times N^1 - PT^2$ |
| STM-64  | VC4 1-32          | VC4 33-64            | $32 \times N - PT$ |

1.  N equals the number of ONS 15xxx SDH nodes in the ring. Nodes can be configured as MS-SPRing nodes but be in another MS-SPRing.

2.  PT equals the number of VC-4 circuits passed through ONS 15xxx SDH nodes in the ring (capacity varies depending on the traffic pattern).

Figure 8-5 shows an example of MS-SPRing bandwidth reuse. The same VC4 carries three different traffic sets simultaneously on different spans around the ring: one set from Node 3 to Node 1, another set from Node 1 to Node 2, and another set from Node 2 to Node 3.

*Figure 8-5*        ***MS-SPRing Bandwidth Reuse***



= Node 3 – Node 1 traffic
= Node 1 – Node 2 traffic
= Node 2 – Node 3 traffic
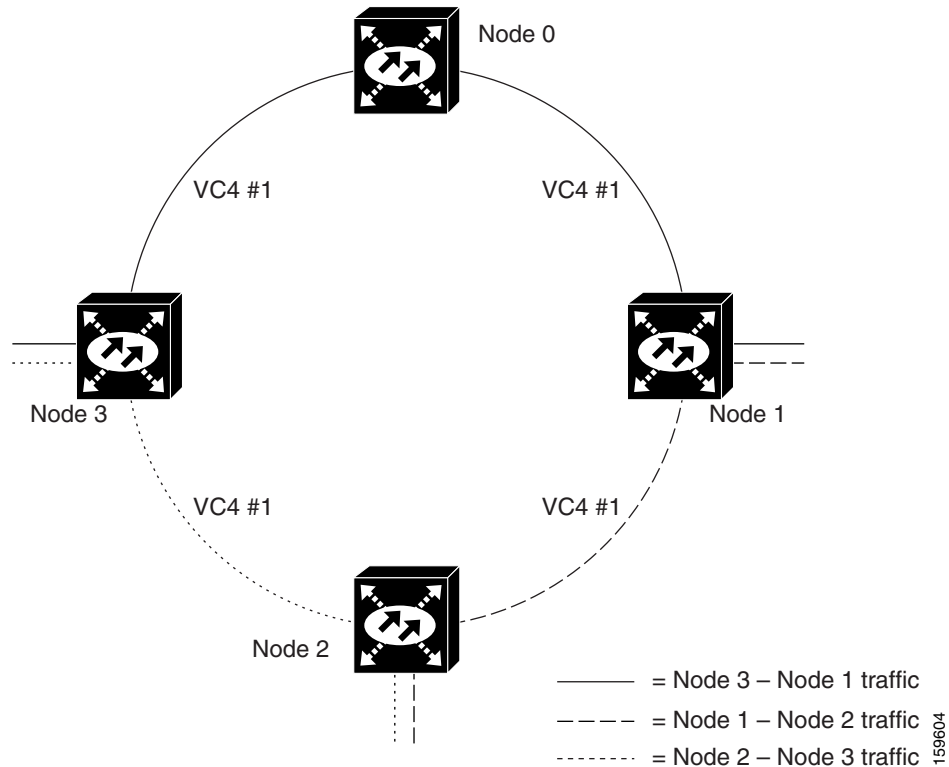
## 8.3.3  MS-SPRing Fiber Connections

Plan your fiber connections and use the same plan for all MS-SPRing nodes. For example, make the east port the farthest slot to the right and the west port the farthest slot to the left. Plug fiber connected to an east port at one node into the west port on an adjacent node. Figure 8-6 shows fiber connections for a two-fiber MS-SPRing with trunk (span) ports in Slot 4 (west) and Slot 12 (east). Refer to the *Cisco ONS 15600 SDH Procedure Guide* for fiber connection procedures.

**Note**    Always plug the transmit (Tx) connector of an STM-N port at one node into the receive (Rx) connector of an STM-N port at the adjacent node. Cards display an SF LED when Tx and Rx connections are mismatched.

**Figure 8-6**      *Connecting Fiber to a Four-Node, Two-Fiber MS-SPRing*
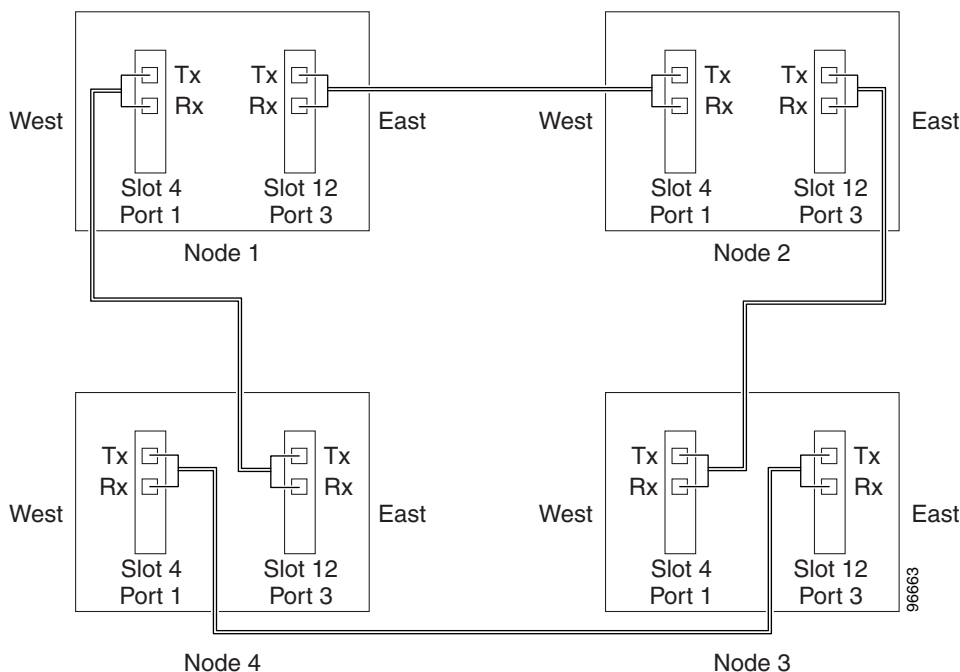


# 8.4  Subnetwork Connection Protection Rings

SNCP rings provide duplicate fiber paths around the ring. Working traffic flows in one direction and protection traffic flows in the opposite direction. If a problem occurs in the working traffic path, the receiving node switches to the path coming from the opposite direction.

CTC automates ring configuration. SNCP traffic is defined within the ONS 15600 SDH on a circuit-by-circuit basis. If a path-protected circuit is not defined within a 1+1 or MS-SPRing line protection scheme and path protection is available and specified, CTC uses SNCP as the default. You can set up a maximum of 64 STM-1/4/16 SNCPs or 16 STM-64 SNCPs for each ONS 15600 SDH node.

An SNCP circuit requires two data communications channel (DCC)-provisioned optical spans per node. SNCP circuits can be created across these spans until their bandwidth is consumed.

**Note**    If an SNCP circuit is created manually by Transaction Language One (TL1), DCCs are not needed; therefore, SNCP circuits are limited by the cross-connection bandwidth or the span bandwidth, but not by the number of DCCs.

The span bandwidth consumed by an SNCP circuit is two times the circuit bandwidth, since the circuit is duplicated. The cross-connection bandwidth consumed by an SNCP circuit is three times the circuit bandwidth at the source and destination nodes only. The cross-connection bandwidth consumed by an intermediate node has a factor of one.

Figure 8-7 shows a basic SNCP configuration. If Node 0 sends a signal to Node 2, the working signal travels on the working traffic path through Node 1. The same signal is also sent on the protect traffic path through Node 3.

*Figure 8-7*      ***Basic Four-Node SNCP***
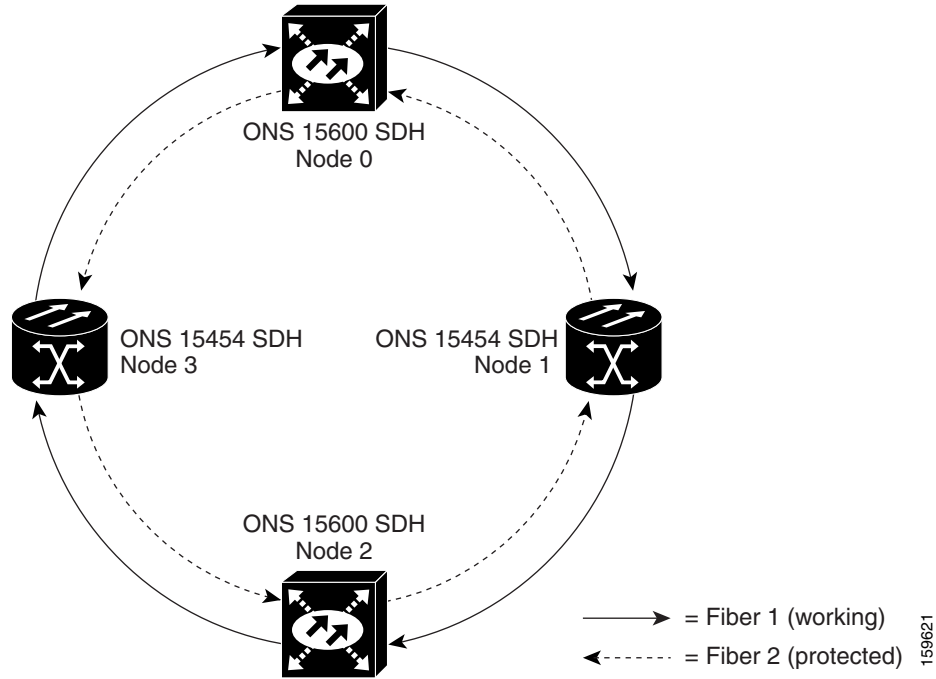


If a fiber break occurs, Node 2 switches its active receiver to the protect signal coming through Node 3 (Figure 8-8).

*Figure 8-8        SNCP with a Fiber Break*
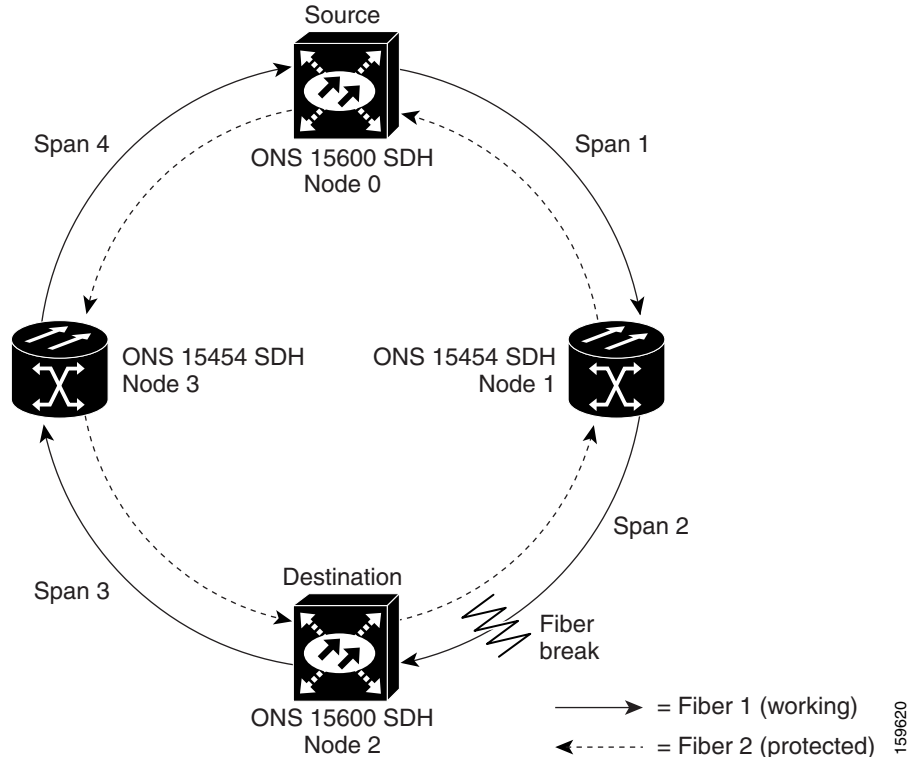


Because each traffic path is transported around the entire ring, SNCP rings are best suited for networks where traffic concentrates at one or two locations and is not widely distributed. SNCP capacity is equal to its bit rate. Services can originate and terminate on the same SNCP, or they can be passed to an adjacent access or interoffice ring for transport to the service-terminating location.

# 8.5  Dual-Ring Interconnect

Dual-ring interconnect (DRI) topology provides an extra level of path protection for circuits on interconnected rings. DRI allows users to interconnect MS-SPRings, SNCP rings, or an SNCP ring with an MS-SPRing, with additional protection provided at the transition nodes. In a DRI topology, ring interconnections occur at two or four nodes.

The drop-and-continue DRI method is used for all ONS 15600 SDH DRIs. In drop-and-continue DRI, a primary node drops the traffic to the connected ring and routes traffic to a secondary node within the same ring. The secondary node also routes the traffic to the connected ring; that is, the traffic is dropped at two different interconnection nodes to eliminate single points of failure. To route circuits on DRI, you must choose the Dual Ring Interconnect option during circuit provisioning. Dual transmit is not supported.

Two DRI topologies can be implemented on the ONS 15600 SDH:

- A traditional DRI requires two pairs of nodes to interconnect two networks. Each pair of user-defined primary and a secondary nodes drop traffic over a pair of interconnection links to the other network.

- An integrated DRI requires one pair of nodes to interconnect two networks. The two interconnected nodes replace the interconnection ring.

For DRI topologies, a hold-off timer sets the amount of time before a selector switch occurs. It reduces the likelihood of multiple switches, such as:

- Both a service selector and a path selector

- Both a line switch and a path switch of a service selector

For example, if an SNCP DRI service selector switch does not restore traffic, then the path selector switches after the hold-off time. The SNCP DRI hold-off timer default is 100 ms. You can change this setting in the SNCP Selectors tab of the Edit Circuits window. For an MS-SPRing DRI, if line switching does not restore traffic, then the service selector switches. The hold-off time delays the recovery provided by the service selector. The MS-SPRing DRI default hold-off time is 100 ms and cannot be changed.

# 8.5.1 MS-SPRing DRI

Unlike MS-SPRing automatic protection switching (APS) protocol, MS-SPRing DRI is a path-level protection protocol at the circuit level. Drop-and-continue MS-SPRing DRI requires a service selector in the primary node for each circuit routing to the other ring. Service selectors monitor signal conditions from dual feed sources and select the one that has the best signal quality. Same-side routing drops the traffic at primary nodes set up on the same side of the connected rings, and opposite-side routing drops the traffic at primary nodes set up on the opposite sides of the connected rings. For MS-SPRing DRI, primary and secondary nodes cannot be the circuit source or destination.

✎ **Note** A DRI circuit cannot be created if an intermediate node exists on the interconnecting link. However, an intermediate node can be added on the interconnecting link after the DRI circuit is created.

Figure 8-9 shows ONS 15600 SDHs in a traditional MS-SPRing DRI topology with same-side routing. In Ring 1, Nodes 3 and 4 are the interconnect nodes, and in Ring 2, Nodes 8 and 9. Duplicate signals are sent from Node 4 (Ring 1) to Node 9 (Ring 2), and from Node 3 (Ring 1) to Node 8 (Ring 2). The primary nodes (Nodes 4 and 9) are on the same side, and the secondary nodes (Nodes 3 and 8) provide an alternative route. In Ring 1, traffic at Node 4 is dropped (to Node 9) and continued (to Node 3). Similarly, at Node 9, traffic is dropped (to Node 4) and continued (to Node 8).

*Figure 8-9*      *ONS 15600 SDH Traditional MS-SPRing Dual-Ring Interconnect (Same-Side Routing)*
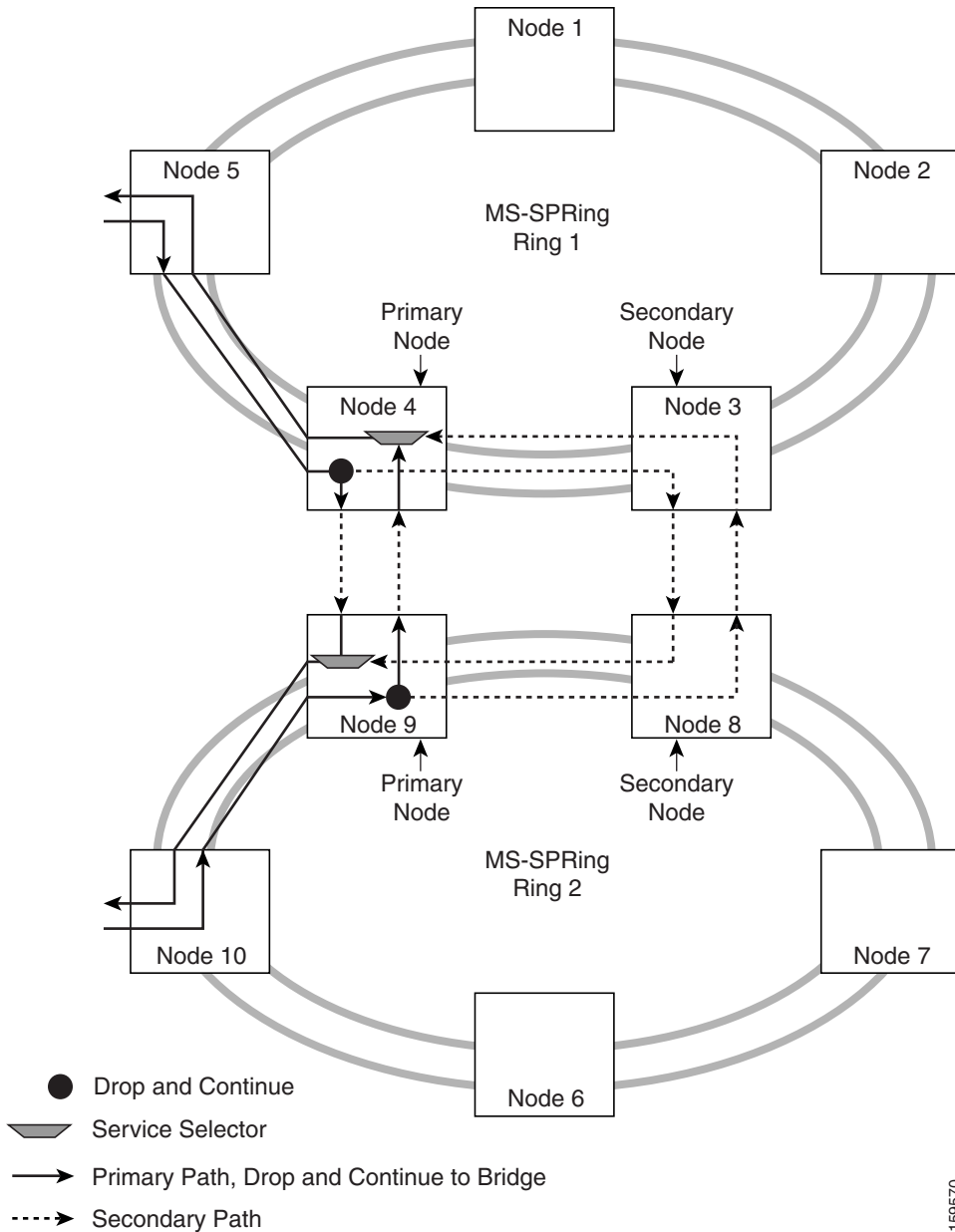


Figure 8-10 shows ONS 15600 SDHs in a traditional MS-SPRing DRI topology with opposite-side routing. In Ring 1, Nodes 3 and 4 are the interconnect nodes, and in Ring 2, Nodes 8 and 9. Duplicate signals are sent from Node 4 (Ring 1) to Node 8 (Ring 2), and from Node 3 (Ring 1) to Node 9 (Ring 2). In Ring 1, traffic at Node 4 is dropped (to Node 9) and continued (to Node 3). Similarly, at Node 8, traffic is dropped (to Node 3) and continued (to Node 9).

*Figure 8-10    ONS 15600 SDH Traditional MS-SPRing Dual-Ring Interconnect (Opposite-Side Routing)*
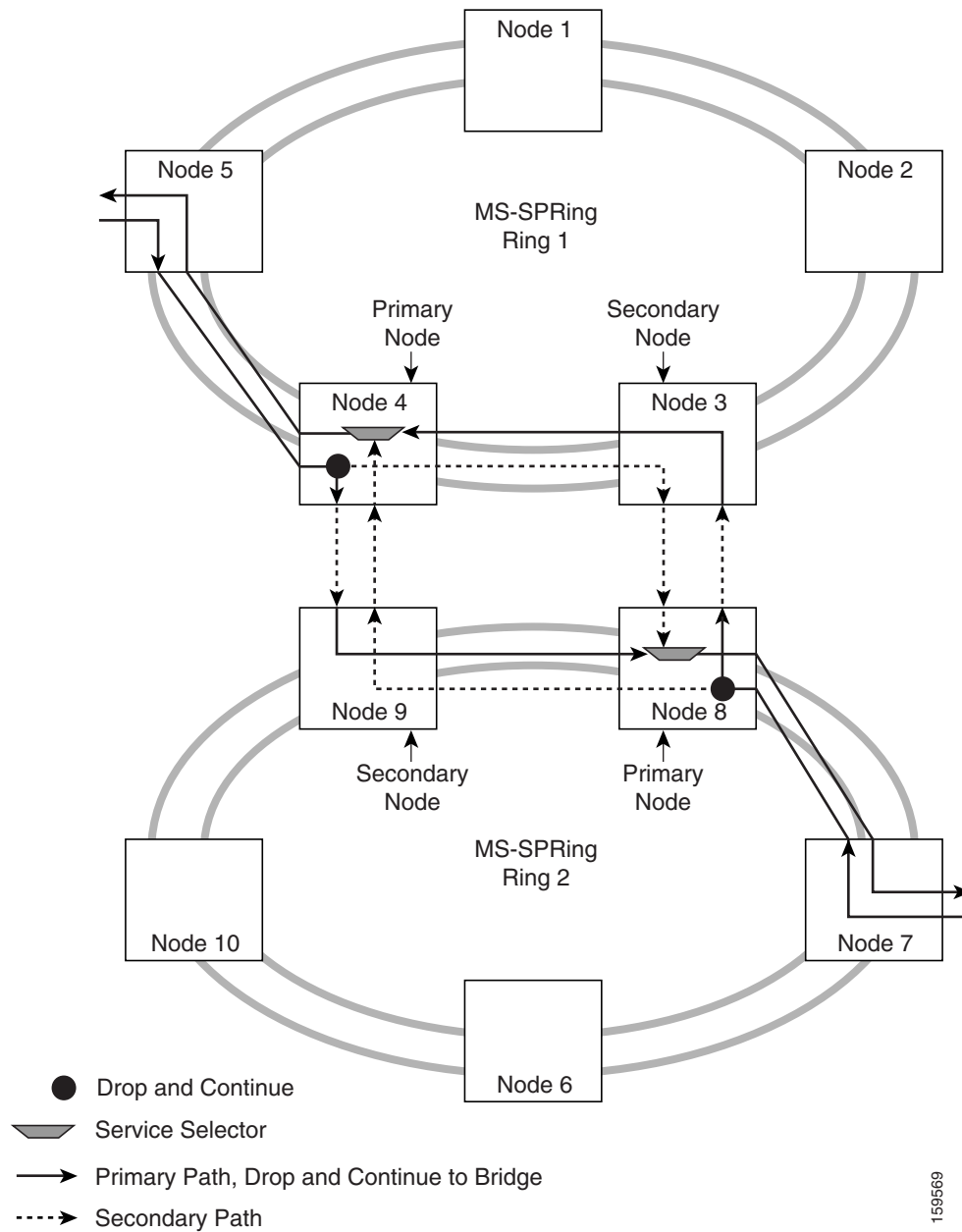


Figure 8-11 shows ONS 15600 SDHs in an integrated MS-SPRing DRI topology. The same drop-and-continue traffic routing occurs at two nodes, rather than four. This is achieved by installing an additional STM-N trunk at the two interconnect nodes. Nodes 3 and 8 are the interconnect nodes.

*Figure 8-11      ONS 15600 SDH Integrated MS-SPRing Dual-Ring Interconnect*
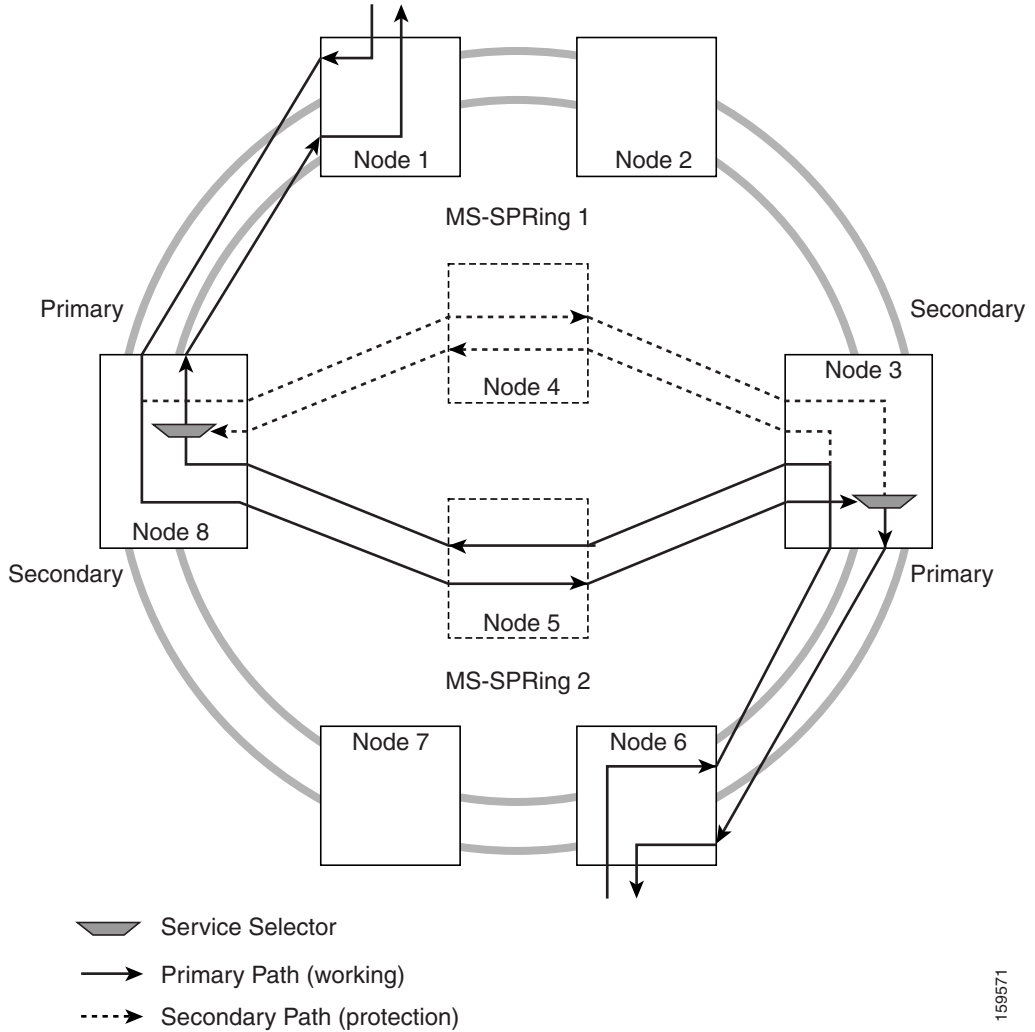


## 8.5.2 SNCP DRI

Figure 8-12 shows ONS 15600 SDHs in a traditional drop-and-continue SNCP DRI topology. In Ring 1, Nodes 4 and 5 are the interconnect nodes, and in Ring 2, Nodes 6 and 7 are the interconnect nodes. Duplicate signals are sent from Node 4 (Ring 1) to Node 6 (Ring 2), and from Node 5 (Ring 1) to Node 7 (Ring 2). In Ring 1, traffic at Node 4 is dropped (to Node 6) and continued (to Node 5). Similarly, at Node 5, traffic is dropped (to Node 7) and continued (to Node 4).

*Figure 8-12     ONS 15600 SDH Traditional SNCP Dual-Ring Interconnect*
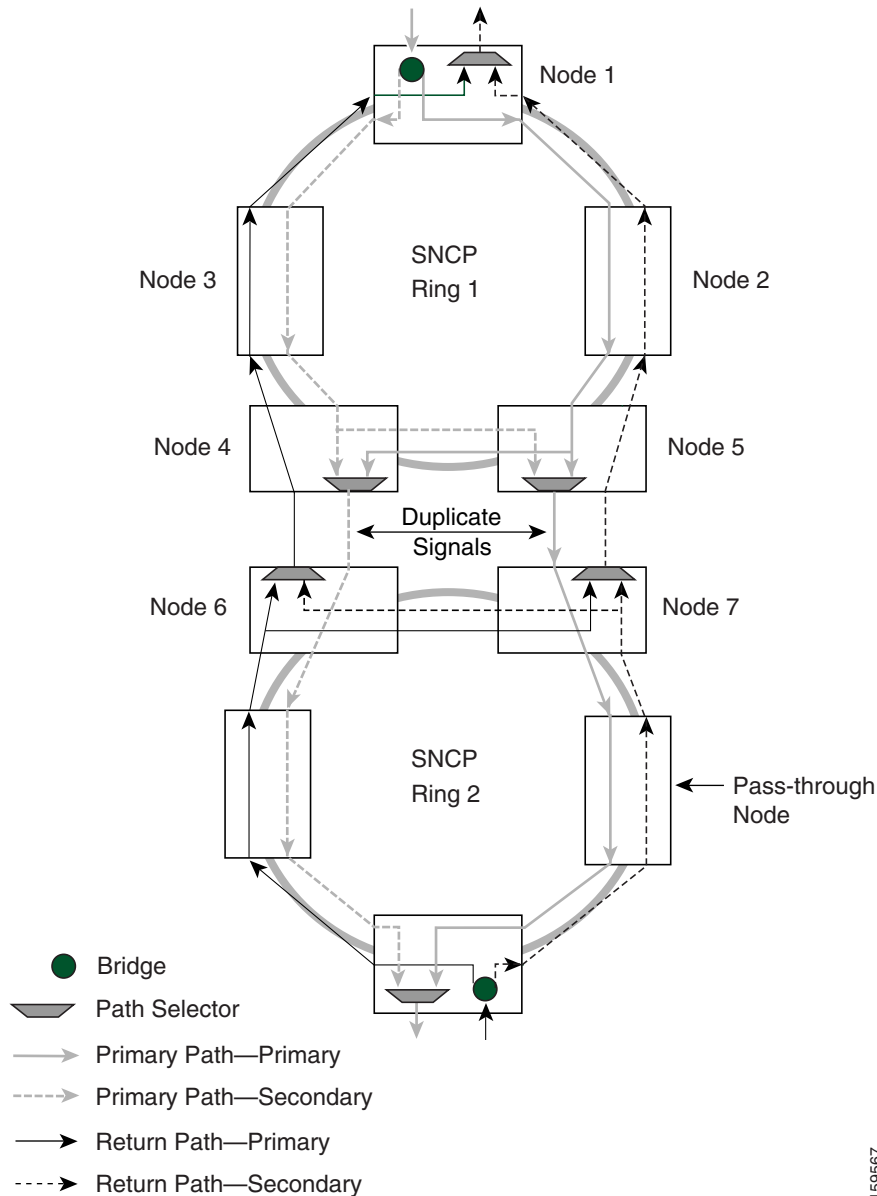


Figure 8-13 shows ONS 15600 SDHs in an integrated DRI topology. The same drop-and-continue traffic routing occurs at two nodes, rather than four. This is achieved by installing an addition STM-N trunk at the two interconnect nodes.

*Figure 8-13*     *ONS 15600 SDH Integrated SNCP Dual-Ring Interconnect*
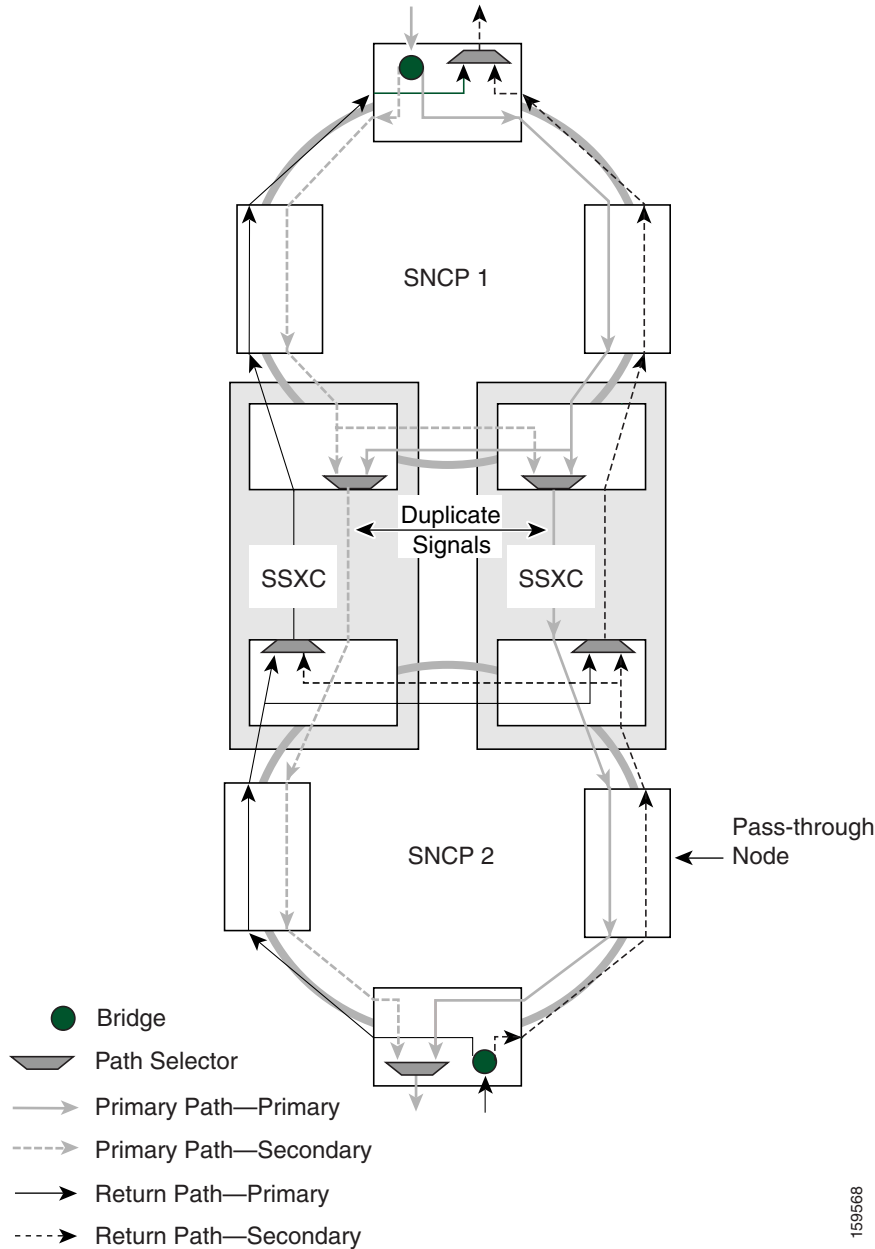


## 8.5.3 SNCP/MS-SPRing DRI Handoff Configurations

SNCP rings and MS-SPRings can also be interconnected. In MS-SPRing/SNCP DRI handoff configurations, primary and secondary nodes can be the circuit source or destination, which is useful when non-DCC optical interconnecting links are present. Figure 8-14 shows an example of an SNCP ring to MS-SPRing traditional DRI handoff.

*Figure 8-14*     *ONS 15600 SDH SNCP to MS-SPRing Traditional DRI Handoff*
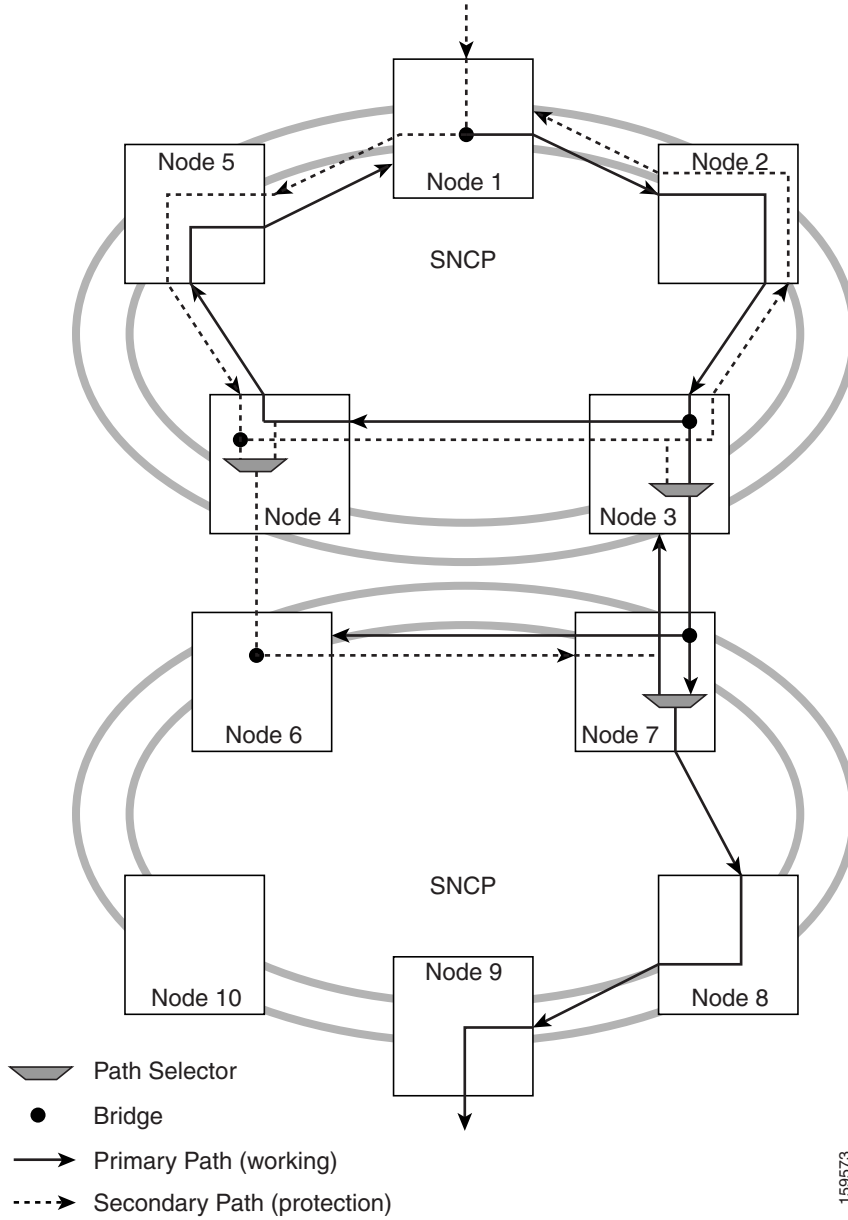


Figure 8-15 shows an example of an SNCP ring to MS-SPRing integrated DRI handoff.

*Figure 8-15*        *ONS 15600 SDH SNCP Ring to MS-SPRing Integrated DRI Handoff*
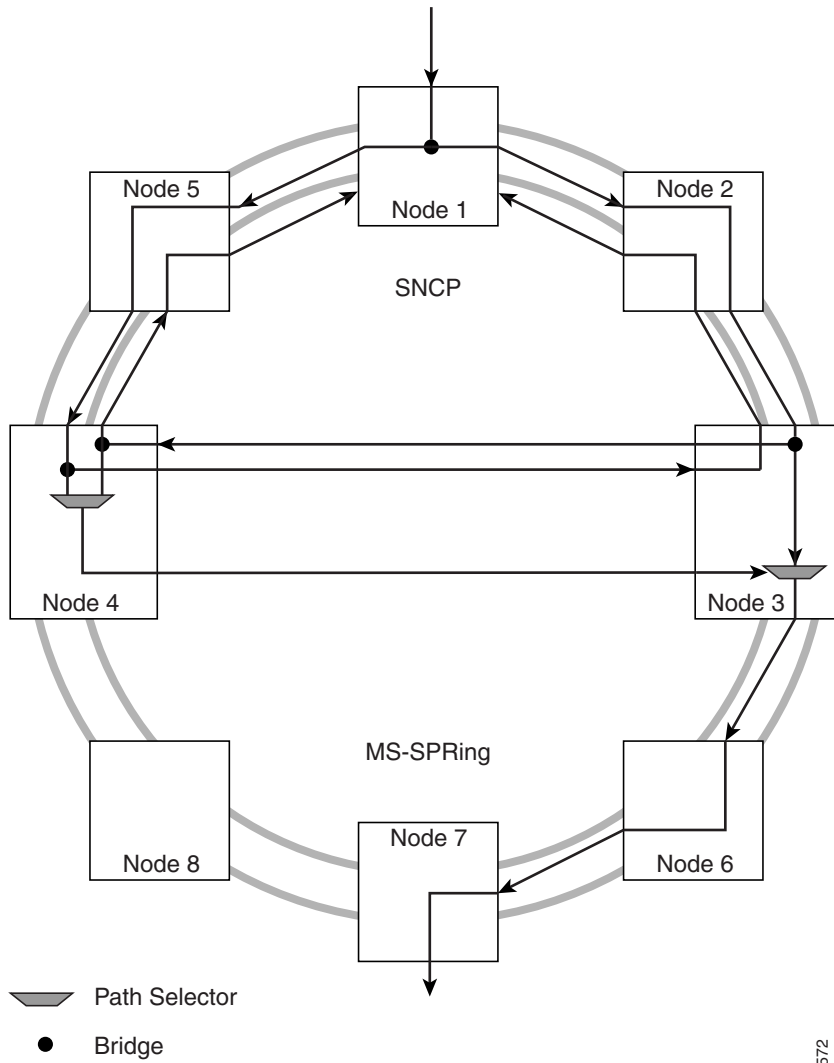


## 8.6  Subtending Rings

Subtending rings reduce the number of nodes and cards required and reduce external shelf-to-shelf cabling. The ONS 15600 SDH supports a maximum of 32 two-fiber MS-SPRings. If all rings have an STM-64 line rate, the maximum is 16 two-fiber MS-SPRings. Figure 8-16 shows an ONS 15600 SDH with multiple subtending rings.

*Figure 8-16*      *ONS 15600 SDH with Multiple Subtending Rings*
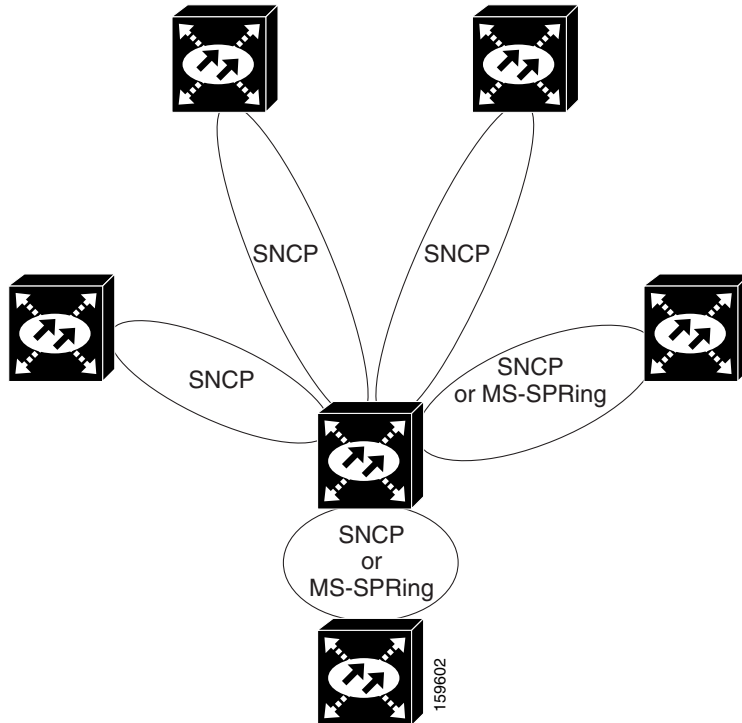


Figure 8-17 shows an SNCP ring subtending from an MS-SPRing. In this example, Node 3 is the only node serving both the MS-SPRing and SNCP ring. STM-N cards in Slots 4 and 12 serve the MS-SPRing, and STM-N cards in Slots 3 and 13 serve the SNCP ring.

*Figure 8-17*      *SNCP Ring Subtending from an MS-SPRing*
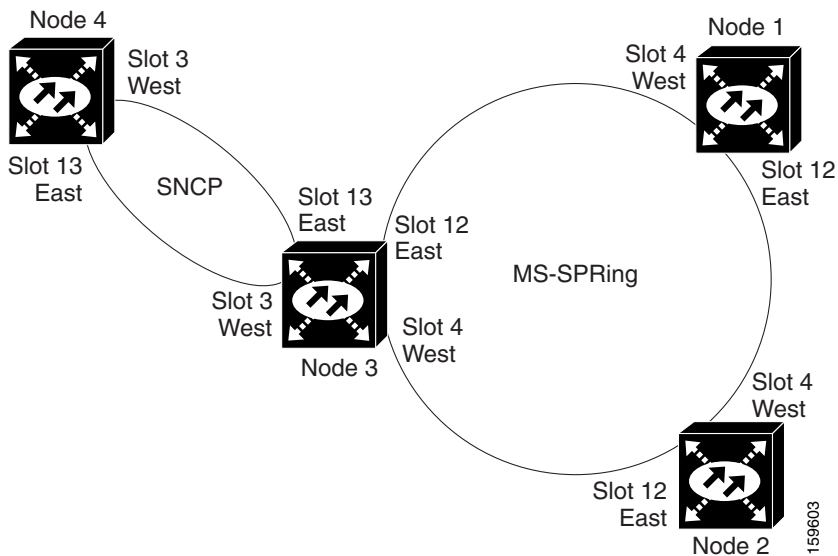
The ONS 15600 SDH can support 32 MS-SPRings on the same node. This capability allows you to deploy an ONS 15600 SDH in applications requiring SDH digital cross-connect systems (DCSs) or multiple SDH ADMs.

Figure 8-18 shows two MS-SPRings shared by one ONS 15600 SDH. Ring 1 runs on Nodes 1, 2, 3, and 4. Ring 2 runs on Nodes 4, 5, 6, and 7. Two MS-SPRings, Ring 1 and Ring 2, are provisioned on Node 4. Ring 1 uses cards in Slots 4 and 12, and Ring 2 uses cards in Slots 3 and 13.

**Note** Nodes in different MS-SPRings can have the same or different node IDs.

*Figure 8-18*      *MS-SPRing Subtending from an MS-SPRing*
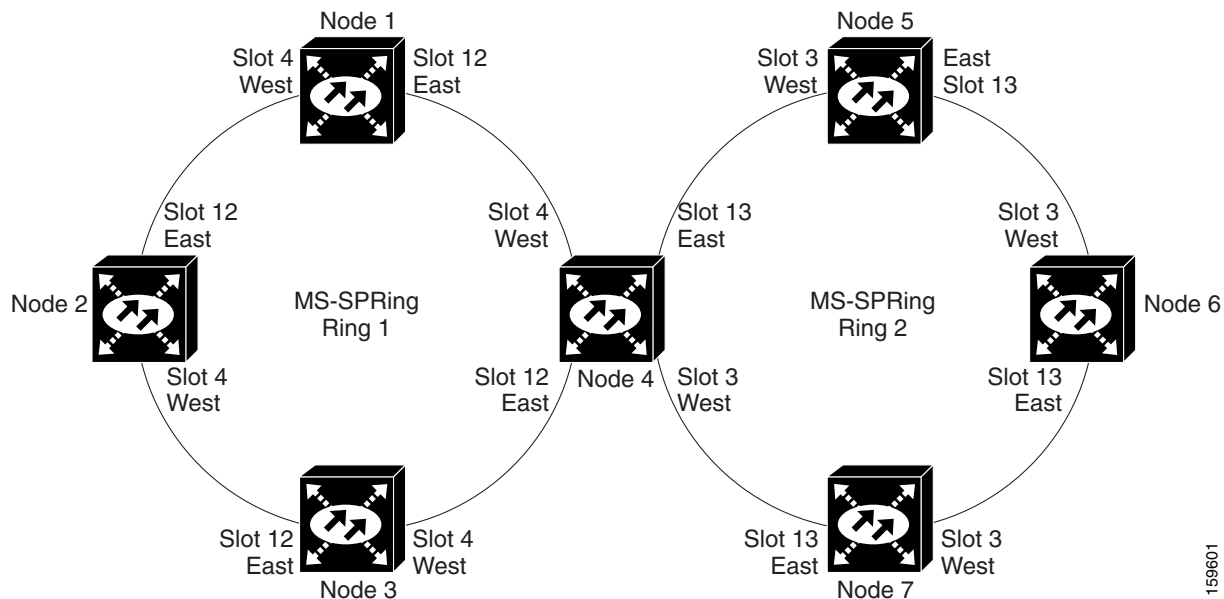


After subtending two MS-SPRings, you can route circuits from nodes in one ring to nodes in the second ring. For example, in Figure 8-18 you can route a circuit from Node 1 to Node 7. The circuit would normally travel from Node 1 to Node 4 to Node 7. If fiber breaks occur, for example between Nodes 1 and 4 and Nodes 4 and 7, traffic is rerouted around each ring: in this example, Nodes 2 and 3 in Ring 1 and Nodes 5 and 6 in Ring 2.

# 8.7  Extended Subnetwork Connection Protection Networks

In addition to single MS-SPRings, SNCP rings, and ADM configurations, you can extend ONS 15600 SDH traffic protection by creating extended SNCP networks. On SONET platforms, this is referred to as path-protected mesh networks (PPMNs). Extended SNCP rings include multiple ONS 15600 SDH topologies and extend the protection provided by a single SNCP ring to the meshed architecture of several interconnecting rings. In an extended SNCP ring, circuits travel diverse paths through a network of single or multiple meshed rings. When you create circuits, CTC automatically routes circuits across the extended SNCP ring, or you can manually route them. You can also choose levels of circuit protection. For example, if you choose full protection, CTC creates an alternate route for the circuit in addition to the main route. The second route follows a unique path through the network between the source and destination and sets up a second set of cross-connections.

For example, in Figure 8-19, a circuit is created from Node 3 to Node 9. CTC determines that the shortest route between the two nodes passes through Node 8 and Node 7, shown by the dotted line, and automatically creates cross-connections at Nodes 3, 8, 7, and 9 to provide the primary circuit path.

*Figure 8-19      Extended SNCP Network*
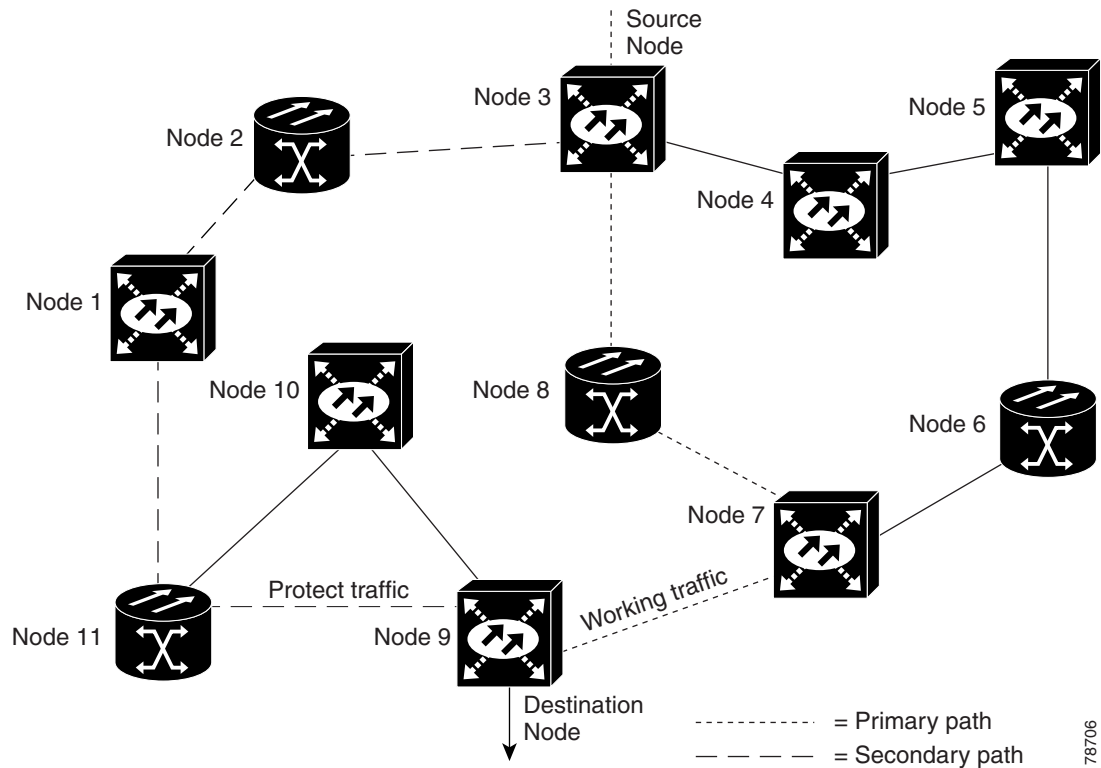


If full protection is selected, CTC creates a second unique route between Nodes 3 and 9 that passes through Nodes 2, 1, and 11. Cross-connections are automatically created at Nodes, 3, 2, 1, 11, and 9, shown by the dashed line. If a failure occurs on the primary path, traffic switches to the second circuit path. In this example, Node 9 switches from the fiber from Node 7 to the fiber from Node 11 and service resumes. The switch occurs within 50 ms.

Extended SNCP also allows spans of different SDH line rates to be mixed together in virtual rings. Figure 8-20 shows Nodes 1, 2, 3, and 4 in an STM-64 ring.

*Figure 8-20    Extended SNCP Virtual Ring*
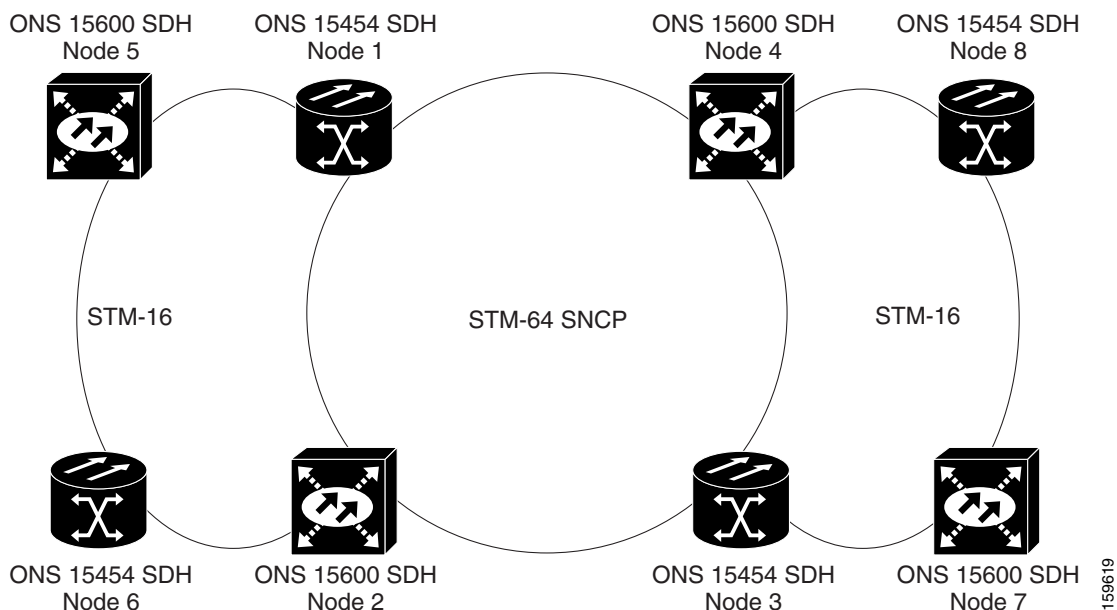


## 8.8 In-Service Topology Upgrades

Topology upgrades can be performed while the network is in service to convert a live network to a different topology. An in-service topology upgrade is potentially service-affecting, and generally allows a traffic hit of 50 ms or less. Traffic might not be protected during the upgrade. The following in-service topology upgrades are supported:

- Point-to-point or linear ADM to two-fiber MS-SPRing
- Node addition or removal from an existing topology

You can perform in-service topology upgrades irrespective of the service state of the involved cross-connects or circuits, however all circuits must have a DISCOVERED status.

ONS 15600 SDH circuit types supported for in-service topology upgrades are:

- Virtual containers (VC)
- Unidirectional and bidirectional
- Automatically routed and manually routed
- CTC-created and TL1-created
- Ethernet (unstitched)
- Multiple source and destination (both sources should be on one node and both drops on one node)

You cannot upgrade stitched Ethernet circuits during topology conversions.

✎
**Note**    A database restore on all nodes in a topology returns converted circuits to their original topology.

**Note** Open-ended SNCP and DRI configurations do not support in-service topology upgrades.

## 8.8.1 Point-to-Point or Linear ADM to Two-Fiber MS-SPRing

A 1+1 point-to-point or linear ADM to two-fiber MS-SPRing conversion is manual. You must remove the protect fibers from all nodes in the linear ADM and route them from the end node to the protect port on the other end node. In addition, you must delete the circuit paths that are located in the bandwidth that will become the protection portion of the two-fiber MS-SPRing (for example, circuits in VC4s 9 and higher on an STM-16 MS-SPRing) and recreate them in the appropriate bandwidth. Finally, you must provision the nodes as MS-SPRing nodes. For in-service topology upgrade procedures, refer to the "Convert Network Configurations" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

## 8.8.2 Add or Remove a Node from a Topology

You can add or remove a node from a linear ADM, MS-SPRing, or SNCP configuration. Adding or removing nodes from MS-SPRings is potentially service affecting, however adding and removing nodes from an existing 1+1 linear ADM or SNCP configuration does not disrupt traffic. CTC provides a wizard for adding a node to a point-to-point or 1+1 linear ADM. This wizard is used when adding a node between two other nodes. For procedures to add or remove a node, refer to the "Add and Remove Nodes" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

C H A P T E R **9**

# Management Network Connectivity

This chapter provides an overview of Cisco ONS 15600 SDH data communications network (DCN) connectivity. Cisco optical network communication is based on IP, including communication between Cisco Transport Controller (CTC) computers and ONS 15600 SDHs, and communication among networked ONS 15600 SDH nodes. The chapter provides scenarios showing ONS 15600 SDHs in common IP network configurations as well as information about the IP routing table, external firewalls, and open gateway network element (GNE) networks.

**Note** This chapter does not provide a comprehensive explanation of IP networking concepts and procedures, nor does it provide IP addressing examples to meet all networked scenarios. For ONS 15600 SDH networking setup instructions, refer to the "Turn Up a Node" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Although ONS 15600 SDH DCN communication is based on IP, ONS 15600 SDHs can be networked to equipment that is based on the Open System Interconnection (OSI) protocol suites. This chapter describes the ONS 15600 SDH OSI implementation and provides scenarios that show how ONS 15600 SDH can be networked within a mixed IP and OSI environment.

Chapter topics include:

- 9.1 IP Networking Overview, page 9-1
- 9.2 ONS 15600 SDH IP Addressing Scenarios, page 9-2
- 9.3 Routing Table, page 9-19
- 9.4 External Firewalls, page 9-22
- 9.5 Open GNE, page 9-23
- 9.6 TCP/IP and OSI Networking, page 9-25
- 9.7 IPv6 Network Compatibility, page 9-56

**Note** To set up ONS 15600 SDHs within an IP network, you must work with a LAN administrator or other individual at your site who has IP networking training and experience.

## 9.1 IP Networking Overview

ONS 15600 SDHs can be connected in many different ways within an IP environment:

- You can connect ONS 15600 SDH nodes and LANs through direct connections or a router.

- IP subnetting can create ONS 15600 SDH node groups, which allow you to provision nodes in a network that are not connected using the data communications channel (DCC).

- Different IP functions and protocols allow you to achieve specific network goals. For example, Proxy Address Resolution Protocol (ARP) enables one LAN-connected ONS 15600 SDH to serve as a gateway for ONS 15600 SDHs that are not connected to the LAN.

- You can create static routes to enable connections among multiple CTC sessions with ONS 15600 SDHs that reside on the same subnet but have different destination IP addresses.

- If ONS 15600 SDHs are connected to Open Shortest Path First (OSPF) networks, ONS 15600 SDH network information is automatically communicated across multiple LANs and WANs.

# 9.2 ONS 15600 SDH IP Addressing Scenarios

ONS 15600 SDH IP addressing generally has eight common scenarios or configurations. Use the scenarios as building blocks for more complex network configurations. Table 9-1 provides a general list of items to check when setting up ONS 15600 SDHs in IP networks.

*Table 9-1*      *General ONS 15600 SDH IP Troubleshooting Checklist*

| Item | What to Check |
|------|---------------|
| Link integrity | Verify that link integrity exists between: <br> • CTC computer and network hub/switch <br> • ONS 15600 SDHs (backplane ports or active TSC card port) and network hub/switch <br> • Router ports and hub/switch ports |
| ONS 15600 SDH hub/switch ports | If connectivity problems occur, set the hub or switch port that is connected to the ONS 15600 SDH to 10 Mbps half-duplex. |
| Ping | Ping the node to test connections between computers and ONS 15600 SDHs. |
| IP addresses/subnet masks | Verify that ONS 15600 SDH IP addresses and subnet masks are set up correctly. |
| Optical connectivity | Verify that ONS 15600 SDH optical trunk ports are in service; DCC is enabled on each trunk port. |

## 9.2.1 Scenario 1: CTC and ONS 15600 SDHs on the Same Subnet

Scenario 1 shows a basic ONS 15600 SDH LAN configuration (Figure 9-1). The ONS 15600 SDHs and CTC computer reside on the same subnet. All ONS 15600 SDHs connect to LAN A, and all ONS 15600 SDHs have DCC connections.

*Figure 9-1*        *Scenario 1: CTC and ONS 15600 SDHs on Same Subnet*

CTC Workstation
IP Address 192.168.1.100
Subnet Mask 255.255.255.0
Default Gateway = N/A
Host Routes = N/A

LAN A

ONS 15600 SDH #2
IP Address 192.168.1.20
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

SDH RING

ONS 15600 SDH #1
IP Address 192.168.1.10
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

ONS 15600 SDH #3
IP Address 192.168.1.30
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

159617

## 9.2.2  Scenario 2: CTC and ONS 15600 SDHs Connected to Router

In Scenario 2, the CTC computer resides on a subnet (192.168.1.0) and attaches to LAN A (Figure 9-2). The ONS 15600 SDHs reside on a different subnet (192.168.2.0) and attach to LAN B. A router connects LAN A to LAN B. The IP address of router interface A is set to LAN A (192.168.1.1), and the IP address of router interface B is set to LAN B (192.168.2.1).

On the CTC computer, the default gateway is set to router interface A. If the LAN uses Dynamic Host Configuration Protocol (DHCP), the default gateway and IP address are assigned automatically. In the Figure 9-2 example, a DHCP server is not available.

*Figure 9-2*        *Scenario 2: CTC and ONS 15600 SDHs Connected to Router*



LAN A

Int "A"

CTC Workstation
IP Address 192.168.1.100
Subnet Mask 255.255.255.0
Default Gateway = 192.168.1.1
Host Routes = N/A

Int "B"   Router
IP Address  of interface "A" to LAN "A" 192.168.1.1
IP Address of interface "B" to LAN "B"  192.168.2.1
Subnet Mask 255.255.255.0
Default Router = N/A
Host Routes =  N/A

LAN B

ONS 15600 SDH #2
IP Address 192.168.2.20
Subnet Mask 255.255.255.0
Default Router = 192.168.2.1
Static Routes = N/A

SDH RING

ONS 15600 SDH #1
IP Address 192.168.2.10
Subnet Mask 255.255.255.0
Default Router = 192.168.2.1
Static Routes = N/A

ONS 15600 SDH #3
IP Address 192.168.2.30
Subnet Mask 255.255.255.0
Default Router = 192.168.2.1
Static Routes = N/A

159616

# 9.2.3  Scenario 3: Using Proxy ARP to Enable an ONS 15600 SDH Gateway

Scenario 3 is similar to Scenario 1, but only one ONS 15600 SDH (Node 1) connects to the LAN (Figure 9-3). Two ONS 15600 SDHs (Nodes 2 and 3) connect to Node1 through the SDH data communications channel (DCC). Because all three ONS 15600 SDHs are on the same subnet, Proxy ARP enables Node 1 to serve as a gateway for Nodes 2 and 3.

**Note**    This scenario assumes that all CTC connections are to Node 1. If you connect a laptop to either Node 2 or Node 3, network partitioning will occur; neither the laptop or the CTC computer will be able to see all nodes. If you want laptops to connect directly to end network elements (ENEs), you will need to create static routes (refer to the "9.2.5  Scenario 5: Using Static Routes to Connect to LANs" section on page 9-6) or enable the ONS 15600 SDH proxy server (see the "9.2.7  Scenario 7: Provisioning the ONS 15600 SDH Proxy Server" section on page 9-11).

***Figure 9-3***     ***Scenario 3: Using Proxy ARP***
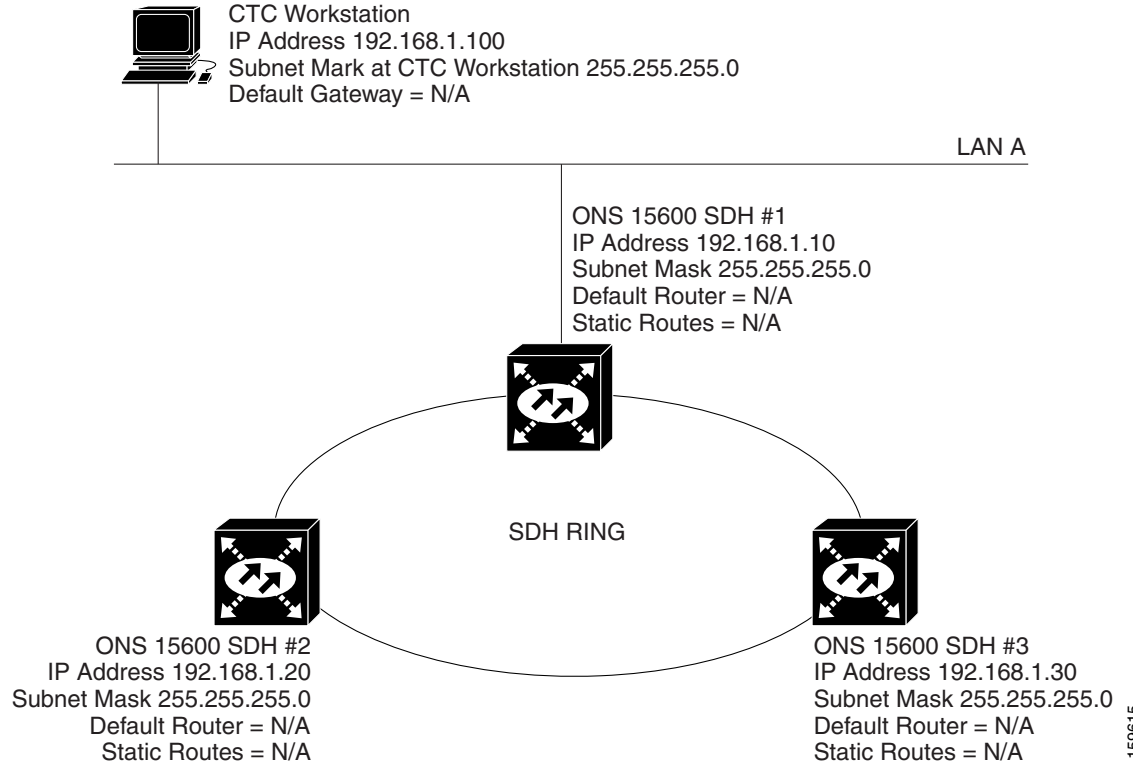


ARP matches higher-level IP addresses to the physical addresses of the destination host. It uses a lookup table (called the ARP cache) to perform the translation. When the address is not found in the ARP cache, a broadcast is sent out on the network with a special format called the ARP request. If one of the machines on the network recognizes its own IP address in the request, it sends an ARP reply back to the requesting host. The reply contains the physical hardware address of the receiving host. The requesting host stores this address in its ARP cache so that all subsequent datagrams (packets) to this destination IP address can be translated to a physical address.

Proxy ARP enables one LAN-connected ONS 15600 SDH to respond to the ARP request for ONS 15600 SDHs that are not connected to the LAN. (ONS 15600 SDH Proxy ARP requires no user configuration.) For this response to occur, the DCC-connected ONS 15600 SDHs must reside on the same subnet. When a LAN device sends an ARP request to an ONS 15600 SDH that is not connected to the LAN, the gateway ONS 15600 SDH returns its MAC address to the LAN device. The LAN device then sends the datagram for the remote ONS 15600 SDH to the MAC address of the proxy ONS 15600 SDH. The proxy ONS 15600 SDH uses its routing table to forward the datagram to the non-LAN ONS 15600 SDH.

## 9.2.4  Scenario 4: Default Gateway on CTC Computer

Scenario 4 is similar to Scenario 3, but Nodes 2 and 3 reside on different subnets, 192.168.2.0 and 192.168.3.0, respectively (Figure 9-4). Node 1 and the CTC computer are on subnet 192.168.1.0. For the CTC computer to communicate with Nodes 2 and 3, you would enter Node 1 as the default gateway on the CTC computer.

*Figure 9-4 Scenario 4: Default Gateway on a CTC Computer*
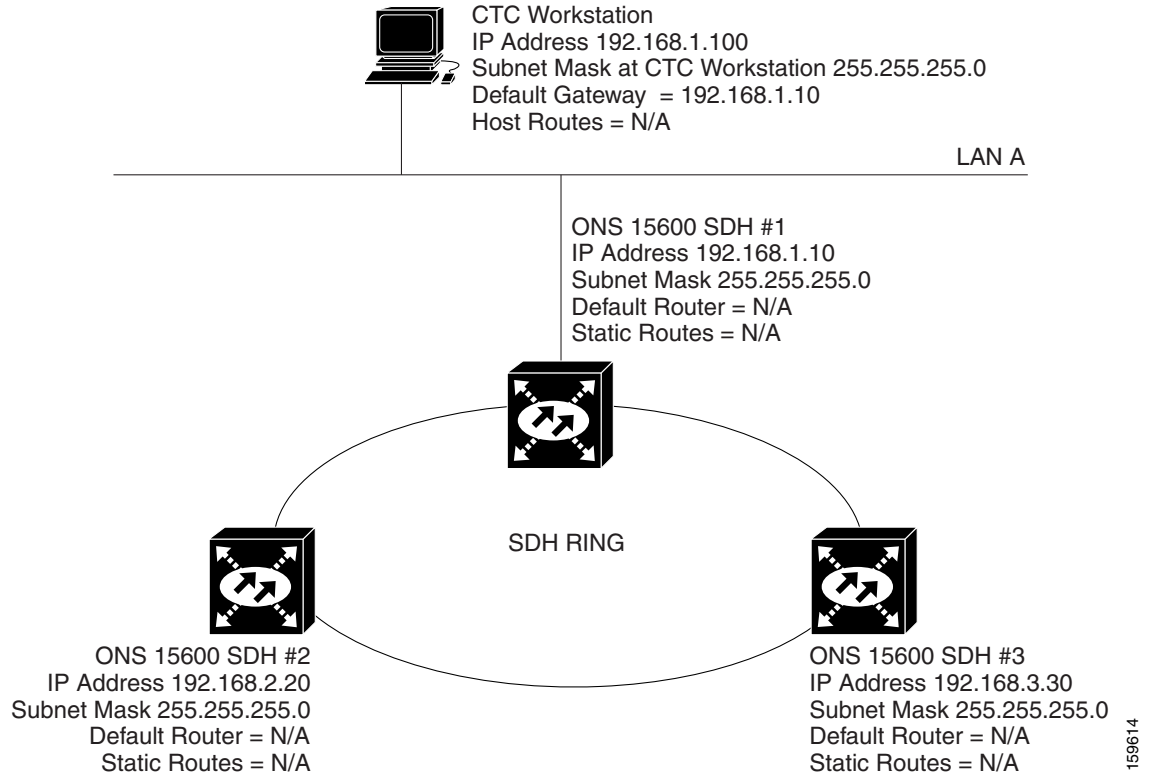


## 9.2.5 Scenario 5: Using Static Routes to Connect to LANs

Use static routes for the following two reasons:

- To connect ONS 15600 SDHs to CTC sessions on one subnet connected by a router to ONS 15600 SDHs residing on another subnet. (These static routes are not needed if OSPF is enabled. Scenario 6 shows an OSPF example.)

- To enable multiple CTC sessions among ONS 15600 SDHs residing on the same subnet.

In Figure 9-5, one CTC residing on subnet 192.168.1.0 connects to a router through interface A. (The router is not set up with OSPF.) ONS 15600 SDHs residing on subnet 192.168.2.0 are connected through Node 1 to the router through interface B. To connect to CTC computers on LAN A, you would create a static route on Node 1.

***Figure 9-5        Scenario 5: Static Route with One CTC Computer Used as a Destination***
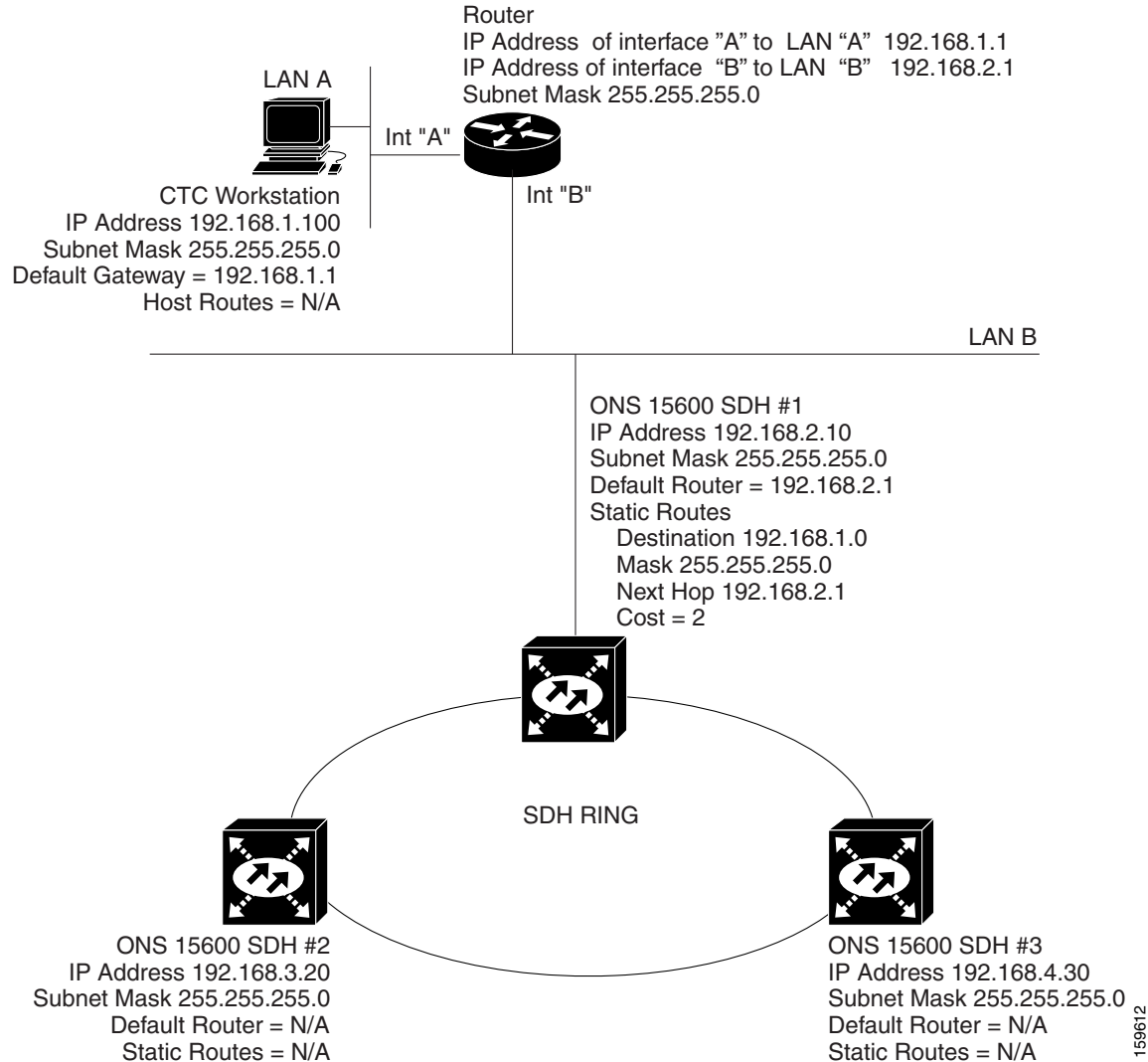


The destination and subnet mask entries control access to the ONS 15600 SDHs:

- If a single CTC computer will be connected to a router, enter the complete CTC "host route" IP address as the destination with a subnet mask of 255.255.255.255.

- If CTC computers on a subnet are connected to a router, enter the destination subnet (in this example, 192.168.1.0) and a subnet mask of 255.255.255.0.

- If all CTC computers are connected to router, enter a destination of 0.0.0.0 and a subnet mask of 0.0.0.0.

Figure 9-6 shows an example. In this figure, the IP address of router interface B is entered as the next hop (the next router that a packet traverses to reach its destination), and the cost (number of hops from source to destination) is 2.

*Figure 9-6*      *Scenario 5: Static Route with Multiple LAN Destinations*
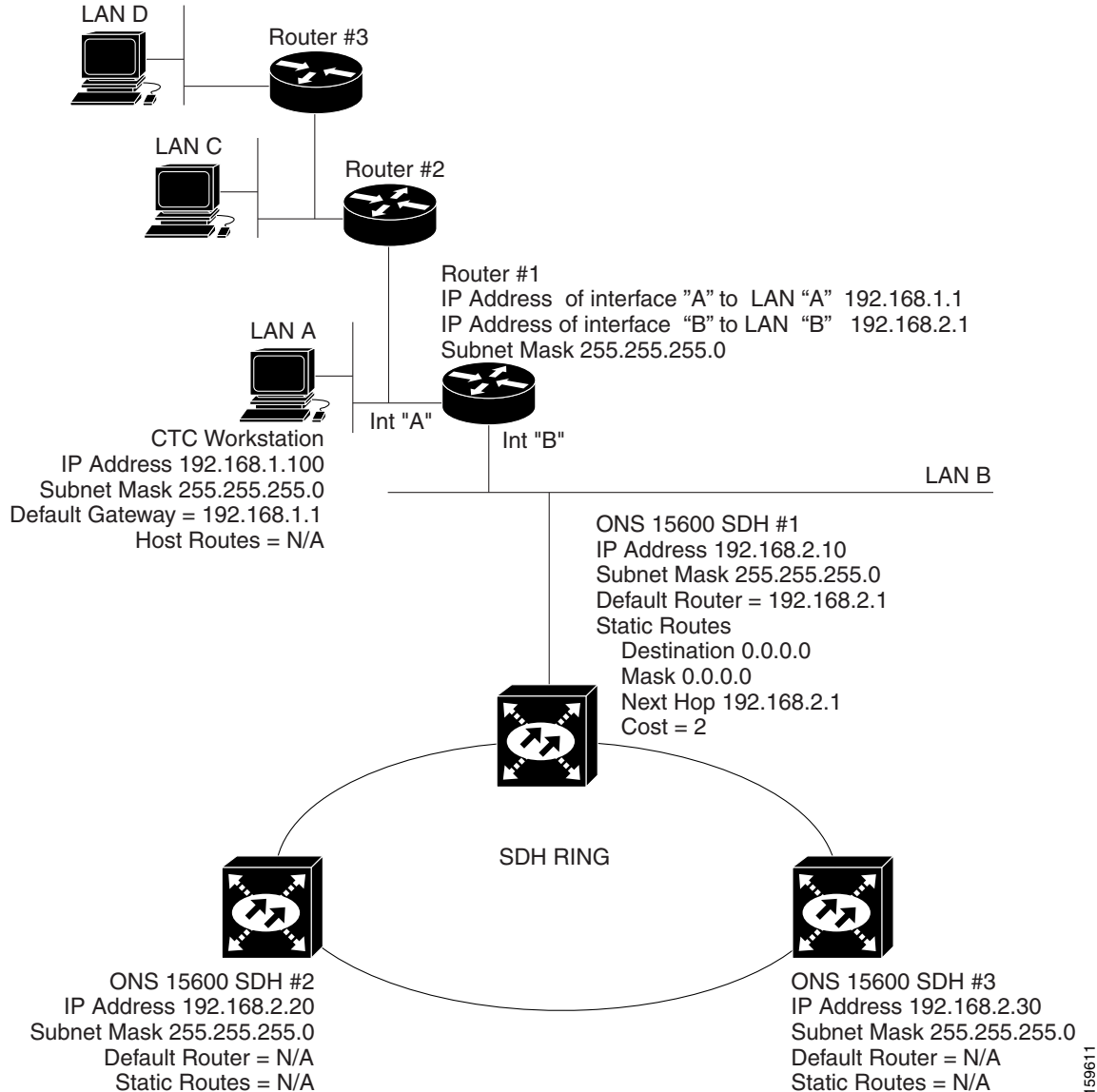


## 9.2.6 Scenario 6: Using OSPF

OSPF is a link state Internet routing protocol. Link state protocols use a "hello protocol" to monitor their links with adjacent routers and to test their links with their neighbors. Link state protocols advertise their directly connected networks and their active links. Each link state router captures the link state advertisements (LSAs) and puts them together to create a topology of the entire network or area. From this database, the router calculates a routing table by constructing a shortest path tree. The router continuously recalculates to capture ongoing topology changes.

ONS 15600 SDHs use the OSPF protocol in internal ONS 15600 SDH networks for node discovery, circuit routing, and node management. You can enable OSPF on the ONS 15600 SDHs so that the ONS 15600 SDH topology is sent to OSPF routers on a LAN. Advertising the ONS 15600 SDH network

topology to LAN routers means you do not need to manually enter static routes for ONS 15600 SDH subnetworks. Figure 9-7 shows the same network enabled for OSPF. When you are logged into a ONS 15600 SDH node, CTC does not allow both a DCC interface and a LAN interface in the same nonzero OSPF area.

*Figure 9-7     Scenario 6: OSPF Enabled*
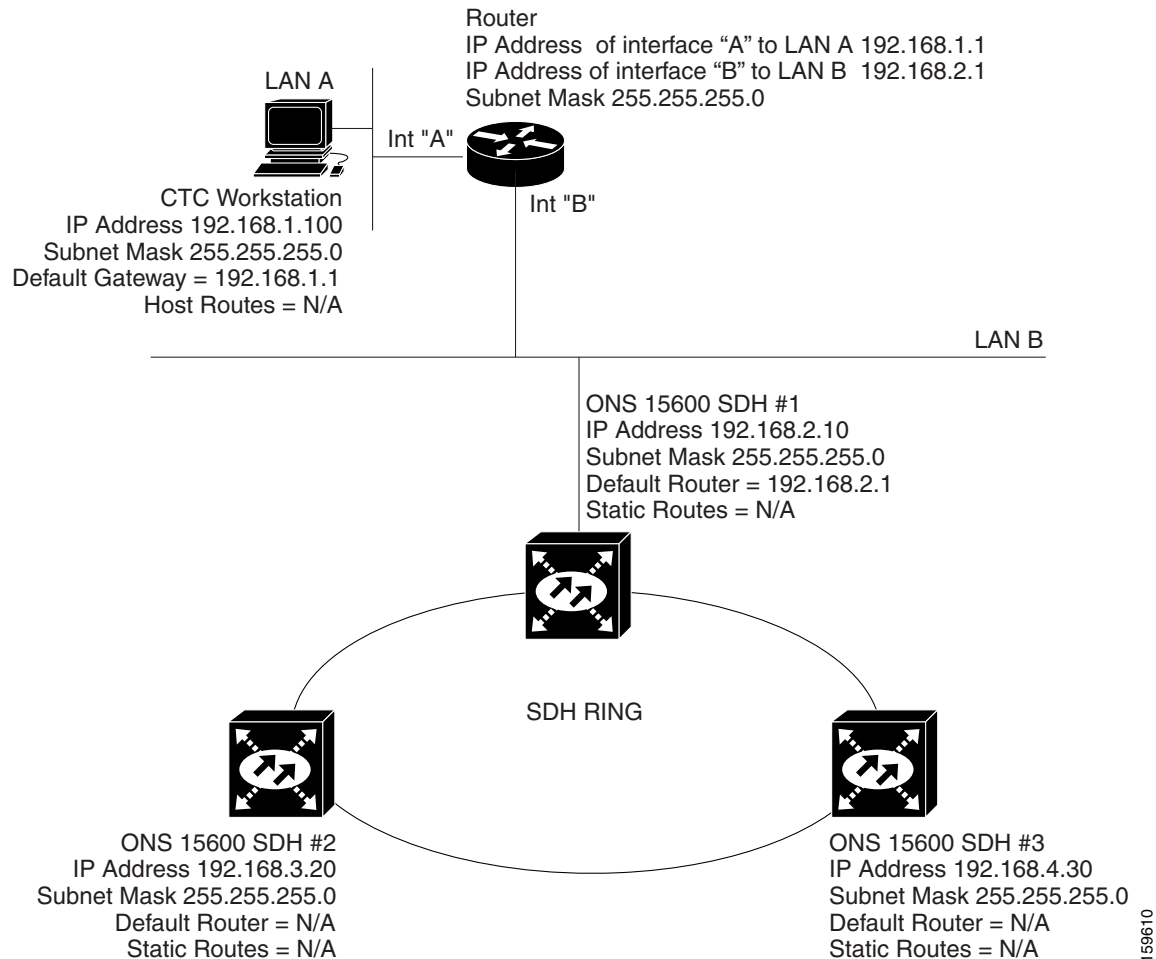


Figure 9-8 shows the same network without OSPF. Static routes must be manually added to the router in order for CTC computers on LAN A to communicate with Nodes 2 and 3 because these nodes reside on different subnets.

*Figure 9-8     Scenario 6: OSPF Not Enabled*



Router
IP Address of interface "A" to LAN A 192.168.1.1
IP Address of interface "B" to LAN B 192.168.2.1
Subnet Mask 255.255.255.0
Static Routes = Destination 192.168.3.20 Next Hop 192.168.2.10
              Destination 192.168.4.30 Next Hop 192.168.2.10

LAN A

Int "A"

Int "B"

CTC Workstation
IP Address 192.168.1.100
Subnet Mask 255.255.255.0
Default Gateway = 192.168.1.1
Host Routes = N/A

LAN B

ONS 15600 SDH #1
IP Address 192.168.2.10
Subnet Mask 255.255.255.0
Default Router = 192.168.2.1
Static Routes
    Destination = 192.168.1.100
    Mask = 255.255.255.255
    Next Hop = 192.168.2.1
    Cost = 2

SDH RING

ONS 15600 SDH #2
IP Address 192.168.3.20
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

ONS 15600 SDH #3
IP Address 192.168.4.30
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

159613

OSPF divides networks into smaller regions, called areas. An area is a collection of networked end systems, routers, and transmission facilities organized by traffic patterns. Each OSPF area has a unique ID number, known as the area ID, that can range from 0 to 4,294,967,295. Every OSPF network has one backbone area called "area 0." All other OSPF areas must connect to area 0.

When you enable ONS 15600 SDH OSPF topology for advertising to an OSPF network, you must assign an OSPF area ID in decimal format to the ONS 15600 SDH network. Coordinate the area ID number assignment with your LAN administrator. All DCC-connected ONS 15600 SDHs should be assigned the same OSPF area ID.

The ONS 15600 SDH supports the multiple OSPF area feature, which allows the ability to configure and support multiple OSPF areas in each DCC-connected topology. A node is in a single OSPF area if all of its DCC or LAN interfaces are in the same OSPF area, while a node is in multiple OSPF areas if it has DCC or LAN interfaces in two or more OSPF areas. If the ONS 15600 SDH has interfaces (DCC or LAN) in multiple OSPF areas, at least one ONS 15600 SDH interface (DCC or LAN) must be in the backbone area 0.

If multiple ONS 15600 SDH nodes and routers are connected to the same LAN in OSPF backbone area 0 and a link between two routers breaks, the backbone OSPF area 0 could divide into multiple gateway network elements (GNEs). If this occurs, the CTC session connected to Router 1 will not be able to communicate with the ONS 15600 SDH connected to Router 2. To resolve, you must repair the link between the routers or provide another form of redundancy in the network. This is standard behavior for an OSPF network.

**Note** To create OSPF virtual links, OSPF must be enabled on the LAN.

**Note** Cisco recommends limiting the number of link-state packets (LSPs) that will be forwarded over the DCC interfaces.

# 9.2.7 Scenario 7: Provisioning the ONS 15600 SDH Proxy Server

The ONS 15600 SDH proxy server is a set of functions that allows you to configure ONS 15600 SDHs in environments where visibility and accessibility between ONS 15600 SDHs and CTC computers must be restricted. For example, you can set up a network so that field technicians and network operations center (NOC) personnel can both access the same ONS 15600 SDHs while preventing the field technicians from accessing the NOC LAN. To do this, one ONS 15600 SDH is provisioned as a GNE and the other ONS 15600 SDHs are provisioned as ENEs. The GNE ONS 15600 SDH tunnels connections between CTC computers and ENE ONS 15600 SDHs, providing management capability while preventing access for purposes other than ONS 15600 SDH management.

The ONS 15600 SDH proxy server performs the following tasks:

- Isolates DCC IP traffic from Ethernet (craft port) traffic and accepts packets based on filtering rules. The filtering rules (see Table 9-3 on page 9-16 and Table 9-4 on page 9-16) depend on whether the packet arrives at the ONS 15600 SDH DCC or TSC Ethernet interface.

- Processes Simple Network Time Protocol/Network Time Protocol (SNTP/NTP) requests. ONS 15600 SDH ENEs can derive time-of-day from an SNTP/NTP LAN server through the ONS node GNE.

- Process SNMPv1 traps. The GNE ONS 15600 SDH receives SNMPv1 traps from the ONS node ENEs and forwards them to all provisioned SNMPv1 trap destinations.

The ONS 15600 SDH proxy server is provisioned using the Enable SOCKS proxy on port check box on the Provisioning > Network > General tab (see Figure 9-9). If checked, the ONS 15600 SDH serves as a proxy for connections between CTC clients and ONS 15600 SDHs that are DCC-connected to the proxy ONS 15600 SDH. The CTC client establishes connections to DCC-connected nodes through the proxy node. The CTC client can connect to nodes that it cannot directly reach from the host on which it runs. If not selected, the node does not proxy for any CTC clients, although any established proxy connections continue until the CTC client exits. If set as a GNE, the CTC computer is visible to other DCC-connected nodes and firewall is enabled. If Proxy-only is selected, the firewall is not enabled. CTC can communicate with any other DCC-connected ONS 15600 SDHs.

**Note** The ONS 15600 SDH ENE option on the Provisioning > Network > General tab behaves the same as the GNE option.

**Note** If you launch CTC against a node through a Network Address Translation (NAT) or Port Address Translation (PAT) router and that node does not have proxy enabled, your CTC session starts and initially appears to be fine. However CTC never receives alarm updates and disconnects and reconnects every two minutes. If the proxy is accidentally disabled, it is still possible to enable the proxy during a reconnect cycle and recover your ability to manage the node, even through a NAT/PAT firewall.

**Note** ENEs that belong to different private subnetworks do not need to have unique IP addresses. Two ENEs that are connected to different GNEs can have the same IP address. However, ENEs that connect to the same GNE must always have unique IP addresses.

*Figure 9-9    Proxy Server Gateway Settings*

## 9.2.7.1 Firewall Not Enabled

Figure 9-10 shows an ONS 15600 SDH proxy server implementation. A ONS 15600 SDH GNE is connected to a central office LAN and to ONS 15600 SDH ENEs. The central office LAN is connected to a NOC LAN, which has CTC computers. The NOC CTC computer and craft technicians must both be able to access the ONS 15600 SDH ENEs. However, the craft technicians must be prevented from accessing or seeing the NOC or central office LANs.

In the example, the ONS 15600 SDH GNE is assigned an IP address within the central office LAN and is physically connected to the LAN through its LAN port. ONS 15600 SDH ENEs are assigned IP addresses that are outside the central office LAN and given private network IP addresses. If the ONS 15600 SDH ENEs are collocated, the craft LAN ports could be connected to a hub. However, the hub should have no other network connections.

*Figure 9-10    ONS 15600 SDH Proxy Server with GNE and ENEs on the Same Subnet*
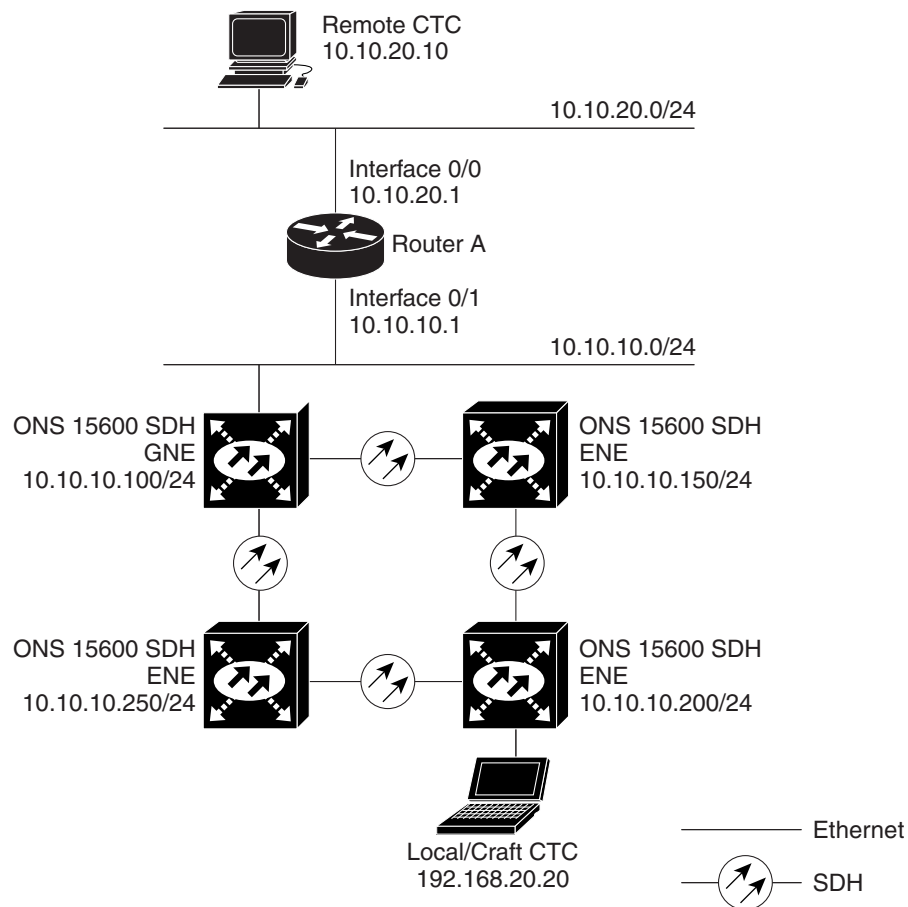


Table 9-2 shows recommended settings for ONS 15600 SDH GNEs and ENEs in the configuration shown in Figure 9-10.

*Table 9-2 ONS 15600 SDH GNE and ENE Settings*

| Setting | ONS 15600 SDH GNE | ONS 15600 SDH ENE |
|---|---|---|
| Enable proxy server on port | On | On |
| GNE | On | Off |
| ENE | Off | On |
| Proxy only | Off | Off |
| OSPF (LAN) | Off | Off |
| SNTP server (if used) | SNTP server IP address | Set to the ONS 15600 SDH GNE IP address |
| SNMP (if used) | SNMPv1 trap destinations | Set SNMPv1 trap destinations to ONS 15600 SDH GNE, port 391 |

Figure 9-11 shows the same proxy server implementation with ONS 15600 SDH ENEs on different subnets. The ONS 15600 SDH GNEs and ENEs are provisioned with the settings shown in Table 9-2.

*Figure 9-11 Scenario 7: ONS 15600 SDH Proxy Server with GNE and ENEs on Different Subnets*
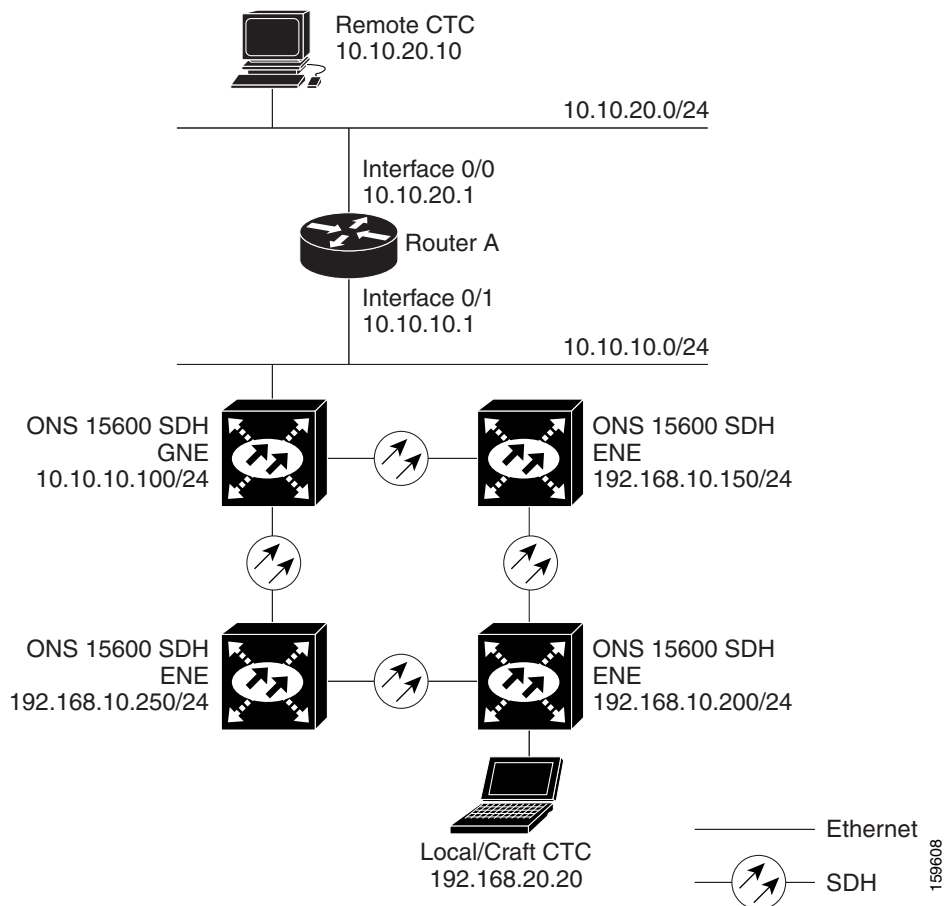
Figure 9-12 shows the Figure 9-11 implementation with ONS 15600 SDH ENEs in multiple rings. The ONS 15600 SDH GNEs and ENEs are provisioned with the settings shown in Table 9-2.

*Figure 9-12* *Scenario 7: ONS 15600 SDH Proxy Server With ENEs on Multiple Rings*
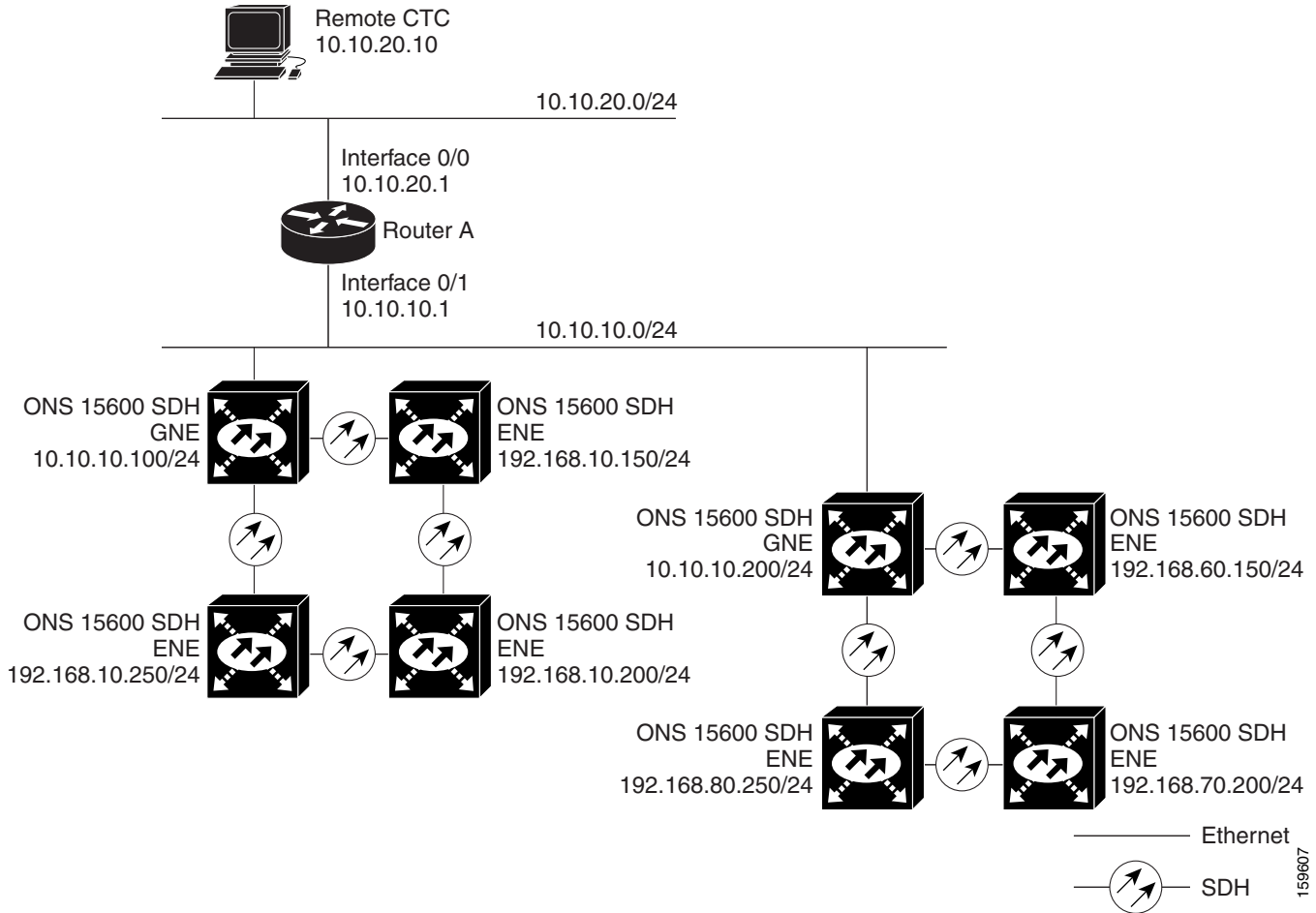


## 9.2.7.2 Firewall Enabled

Table 9-3 shows the rules the ONS 15600 SDH uses to filter packets when the firewall is enabled.

*Table 9-3        Proxy Server Firewall Filtering Rules*

| Packets Arriving At: | Are Accepted if the IP Destination Address Is: |
|---|---|
| TSC Ethernet interface | • The ONS 15600 SDH itself<br>• The ONS 15600 SDH subnet broadcast address<br>• Within the 224.0.0.0/8 network (reserved network used for standard multicast messages) |
| DCC interface | • The ONS 15600 SDH itself<br>• Any destination connected through another DCC interface<br>• Within the 224.0.0.0/8 network |

The rules in Table 9-4 are applied if a packet is addressed to the ONS 15600 SDH. Rejected packets are discarded.

*Table 9-4        Proxy Server Firewall Filtering Rules When Packet Addressed to ONS 15600 SDH*

| Packets Arriving At: | Accepts | Rejects |
|---|---|---|
| TSC Ethernet interface | • All IP protocols except user datagram protocol (UDP)<br>• All UDP packets except packets address to the SNMP trap relay port | • UDP packets addressed to the SNMP trap relay port (391) |
| DCC interface | • All ICMP, OSPF, RSVP, and LMP packets<br>• All TCP packets except packets addressed to the Telnet and proxy server ports | • TCP packets addressed to the Telnet port<br>• TCP packets addressed to the proxy server port<br>• Protocols not listed in the Accepted column |

If an ONS 15600 SDH or CTC computer resides behind a firewall that uses port filtering, you must enable an Internet Inter-ORB Protocol (IIOP) port on the ONS 15600 SDH and/or CTC computer, depending on whether one or both devices reside behind a firewall. You can enable an IIOP port on the Provisioning > Network > General tab in CTC.

Figure 9-13 shows ONS 15600 SDHs in a protected network and the CTC computer in an external network. For the computer to access the ONS 15600 SDHs, you must provision the IIOP listener port specified by your firewall administrator on the ONS 15600 SDH. The ONS 15600 SDH sends the port number to the CTC computer during the initial contact between the devices using Hyper-Text Transfer Protocol (HTTP). After the CTC computer obtains the ONS 15600 SDH IIOP port, the computer opens a direct session with the node using the specified IIOP port.

*Figure 9-13*      ***Nodes Behind a Firewall***
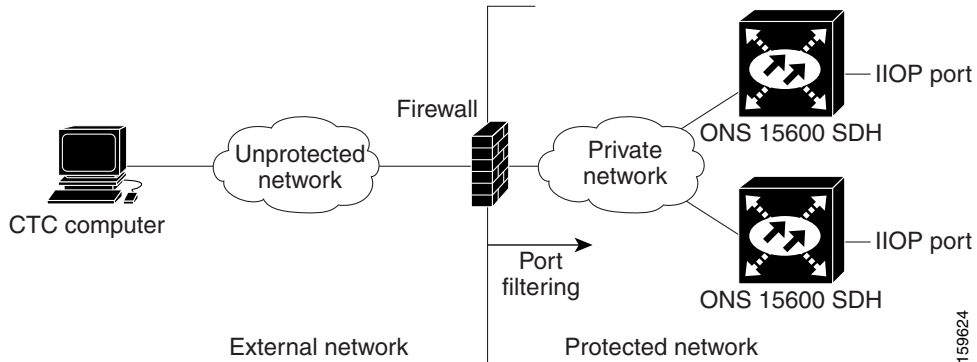


Figure 9-14 shows a CTC computer and ONS 15600 SDHs behind firewalls. For the computer to access the ONS 15600 SDH, you must provision the IIOP port on the CTC computer and on the ONS 15600 SDH. Each firewall can use a different IIOP port. For example, if the CTC computer firewall uses IIOP port 4000, and the ONS 15600 SDH firewall uses IIOP port 5000, 4000 is the IIOP port you provision for the CTC computer and 5000 is the IIOP port you provision for the ONS 15600 SDH.

*Figure 9-14*      ***CTC Computer and ONS 15600 SDHs Residing Behind Firewalls***
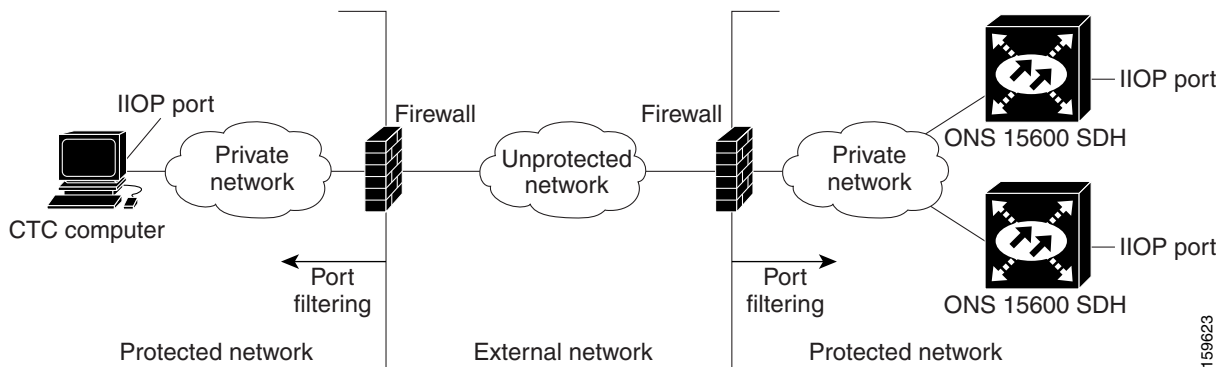


If you implement the proxy server, note that all DCC-connected ONS 15600 SDHs on the same Ethernet segment must have the same gateway setting. Mixed values produce unpredictable results, and might leave some nodes unreachable through the shared Ethernet segment.

If nodes become unreachable, correct the setting by performing one of the following actions:

- Disconnect the craft computer from the unreachable ONS 15600 SDH. Connect to the ONS 15600 SDH through another network ONS 15600 SDH that has a DCC connection to the unreachable ONS 15600 SDH.

- Disconnect all DCCs to the node by disabling them on neighboring nodes. Connect a CTC computer directly to the ONS 15600 SDH and change its provisioning.

# 9.2.8 Scenario 8: Dual GNEs on a Subnet

The ONS 15600 SDH provides GNE load balancing, which allows CTC to reach ENEs over multiple GNEs without the ENEs being advertised over OSPF. This feature allows a network to quickly recover from the loss of a GNE, even if the GNE is on a different subnet. If a GNE fails, all connections through

that GNE fail. CTC disconnects from the failed GNE and from all ENEs for which the GNE was a proxy and then reconnects through the remaining GNEs. GNE load balancing reduces the dependency on the launch GNE and DCC bandwidth, which enhances CTC performance. Figure 9-15 shows a network with dual GNEs on the same subnet.

*Figure 9-15*     *Scenario 8: Dual GNEs on the Same Subnet*
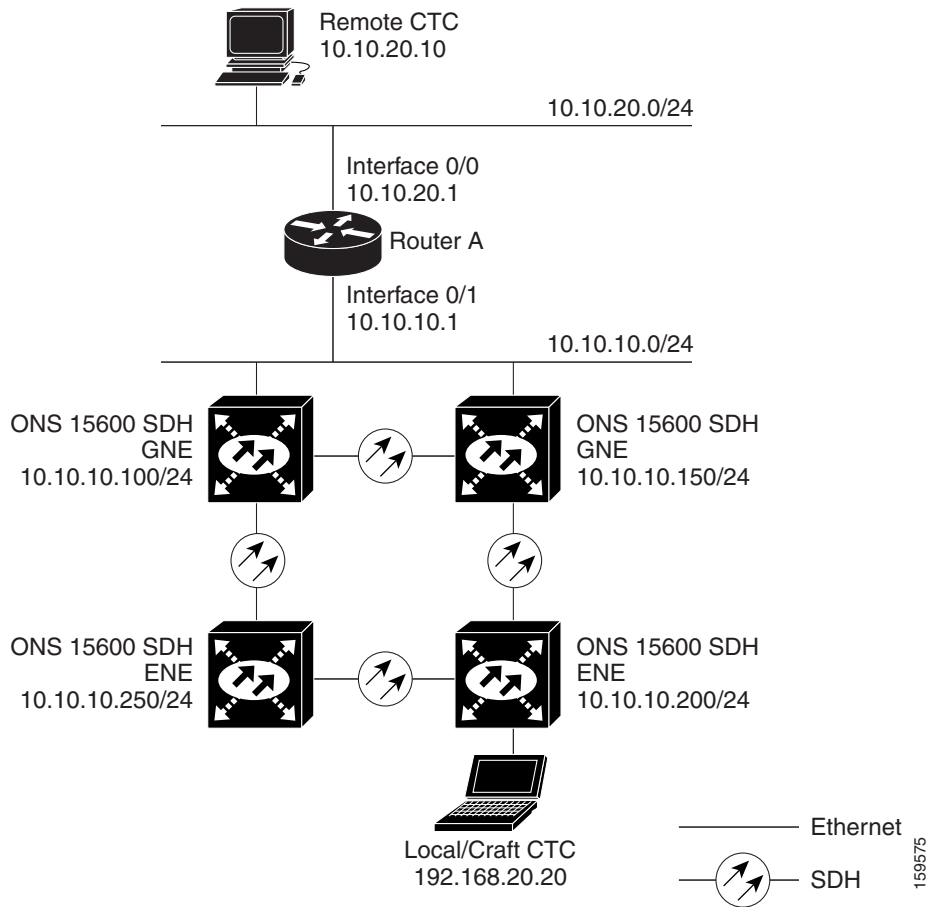
Figure 9-16 shows a network with dual GNEs on different subnets.

*Figure 9-16*      ***Scenario 8: Dual GNEs on Different Subnets***
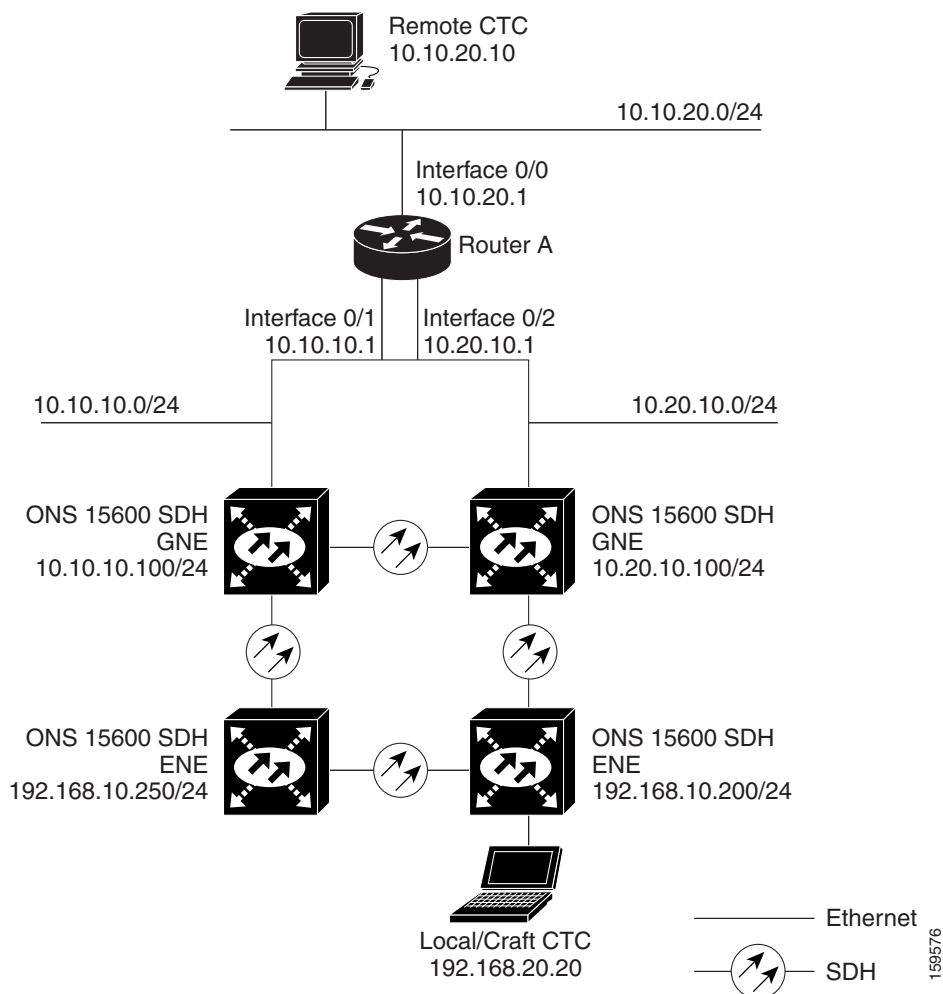


# 9.3 Routing Table

ONS 15600 SDH routing information appears on the Maintenance > Routing Table tab (Figure 9-17). The routing table provides the following information:

- Destination—Displays the IP address of the destination network or host.

- Mask—Displays the subnet mask used to reach the destination host or network.

- Gateway—Displays the IP address of the gateway used to reach the destination network or host.

- Usage—Shows the number of times this route has been used.

- Interface—Shows the ONS 15600 SDH interface used to access the destination.

    - pend0—The Ethernet management interface.

- – pdcc—An RS-DCC interface, that is, an STM-N trunk (span) card identified as the RS-DCC termination (0 to 128).

- – lo0—A loopback interface.

- – pend2—The craft-only RJ-45 jack on the front of the TSC.

- – motfcc0—Interface on the TSC that connect the TSC to all other cards except the other TSC.

- – hdlc0—Connects the two TSC cards together; traffic cards forward DCC packets over the motfcc0 Ethernet interface.

*Figure 9-17        Viewing the ONS 15600 SDH Routing Table*



Table 9-5 shows sample routing entries for an ONS 15600 SDH.

*Table 9-5        Sample Routing Table Entries*

| Entry | Destination | Mask | Gateway | Interface |
|---|---|---|---|---|
| 1 | 0.0.0.0 | 0.0.0.0 | 172.20.214.1 | cpm0 |
| 2 | 172.20.214.0 | 255.255.255.0 | 172.20.214.92 | cpm0 |
| 3 | 172.20.214.92 | 255.255.255.255 | 127.0.0.1 | lo0 |

*Table 9-5      Sample Routing Table Entries (continued)*

| Entry | Destination | Mask | Gateway | Interface |
|-------|-------------|------|---------|-----------|
| 4 | 172.20.214.93 | 255.255.255.255 | 0.0.0.0 | pdcc0 |
| 5 | 172.20.214.94 | 255.255.255.255 | 172.20.214.93 | pdcc0 |

Entry 1 shows the following:

- Destination (0.0.0.0) is the default route entry. All undefined destination network or host entries on this routing table will be mapped to the default route entry.

- Mask (0.0.0.0) is always 0 for the default route.

- Gateway (172.20.214.1) is the default gateway address. All outbound traffic that cannot be found in this routing table or is not on the node's local subnet will be sent to this gateway.

- Interface (cpm0) indicates that the ONS 15600 SDH Ethernet interface is used to reach the gateway.

Entry 2 shows the following:

- Destination (172.20.214.0) is the destination network IP address.

- Mask (255.255.255.0) is a 24-bit mask, meaning all addresses within the 172.20.214.0 subnet can be destinations.

- Gateway (172.20.214.92) is the gateway address. All outbound traffic belonging to this network is sent to this gateway.

- Interface (cpm0) indicates that the ONS 15600 SDH Ethernet interface is used to reach the gateway.

Entry 3 shows the following:

- Destination (172.20.214.92) is the destination host IP address.

- Mask (255.255.255.255) is a 32-bit mask, meaning only the 172.20.214.92 address is a destination.

- Gateway (127.0.0.1) is a loopback address. The host directs network traffic to itself using this address.

- Interface (lo0) indicates that the local loopback interface is used to reach the gateway.

Entry 4 shows the following:

- Destination (172.20.214.93) is the destination host IP address.

- Mask (255.255.255.255) is a 32-bit mask, meaning only the 172.20.214.93 address is a destination.

- Gateway (0.0.0.0) means the destination host is directly attached to the node.

- Interface (pdcc0) indicates that a SDH DCC interface is used to reach the destination host.

Entry 5 shows a DCC-connected node that is accessible through a node that is not directly connected:

- Destination (172.20.214.94) is the destination host IP address.

- Mask (255.255.255.255) is a 32-bit mask, meaning only the 172.20.214.94 address is a destination.

- Gateway (172.20.214.93) indicates that the destination host is accessed through a node with the IP address 172.20.214.93.

- Interface (pdcc0) indicates that a SDH DCC interface is used to reach the gateway.

# 9.4 External Firewalls

This section provides sample access control lists for external firewalls. Table 9-6 lists the ports that are used by the TSC.

*Table 9-6        Ports Used by the TSC*

| Port | Function | Action[1] |
|------|----------|-----------|
| 0 | Never used | D |
| 20 | FTP | D |
| 21 | FTP control | D |
| 22 | SSH (Secure Shell) | D |
| 23 | Telnet | D |
| 80 | HTTP | D |
| 111 | SUNRPC (Sun Remote Procedure Call) | D |
| 161 | SNMP traps destinations | D |
| 162 | SNMP traps destinations | D |
| 513 | rlogin | D |
| 683 | CORBA IIOP | OK |
| 1080 | Proxy server (socks) | D |
| 2001-2017 | I/O card Telnet | NA |
| 2018 | DCC processor on active TCC2/TCC2P | D |
| 2361 | TL1 | D |
| 3082 | Raw TL1 | D |
| 3083 | TL1 | D |
| 5001 | MS-SPRing server port | D |
| 5002 | MS-SPRing client port | D |
| 7200 | SNMP alarm input port | D |
| 9100 | EQM port | D |
| 9401 | TCC boot port | D |
| 9999 | Flash manager | NA |
| 10240-12287 | Proxy client | D |
| 57790 | Default TCC listener port | OK |

1.  D = deny, NA = not applicable, OK = do not deny

The following ACL (access control list) example shows a firewall configuration when the SOCKS proxy server gateway setting is not enabled. In the example, the CTC workstation's address is 192.168.10.10. and the ONS 15600 SDH address is 10.10.10.100. The firewall is attached to the GNE, so the inbound direction is from CTC to the GNE and the outbound direction is from the GNE to CTC. The CTC Common Object Request Broker Architecture (CORBA) Standard constant is 683 and the TCC CORBA Default is TCC Fixed (57790).

```
access-list 100 remark *** Inbound ACL, CTC -> NE ***
```

```
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 eq www
access-list 100 remark *** allows initial contact with ONS 15600 SDH using http (port 80)
***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 eq 57790
access-list 100 remark *** allows CTC communication with ONS 15600 SDH GNE (port 57790)
***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 established
access-list 100 remark *** allows ACKs back from CTC to ONS 15600 SDH GNE ***

access-list 101 remark *** Outbound ACL, NE -> CTC ***
access-list 101 remark
access-list 101 permit tcp host 10.10.10.100 host 192.168.10.10 eq 683
access-list 101 remark *** allows alarms etc., from the 15600 SDH (random port) to the CTC
workstation (port 683) ***
access-list 100 remark
access-list 101 permit tcp host 10.10.10.100 host 192.168.10.10 established
access-list 101 remark *** allows ACKs from the 15600 SDH GNE to CTC ***
```

The following ACL (access control list) example shows a firewall configuration when the SOCKS proxy server gateway setting is enabled. As with the first example, the CTC workstation address is 192.168.10.10 and the ONS 15600 SDH address is 10.10.10.100. The firewall is attached to the GNE, so inbound is CTC to the GNE and outbound is from the GNE to CTC. CTC CORBA Standard constant (683) and TCC CORBA Default is TCC Fixed (57790).

```
access-list 100 remark *** Inbound ACL, CTC -> NE ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 eq www
access-list 100 remark *** allows initial contact with the 15600 SDH using http (port 80)
***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 eq 1080
access-list 100 remark *** allows CTC communication with the 15600 SDH GNE (port 1080) ***
access-list 100 remark

access-list 101 remark *** Outbound ACL, NE -> CTC ***
access-list 101 remark
access-list 101 permit tcp host 10.10.10.100 host 192.168.10.10 established
access-list 101 remark *** allows ACKs from the 15600 SDH GNE to CTC ***
```

# 9.5 Open GNE

The ONS 15600 SDH can communicate with non-ONS nodes that do not support point-to-point protocol (PPP) vendor extensions or OSPF type 10 opaque link-state advertisements (LSA), both of which are necessary for automatic node and link discovery. An open GNE configuration allows the DCC-based network to function as an IP network for non-ONS nodes.

To configure an open GNE network, you can provision RS-DCC and MS-DCC terminations to include a far-end, non-ONS node using either the default IP address of 0.0.0.0 or a specified IP address. You provision a far-end, non-ONS node by checking the "Far End is Foreign" check box during RS-DCC and MS-DCC creation. The default 0.0.0.0 IP address allows the far-end, non-ONS node to provide the IP address; if you set an IP address other than 0.0.0.0, a link is established only if the far-end node identifies itself with that IP address, providing an extra level of security.

By default, the proxy server only allows connections to discovered ONS peers and the firewall blocks all IP traffic between the DCC network and LAN. You can, however, provision proxy tunnels to allow up to 12 additional destinations for SOCKS version 5 connections to non-ONS nodes. You can also

provision firewall tunnels to allow up to 12 additional destinations for direct IP connectivity between the DCC network and LAN. Proxy and firewall tunnels include both a source and destination subnet. The connection must originate within the source subnet and terminate within the destination subnet before either the SOCKS connection or IP packet flow is allowed.

To set up proxy and firewall subnets in CTC, use the Provisioning > Network > Proxy tab and the Provisioning > Networki > Firewalls tab. The availability of proxy and/or firewall tunnels depends on the network access settings of the node:

- If the node is configured with the proxy server enabled in GNE or ENE mode, you must set up a proxy tunnel and/or a firewall tunnel.

- If the node is configured with the proxy server enabled in proxy-only mode, you can set up proxy tunnels. Firewall tunnels are not allowed.

- If the node is configured with the proxy server disabled, neither proxy tunnels or firewall tunnels are allowed.

Figure 9-18 shows an example of a foreign node connected to the DCC network. Proxy and firewall tunnels are useful in this example because the GNE would otherwise block IP access between the PC and the foreign node.

*Figure 9-18    Proxy and Firewall Tunnels for Foreign Terminations*
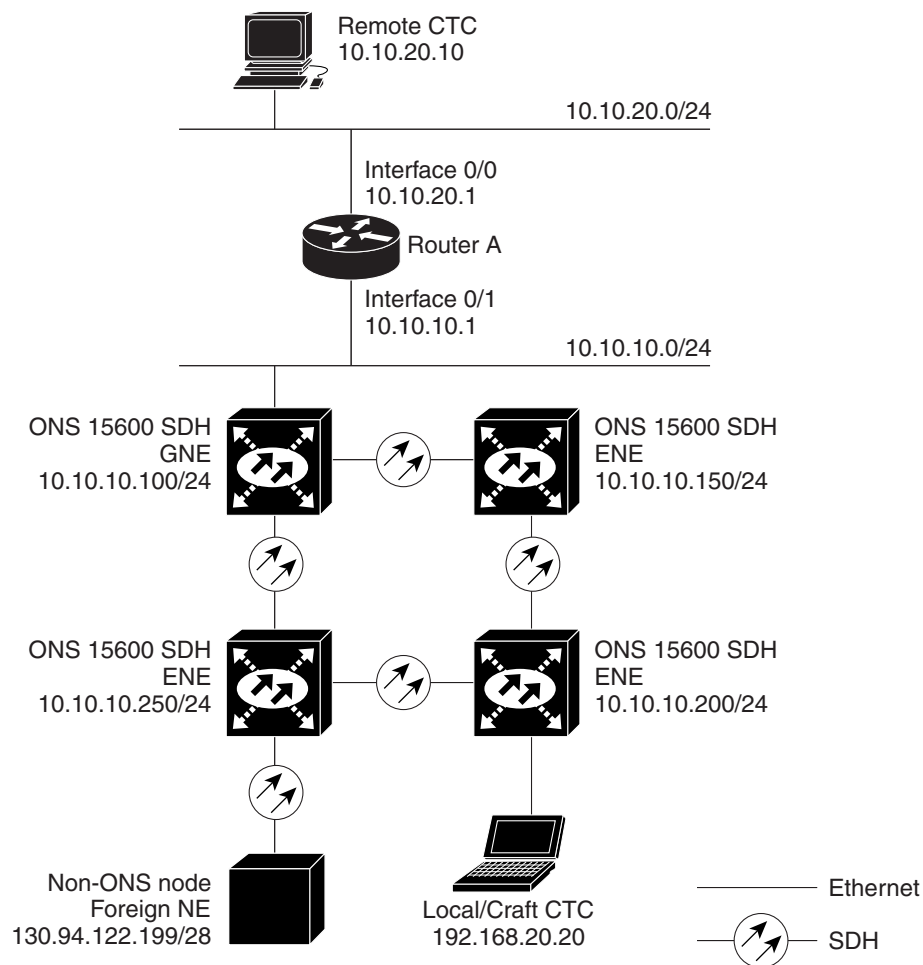
Figure 9-19 shows a remote node connected to an ENE Ethernet port. Proxy and firewall tunnels are useful in this example because the GNE would otherwise block IP access between the PC and foreign node. This configuration also requires a firewall tunnel on the ENE.

*Figure 9-19 Foreign Node Connection to an ENE Ethernet Port*
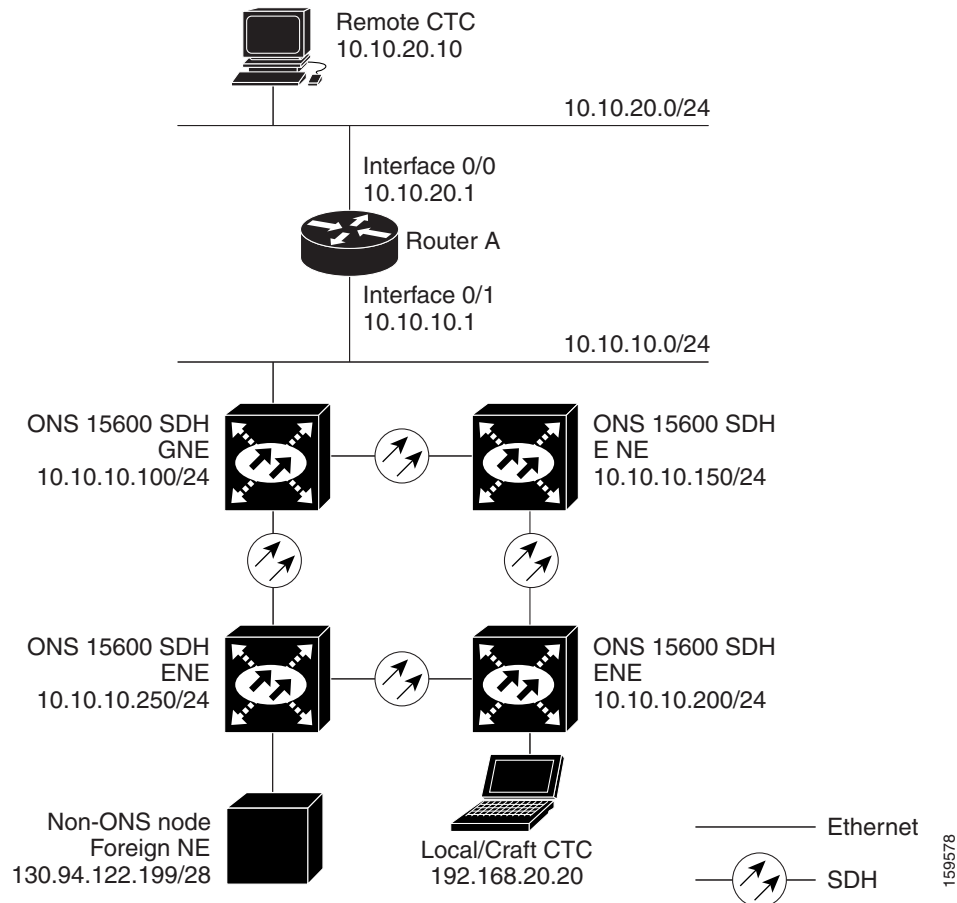


## 9.6 TCP/IP and OSI Networking

ONS 15600 SDH DCN communication is based on the TCP/IP protocol suite. However, ONS 15600 SDHs can also be networked with equipment that uses the OSI protocol suite. While TCP/IP and OSI protocols are not directly compatible, they do have the same objectives and occupy similar layers of the OSI reference model. Table 9-7 shows the protocols and mediation processes that are involved when TCP/IP-based NEs are networked with OSI-based NEs.

*Table 9-7*        *TCP/IP and OSI Protocols*

| OSI Model | IP Protocols | OSI Protocols | | IP-OSI Mediation |
|---|---|---|---|---|
| Layer 7 Application | • TL1<br>• FTP<br>• HTTP<br>• Telnet<br>• IIOP | • TARP[1] | • TL1 (over OSI)<br>• FTAM[2]<br>• ACSE[3] | • T–TD[4]<br>• FT–TD[5] |
| Layer 6 Presentation | | | • PST[6] | — |
| Layer 5 Session | | | • Session | — |
| Layer 4 Transport | • TCP<br>• UDP | | • TP (Transport) Class 4 | • IP-over-CLNS[7] tunnels |
| Layer 3 Network | • IP<br>• OSPF | • CLNP[8]<br>• ES-IS[9]<br>• IS-IS[10] | | |
| Layer 2 Data link | • PPP | • PPP<br>• LAP-D[11] | | |
| Layer 1 Physical | DCC, LAN, fiber, electrical | DCC, LAN, fiber, electrical | | — |

1. TARP = TID Address Resolution Protocol
2. FTAM = File Transfer and Access Management
3. ACSE = Association-control service element
4. T–TD = TL1–Translation Device
5. FT–TD = File Transfer—Translation Device
6. PST = Presentation layer
7. CLNS = Connectionless Network Layer Service
8. CLNP = Connectionless Network Layer Protocol
9. ES-IS = End System-to-Intermediate System
10. IS-IS = Intermediate System-to-Intermediate System
11. LAP-D = Link Access Protocol on the D Channel

## 9.6.1 Point-to-Point Protocol

PPP is a data link (Layer 2) encapsulation protocol that transports datagrams over point-to-point links. Although PPP was developed to transport IP traffic, it can carry other protocols including the OSI CLNP. PPP components used in the transport of OSI include:

• High-level data link control (HDLC)—Performs the datagram encapsulation for transport across point-to-point links.

• Link control protocol (LCP)—Establishes, configures, and tests the point-to-point connections.

CTC automatically enables IP over PPP whenever you create an RS-DCC or MS-DCC. The RS-DCC or MS-DCC can be provisioned to support OSI over PPP.

## 9.6.2  Link Access Protocol on the D Channel

LAP-D is a data link protocol used in the OSI protocol stack. LAP-D is assigned when you provision an ONS 15600 SDH RS-DCC as OSI-only. Provisionable LAP-D parameters include:

- Transfer Service—One of the following transfer services must be assigned:

  - Acknowledged Information Transfer Service (AITS)—(Default) 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.

  - Unacknowledged Information Transfer Service (UITS)—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.

- Mode—LAP-D is set to either Network or User mode. This parameter sets the LAP-D frame command/response (C/R) value, which indicates whether the frame is a command or a response.

- Maximum transmission unit (MTU)—The LAP-D N201 parameter sets the maximum number of octets in a LAP-D information frame. The range is 512 to 1500 octets.

> **Note**    The MTU must be the same size for all NEs on the network.

- Transmission Timers—The following LAP-D timers can be provisioned:

  - The T200 timer sets the timeout period for initiating retries or declaring failures.

  - The T203 timer provisions the maximum time between frame exchanges, that is, the trigger for transmission of the LAP-D "keep-alive" Receive Ready (RR) frames.

Fixed values are assigned to the following LAP-D parameters:

- Terminal Endpoint Identifier (TEI)—A fixed value of 0 is assigned.

- Service Access Point Identifier (SAPI)—A fixed value of 62 is assigned.

- N200 supervisory frame retransmissions—A fixed value of 3 is assigned.

## 9.6.3  OSI Connectionless Network Service

OSI connectionless network service is implemented by using the Connectionless Network Protocol (CLNP) and Connectionless Network Service (CLNS). CLNP and CLNS are described in the ISO 8473 standard. CLNS provides network layer services to the transport layer through CLNP. CLNS does not perform connection setup or termination because paths are determined independently for each packet that is transmitted through a network. CLNS relies on transport layer protocols to perform error detection and correction.

CLNP is an OSI network layer protocol that carries upper-layer data and error indications over connectionless links. CLNP provides the interface between the CLNS and upper layers. CLNP performs many of the same services for the transport layer as IP. The CLNP datagram is very similar to the IP datagram. It provides mechanisms for fragmentation (data unit identification, fragment/total length, and offset). Like IP, a checksum computed on the CLNP header verifies that the information used to process the CLNP datagram is transmitted correctly, and a lifetime control mechanism (Time to Live) limits the amount of time a datagram is allowed to remain in the system.

CLNP uses network service access points (NSAPs) to identify network devices. The CLNP source and destination addresses are NSAPs. In addition, CLNP uses a network element title (NET) to identify a network-entity in an end system (ES) or intermediate system (IS). NETs are allocated from the same name space as NSAP addresses. Whether an address is an NSAP address or a NET depends on the network selector value in the NSAP.

The ONS 15600 SDH supports the ISO Data Country Code (ISO-DCC) NSAP address format as specified in ISO 8348. The NSAP address is divided into an initial domain part (IDP) and a domain-specific part (DSP). NSAP fields are shown in Table 9-8. NSAP field values are in hexadecimal format. All NSAPs are editable. Shorter NSAPs can be used. However NSAPs for all NEs residing within the same OSI network area usually have the same NSAP format.

*Table 9-8        NSAP Fields*

| Field | Definition | Description |
|-------|-----------|-------------|
| **IDP** | | |
| AFI | Authority and format identifier | Specifies the NSAP address format. The initial value is 39 for the ISO-DCC address format. |
| IDI | Initial domain identifier | Specifies the country code. The initial value is 840F, the United States country code padded with an F. |
| **DSP** | | |
| DFI | DSP format identifier | Specifies the DSP format. The initial value is 80, indicating the DSP format follows American National Standards Institute (ANSI) standards. |
| ORG | Organization | Organization identifier. The initial value is 000000. |
| Reserved | Reserved | Reserved NSAP field. The Reserved field is normally all zeros (0000). |
| RD | Routing domain | Defines the routing domain. The initial value is 0000. |
| AREA | Area | Identifies the OSI routing area to which the node belongs. The initial value is 0000. |

*Table 9-8 NSAP Fields (continued)*

| Field | Definition | Description |
|-------|-----------|-------------|
| System | System identifier | The ONS 15600 SDH system identifier is set to its IEEE 802.3 MAC address. Each ONS 15600 SDH supports twelve OSI virtual routers. Each router NSAP system identifier is the ONS 15600 SDH IEEE 802.3 MAC address + $n$, where $n$ = 0 to 2. For the primary virtual router, $n$ = 0. |
| SEL | Selector | The selector field directs the protocol data units (PDUs) to the correct destination using the CLNP network layer service. Selector values supported by the ONS 15600 SDH include: |
| | | • 00—Network Entity Title (NET). Used to exchange PDUs in the ES-IS and IS-IS routing exchange protocols. (See the "9.6.4.1 End System-to-Intermediate System Protocol" section on page 9-31, and "9.6.4.2 Intermediate System-to-Intermediate System" section on page 9-31.) |
| | | • 1D—Selector for Transport Class 4 (and for FTAM and TL1 applications (Telcordia GR-253-CORE standard) |
| | | • AF—Selector for the TARP protocol (Telcordia GR-253-CORE standard) |
| | | • 2F—Selector for the GRE IP-over-CLNS tunnel (ITU/RFC standard) |
| | | • CC—Selector for the Cisco IP-over-CLNS tunnels (Cisco specific) |
| | | • E0—Selector for the OSI ping application (Cisco specific) |
| | | NSELs are only advertised when the node is configured as an ES. They are not advertised when a node is configured as an IS. Tunnel NSELs are not advertised until a tunnel is created. |

Figure 9-20 shows the ISO-DCC NSAP address with the default values delivered with the ONS 15600 SDH. The System ID is automatically populated with the node MAC address.

*Figure 9-20 ISO-DCC NSAP Address*
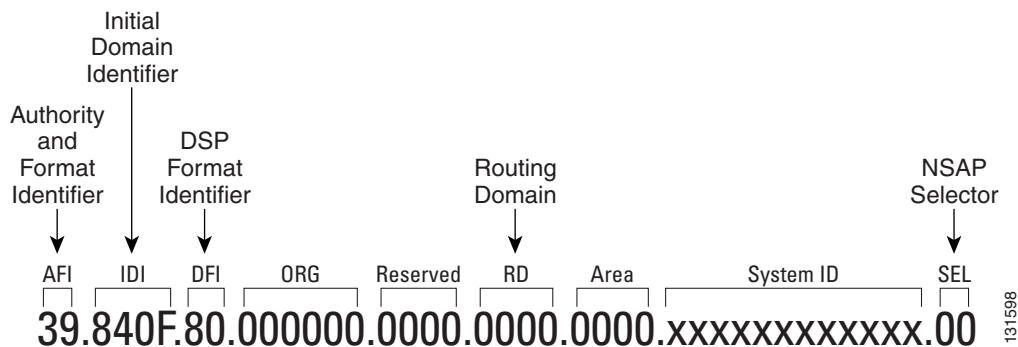
The ONS 15600 SDH main NSAP address is shown on the node view Provisioning > OSI > Main Setup tab. This address is also the Router 1 primary manual area address, which is viewed and edited on Provisioning > OSI > Routers tab. See the "9.6.7 OSI Virtual Routers" section on page 9-36 for information about the OSI router and manual area addresses in CTC.

## 9.6.4  OSI Routing

OSI architecture includes ESs and ISs. The OSI routing scheme includes:

- A set of routing protocols that allow ESs and ISs to collect and distribute the information necessary to determine routes. Protocols include the ES-IS and IS-IS protocols. ES-IS routing establishes connectivity and reach ability among ESs and ISs attached to the same (single) subnetwork.

- A routing information base (RIB) containing this information, from which routes between ESs can be computed. The RIB consists of a table of entries that identify a destination (for example, an NSAP), the subnetwork over which packets should be forwarded to reach that destination, and a routing metric. The routing metric communicates characteristics of the route (such as delay properties or expected error rate) that are used to evaluate the suitability of a route compared to another route with different properties, for transporting a particular packet or class of packets.

- A routing algorithm, Shortest Path First (SPF), that uses information contained in the RIB to derive routes between ESs.

In OSI networking, discovery is based on announcements. An ES uses the ES-IS protocol end system hello (ESH) message to announce its presence to ISs and ESs connected to the same network. Any ES or IS that is listening for ESHs gets a copy. ISs store the NSAP address and the corresponding subnetwork address pair in routing tables. ESs might store the address, or they might wait to be informed by ISs when they need such information.

An IS composes intermediate system hello (ISH) messages to announce its configuration information to ISs and ESs that are connected to the same broadcast subnetwork. Like the ESHs, the ISH contains the addressing information for the IS (the NET and the subnetwork point-of-attachment address [SNPA]) and a holding time. ISHs might also communicate a suggested ES configuration time recommending a configuration timer to ESs.

The exchange of ISHs is called neighbor greeting or initialization. Each router learns about the other routers with which they share direct connectivity. After the initialization, each router constructs a link-state packet (LSP). The LSP contains a list of the names of the IS's neighbors and the cost to reach each of the neighbors. Routers then distribute the LSPs to all of the other routers. When all LSPs are propagated to all routers, each router has a complete map of the network topology (in the form of LSPs). Routers use the LSPs and the SPF algorithm to compute routes to every destination in the network.

OSI networks are divided into areas and domains. An area is a group of contiguous networks and attached hosts that is designated as an area by a network administrator. A domain is a collection of connected areas. Routing domains provide full connectivity to all ESs within them. Routing within the same area is known as Level 1 routing. Routing between two areas is known as Level 2 routing. LSPs that are exchanged within a Level 1 area are called L1 LSPs. LSPs that are exchanged across Level 2 areas are called L2 LSPs. Figure 9-21 shows an example of Level 1 and Level 2 routing.

**Figure 9-21** *Level 1 and Level 2 OSI Routing*
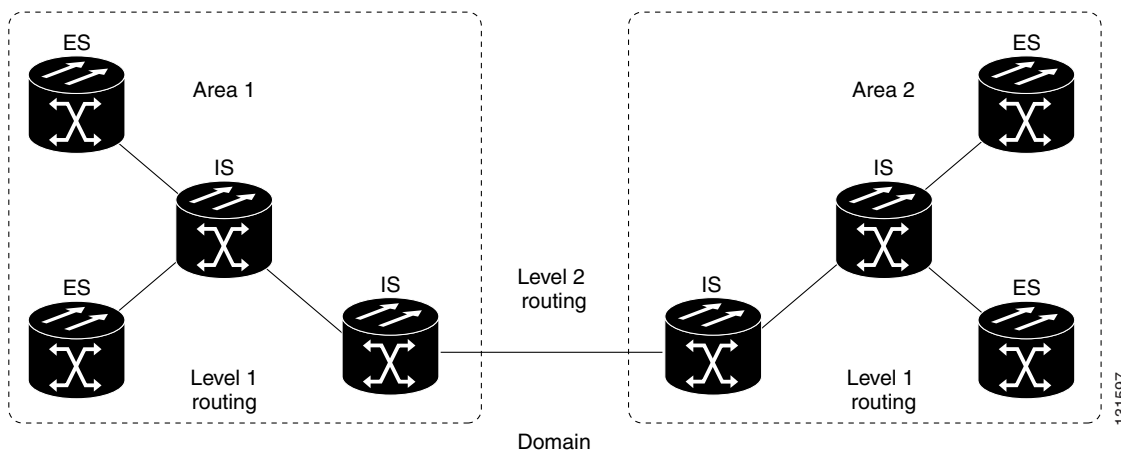


When you provision an ONS 15600 SDH for a network with NEs that use both the TCP/IP and OSI protocol stacks, you will provision it as one of the following:

- Intermediate System Level 1—The ONS 15600 SDH performs OSI IS functions. It communicates with IS and ES nodes that reside within its OSI area. It depends upon an IS L1/L2 node to communicate with IS and ES nodes that reside outside its OSI area.

- Intermediate System Level 1/Level 2—The ONS 15600 SDH performs IS functions. It communicates with IS and ES nodes that reside within its OSI area. It also communicates with IS L1/L2 nodes that reside in other OSI areas. This option should not be provisioned unless the node is connected to another IS L1/L2 node that resides in a different OSI area. The node must also be connected to all nodes within its area that are provisioned as IS L1/L2.

## 9.6.4.1 End System-to-Intermediate System Protocol

ES-IS is an OSI protocol that defines how ESs (hosts) and ISs (routers) learn about each other. ES-IS configuration information is transmitted at regular intervals through the ES and IS hello messages. The hello messages contain the subnetwork and network layer addresses of the systems that generate them.

The ES-IS configuration protocol communicates both OSI network layer addresses and OSI subnetwork addresses. OSI network layer addresses identify either the NSAP, which is the interface between OSI Layer 3 and Layer 4, or the NET, which is the network layer entity in an OSI IS. OSI SNPAs are the points at which an ES or IS is physically attached to a subnetwork. The SNPA address uniquely identifies each system attached to the subnetwork. In an Ethernet network, for example, the SNPA is the 48-bit MAC address. Part of the configuration information transmitted by ES-IS is the NSAP-to-SNPA or NET-to-SNPA mapping.

## 9.6.4.2 Intermediate System-to-Intermediate System

IS-IS is an OSI link-state hierarchical routing protocol that floods the network with link-state information to build a complete, consistent picture of a network topology. IS-IS distinguishes between Level 1 and Level 2 ISs. Level 1 ISs communicate with other Level 1 ISs in the same area. Level 2 ISs route between Level 1 areas and form an intradomain routing backbone. Level 1 ISs need to know only how to get to the nearest Level 2 IS. The backbone routing protocol can change without impacting the intra-area routing protocol.

OSI routing begins when the ESs discover the nearest IS by listening to ISH packets. When an ES wants to send a packet to another ES, it sends the packet to one of the ISs on its directly attached network. The router then looks up the destination address and forwards the packet along the best route. If the destination ES is on the same subnetwork, the local IS knows this from listening to ESHs and forwards the packet appropriately. The IS also might provide a redirect (RD) message back to the source to tell it that a more direct route is available. If the destination address is an ES on another subnetwork in the same area, the IS knows the correct route and forwards the packet appropriately. If the destination address is an ES in another area, the Level 1 IS sends the packet to the nearest Level 2 IS. Forwarding through Level 2 ISs continues until the packet reaches a Level 2 IS in the destination area. Within the destination area, the ISs forward the packet along the best path until the destination ES is reached.

Link-state update messages help ISs learn about the network topology. Each IS generates an update specifying the ESs and ISs to which it is connected, as well as the associated metrics. The update is then sent to all neighboring ISs, which forward (flood) it to their neighbors, and so on. (Sequence numbers terminate the flood and distinguish old updates from new ones.) Using these updates, each IS can build a complete topology of the network. When the topology changes, new updates are sent.

IS-IS uses a single required default metric with a maximum path value of 1024. The metric is arbitrary and typically is assigned by a network administrator. Any single link can have a maximum value of 64, and path links are calculated by summing link values. Maximum metric values were set at these levels to provide the granularity to support various link types while at the same time ensuring that the shortest-path algorithm used for route computation is reasonably efficient. Three optional IS-IS metrics (costs)—delay, expense, and error—are not supported by the ONS 15600 SDH. IS-IS maintains a mapping of the metrics to the quality of service (QoS) option in the CLNP packet header. IS-IS uses the mappings to compute routes through the internetwork.

# 9.6.5 TARP

TARP is used when TL1 target identifiers (TIDs) must be translated to NSAP addresses. The TID-to-NSAP translation occurs by mapping TIDs to the NETs, then deriving NSAPs from the NETs by using the NSAP selector values (Table 9-8 on page 9-28).

TARP uses a selective PDU propagation methodology in conjunction with a distributed database (that resides within the NEs) of TID-to-NET mappings. TARP allows NEs to translate between TID and NET by automatically exchanging mapping information with other NEs. The TARP PDU is carried by the standard CLNP Data PDU. TARP PDU fields are shown in Table 9-9.

*Table 9-9*     *TARP PDU Fields*

| Field | Abbreviation | Size (bytes) | Description |
|---|---|---|---|
| TARP Lifetime | tar-lif | 2 | The TARP time-to-live in hops. |
| TARP Sequence Number | tar-seq | 2 | The TARP sequence number used for loop detection. |
| Protocol Address Type | tar-pro | 1 | Used to identify the type of protocol address that the TID must be mapped to. The value FE is used to identify the CLNP address type. |
| TARP Type Code | tar-tcd | 1 | The TARP Type Code identifies the TARP type of PDU. Five TARP types, shown in Table 9-10, are defined. |
| TID Target Length | tar-tln | 1 | The number of octets that are in the tar-ttg field. |

*Table 9-9*      *TARP PDU Fields (continued)*

| Field | Abbreviation | Size (bytes) | Description |
|---|---|---|---|
| TID Originator Length | tar-oln | 1 | The number of octets that are in the tar-tor field. |
| Protocol Address Length | tar-pln | 1 | The number of octets that are in the tar-por field. |
| TID of Target | tar-ttg | $n = 0, 1, 2...$ | TID value for the target NE. |
| TID of Originator | tar-tor | $n = 0, 1, 2...$ | TID value of the TARP PDU originator. |
| Protocol Address of Originator | tar-por | $n = 0, 1, 2...$ | Protocol address (for the protocol type identified in the tar-pro field) of the TARP PDU originator. When the tar-pro field is set to FE (hex), tar-por will contain a CLNP address (that is, the NET). |

Table 9-10 shows the TARP PDUs types that govern TARP interaction and routing.

*Table 9-10*      *TARP PDU Types*

| Type | Description | Procedure |
|---|---|---|
| 1 | Sent when a device has a TID for which it has no matching NSAP. | After an NE originates a TARP Type 1 PDU, the PDU is sent to all adjacencies within the NE's routing area. |
| 2 | Sent when a device has a TID for which it has no matching NSAP and no response was received from the Type 1 PDU. | After an NE originates a TARP Type 2 PDU, the PDU is sent to all Level 1 and Level 2 neighbors. |
| 3 | Sent as a response to Type 1, Type 2, or Type 5 PDUs. | After a TARP Request (Type 1 or 2) PDU is received, a TARP Type 3 PDU is sent to the request originator. Type 3 PDUs do not use the TARP propagation procedures. |
| 4 | Sent as a notification when a change occurs locally, for example, a TID or NSAP change. It might also be sent when an NE initializes. | A Type 4 PDU is a notification of a TID or Protocol Address change at the NE that originates the notification. The PDU is sent to all adjacencies inside and outside the NE's routing area. |
| 5 | Sent when a device needs a TID that corresponds to a specific NSAP. | When a Type 5 PDU is sent, the CLNP destination address is known, so the PDU is sent to only that address. Type 5 PDUs do not use the TARP propagation procedures. |

## 9.6.5.1 TARP Processing

A TARP data cache (TDC) is created at each NE to facilitate TARP processing. In CTC, the TDC is displayed and managed on the node view Maintenance > OSI > TDC tab. This tab contains the following TARP PDU fields:

- TID—TID of the originating NE (tar-tor).
- NSAP—NSAP of the originating NE.

- Type— Indicates whether the TARP PDU was created through the TARP propagation process (dynamic) or manually created (static).

Provisionable timers, shown in Table 9-11, control TARP processing.

*Table 9-11     TARP Timers*

| Timer | Description | Default (seconds) | Range (seconds) |
|---|---|---|---|
| T1 | Waiting for response to TARP Type 1 Request PDU | 15 | 0–3600 |
| T2 | Waiting for response to TARP Type 2 Request PDU | 25 | 0–3600 |
| T3 | Waiting for response to address resolution request | 40 | 0–3600 |
| T4 | Timer starts when T2 expires (used during error recovery) | 20 | 0–3600 |

Table 9-12 shows the main TARP processes and the general sequence of events that occurs in each process.

*Table 9-12     TARP Processing Flow*

| Process | General TARP Flow |
|---|---|
| Find a NET that matches a TID | 1. TARP checks its TDC for a match. If a match is found, TARP returns the result to the requesting application.<br>2. If no match is found, a TARP Type 1 PDU is generated and Timer T1 is started.<br>3. If Timer T1 expires before a match if found, a Type 2 PDU is generated and Timer T2 is started.<br>4. If Timer T2 expires before a match is found, Timer T4 is started.<br>5. If Timer T4 expires before a match is found, a Type 2 PDU is generated and Timer T2 is started. |
| Find a TID that matches a NET | A Type 5 PDU is generated. Timer T3 is used. However, if the timer expires, no error recovery procedure occurs, and a status message is provided to indicate that the TID cannot be found. |
| Send a notification of TID or protocol address change | TARP generates a Type 4 PDU in which the tar-ttg field contains the NE's TID value that existed prior to the change of TID or protocol address. Confirmation that other NEs successfully received the address change is not sent. |

## 9.6.5.2  TARP Loop Detection Buffer

The TARP loop detection buffer (LDB) can be enabled to prevent duplicate TARP PDUs from entering the TDC. When a TARP Type 1, 2, or 4 PDU arrives, TARP checks its LDB for a NET address (tar-por) of the PDU originator match. If no match is found, TARP processes the PDU and assigns a tar-por, tar-seq (sequence) entry for the PDU to the LDB. If the tar-seq is zero, a timer associated with the LDB entry is started using the provisionable LDB entry timer on the node view OSI > TARP > Config tab. If a match exists, the tar-seq is compared to the LDB entry. If the tar-seq is not zero and is less than or equal to the LDB entry, the PDU is discarded. If the tar-seq is greater than the LDB entry, the PDU is processed and the tar-seq field in the LDB entry is updated with the new value. The ONS 15600 SDH LDB holds approximately 500 entries. The LDB is flushed periodically based on the time set in the LDB Flush timer on the node view OSI > TARP > Config tab.

### 9.6.5.3 Manual TARP Adjacencies

TARP adjacencies can be manually provisioned in networks where ONS 15600 SDHs must communicate across routers or non-SDH NEs that lack TARP capability. In CTC, manual TARP adjacencies are provisioned on the node view Provisioning > OSI > TARP > MAT (Manual Area Table) tab. The manual adjacency causes a TARP request to hop through the general router or non-SDH NE, as shown in Figure 9-22.

*Figure 9-22    Manual TARP Adjacencies*
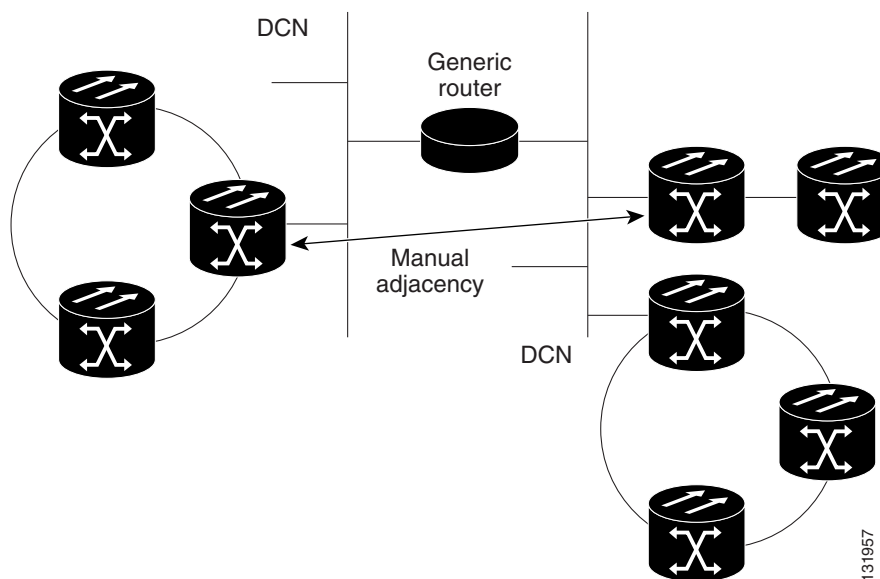


### 9.6.5.4 Manual TID to NSAP Provisioning

TIDs can be manually linked to NSAPs and added to the TDC. Static TDC entries are similar to static routes. For a specific TID, you force a specific NSAP. Resolution requests for that TID always return that NSAP. No TARP network propagation or instantaneous replies are involved. Static entries allow you to forward TL1 commands to NEs that do not support TARP. However, static TDC entries are not dynamically updated, so outdated entries are not removed after the TID or the NSAP changes on the target node.

## 9.6.6 TCP/IP and OSI Mediation

Two mediation processes facilitate TL1 networking and file transfers between NEs and ONS client computers running TCP/IP and OSI protocol suites:

- T–TD—Performs a TL1-over-IP to TL1-over-OSI gateway mediation to enable an IP-based OSS to manage OSI-only NEs subtended from a GNE. Figure 9-23 shows the T–TD protocol flow.

*Figure 9-23 T–TD Protocol Flow*
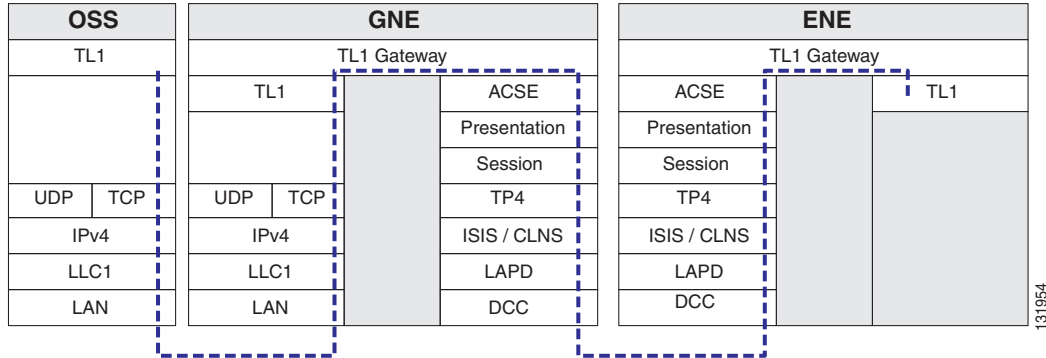


- FT–TD—Performs an FTP conversion between FTAM and FTP. The FT–TD gateway entity includes an FTAM responder (server) and an FTP client, allowing FTAM initiators (clients) to store, retrieve, or delete files from an FTP server. The FT–TD gateway is unidirectional and is driven by the FTAM initiator. The FT–TD FTAM responder exchanges messages with the FTAM initiator over the full OSI stack. Figure 9-24 shows the FT–TD protocol flow.

*Figure 9-24 FT–TD Protocol Flow*
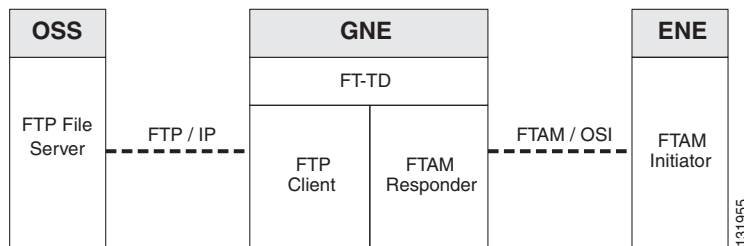


The ONS 15600 SDH uses FT–TD for the following file transfer processes:

- Software downloads
- Database backups and restores

## 9.6.7 OSI Virtual Routers

The ONS 15600 SDH supports twelve OSI virtual routers. The routers are provisioned on the Provisioning > OSI > Routers tab. Each router has an editable manual area address and a unique NSAP System ID that is set to the node MAC address + $n$. For Router 1, $n = 0$. For Router 2, $n = 1$. For Router 3, $n = 2$, and for Router 12, $n = 11$. Each router can be enabled and connected to different OSI routing areas. However, Router 1 is the primary router, and it must be enabled before Routers 2 through 12 can be enabled. The Router 1 manual area address and System ID create the NSAP address assigned to the node's TID. In addition, Router 1 supports OSI TARP, mediation, and tunneling functions that are not supported by Routers 2 through 12. These include:

- TID-to-NSAP resolution
- TARP data cache
- IP-over-CLNS tunnels
- FTAM

- FT-TD
- T-TD
- LAN subnet

OSI virtual router constraints depend on the routing mode provisioned for the node. Table 9-13 shows the number of IS L1s, IS L1/L2s, and DCCs that are supported by each router. An IS L1 and IS L1/L2 support one ES per DCC subnet and up to 100 ESs per LAN subnet.

*Table 9-13        OSI Virtual Router Constraints*

| Routing Mode | Router 1 | Routers 2–12 | IS L1 per Area | IS L1/L2 per Area | DCC per IS |
|---|---|---|---|---|---|
| IS L1 | Yes | Yes | 250 | — | 60 |
| IS L1/L2 | Yes | Yes | 250 | 50 | 60 |

Each OSI virtual router has a primary manual area address. You can also create two additional manual area addresses. These manual area addresses can be used to:

- Split up an area—Nodes within a given area can accumulate to a point that they are difficult to manage, cause excessive traffic, or threaten to exceed the usable address space for an area. Additional manual area addresses can be assigned so that you can smoothly partition a network into separate areas without disrupting service.

- Merge areas—Use transitional area addresses to merge as many as three separate areas into a single area that shares a common area address.

- Change to a different address—You might need to change an area address for a particular group of nodes. Use multiple manual area addresses to allow incoming traffic intended for an old area address to continue being routed to associated nodes.

# 9.6.8  IP-over-CLNS Tunnels

IP-over-CLNS tunnels are used to encapsulate IP for transport across OSI NEs. The ONS 15600 SDH supports two tunnel types:

- GRE—Generic Routing Encapsulation is a tunneling protocol that encapsulates one network layer for transport across another. GRE tunnels add both a CLNS header and a GRE header to the tunnel frames. GRE tunnels are supported by Cisco routers and some other vendor NEs.

- Cisco IP—The Cisco IP tunnel directly encapsulates the IP packet with no intermediate header. Cisco IP is supported by most Cisco routers.

Figure 9-25 shows the protocol flow when an IP-over-CLNS tunnel is created through four NEs (A, B, C, and D). The tunnel ends are configured on NEs A and D, which support both IP and OSI. NEs B and C only support OSI, so they only route the OSI packets.

*Figure 9-25* **IP-over-CLNS Tunnel Flow**
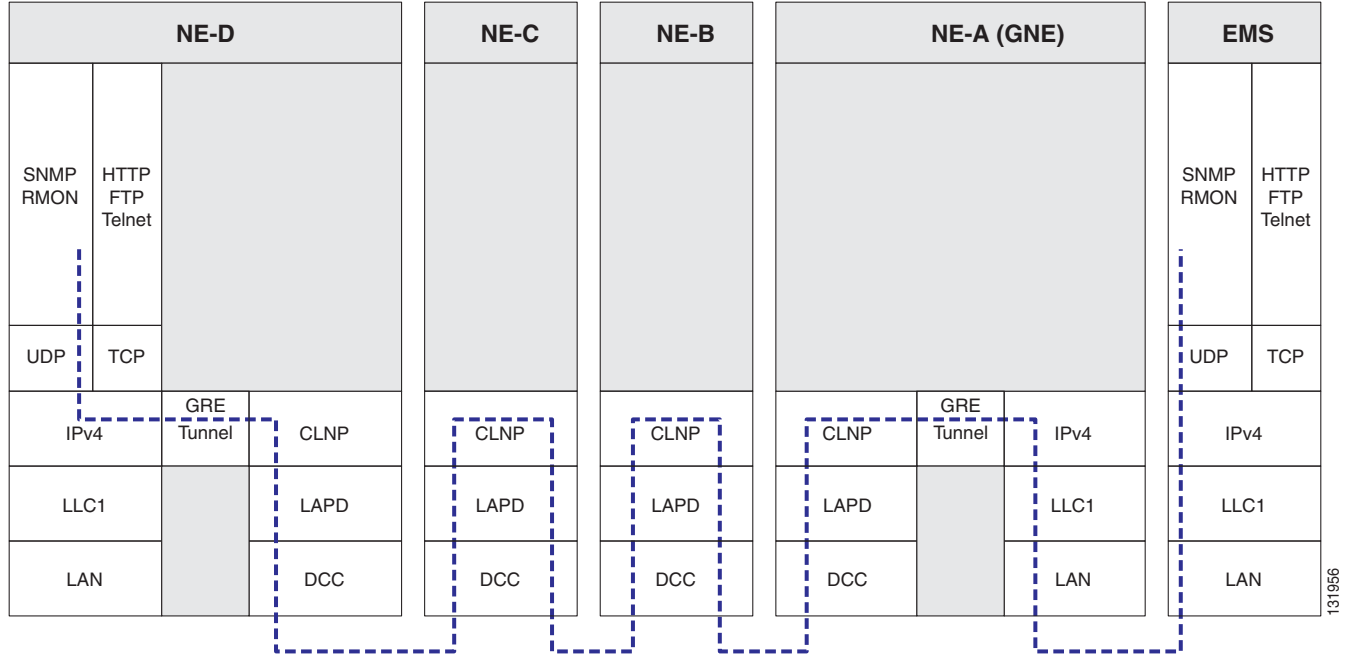


## 9.6.8.1 Provisioning IP-over-CLNS Tunnels

IP-over-CLNS tunnels must be carefully planned to prevent nodes from losing visibility or connectivity. Before you begin a tunnel, verify that the tunnel type, either Cisco IP or GRE, is supported by the equipment at the other end. Always verify IP and NSAP addresses. Provisioning of IP-over-CLNS tunnels in CTC is performed on the node view Provisioning > OSI > IP over CLNS Tunnels tab. For procedures, refer to the "Turn Up a Node" chapter in the *ONS 15600 SDH Procedurs Guide*.

Provisioning IP-over-CLNS tunnels on Cisco routers requires the following prerequisite tasks, as well as other OSI provisioning:

- (Required) Enable IS-IS.
- (Optional) Enable routing for an area on an interface.
- (Optional) Assign multiple area addresses.
- (Optional) Configure IS-IS interface parameters.
- (Optional) Configure miscellaneous IS-IS parameters.

The Cisco IOS commands used to create IP-over-CLNS tunnels (CTunnels) are shown in Table 9-14.

*Table 9-14    IP Over CLNS Tunnel IOS Commands*

| Step | Step | Purpose |
|------|------|---------|
| 1 | Router (config) # **interface ctunnel** *interface-number* | Creates a virtual interface to transport IP over a CLNS tunnel and enters interface configuration mode. The interface number must be unique for each CTunnel interface. |
| 2 | Router (config-if # **ctunnel destination** *remote-nsap-address* | Configures the destination parameter for the CTunnel. Specifies the destination NSAP1 address of the CTunnel, where the IP packets are extracted. |
| 3 | Router (config-if) # **ip address** *ip-address mask* | Sets the primary or secondary IP address for an interface. |

If you are provisioning an IP-over-CLNS tunnel on a Cisco router, always follow procedures provided in the Cisco IOS documentation for the router you are provisioning. For information about ISO CLNS provisioning including IP-over-CLNS tunnels, see the "Configuring ISO CLNS" chapter in the *Cisco IOS Apollo Domain, Banyon VINES, DECnet, ISO CLNS, and XNS Configuration Guide*.

## 9.6.8.2  IP-Over-CLNS Tunnel Scenario 1: ONS Node to Other Vendor GNE

Figure 9-26 shows an IP-over-CLNS tunnel created from an ONS node to another vendor GNE. The other vendor NE has an IP connection to an IP DCN to which a CTC computer is attached. An OSI-only (LAP-D) RS-DCC and a GRE tunnel are created between the ONS NE 1 to the other vender GNE.

IP-over-CLNS tunnel on the ONS NE 1:

- Destination: 10.10.10.100 (CTC 1)
- Mask: 255.255.255.255 for host route (CTC 1 only), or 255.255.255.0 for subnet route (all CTC computers residing on the 10.10.10.0 subnet)
- NSAP: 39.840F.80.1111.0000.1111.1111.cccccccccccc.00 (other vendor GNE)
- Metric: 110
- Tunnel Type: GRE

IP-over-CLNS tunnel on the other vender GNE:

- Destination: 10.20.30.30 (ONS NE 1)
- Mask: 255.255.255.255 for host route (ONS NE 1 only), or 255.255.255.0 for subnet route (all ONS nodes residing on the 10.30.30.0 subnet)
- NSAP: 39.840F.80.1111.0000.1111.1111.dddddddddddd.00 (ONS NE 1)
- Metric: 110
- Tunnel Type: GRE

*Figure 9-26*        *IP Over CLNS Tunnel Scenario 1: ONS NE to Other Vender GNE*



CTC 1
10.10.10.100/24

IP
DCN

Router 2
Interface 0/0: 10.10.10.10/24
Interface 0/1: 10.10.20.10/24
39.840F.80.111111.0000.1111.1111.aaaaaaaaaaaa.00

Router 1
Interface 0/0: 10.10.20.20/24
Interface 0/1: 10.10.30.10/24
39.840F.80. 111111.0000.1111.1111.bbbbbbbbbbbb.00

IP/OSI

Vendor GNE
10.10.30.20/24
39.840F.80. 111111.0000.1111.1111.cccccccccccc.00

GRE tunnel

OSI

OSI-only
DCC (LAPD)

OSI

Other vendor
NE

ONS NE 1
10.10.30.30/24
39.840F.80. 111111.0000.1111.1111.dddddddddddd.00

134355

## 9.6.8.3  IP-Over-CLNS Tunnel Scenario 2: ONS Node to Router

Figure 9-27 shows an IP-over-CLNS tunnel from an ONS node to a router. The other vendor NE has an OSI connection to a router on an IP DCN, to which a CTC computer is attached. An OSI-only (LAP-D) RS-DCC is created between the ONS NE 1 and the other vender GNE. The OSI-over-IP tunnel can be either the Cisco IP tunnel or a GRE tunnel, depending on the tunnel types supported by the router.

IP-over-CLNS tunnel on ONS NE 1:

- Destination: 10.10.30.10 (Router 1, Interface 0/1)
- Mask: 255.255.255.255 for host route (Router 1 only), or 255.255.255.0 for subnet route (all routers on the same subnet)
- NSAP: 39.840F.80.1111.0000.1111.1111.bbbbbbbbbbbb.00 (Router 1)
- Metric: 110
- Tunnel Type: Cisco IP

CTunnel (IP-over-CLNS) on Router 1:

    ip routing

    clns routing

    interface ctunnel 102

        ip address 10.10.30.30 255.255.255.0

        ctunnel destination 39.840F.80.1111.0000.1111.1111.dddddddddddd.00

    interface Ethernet0/1

        clns router isis

    router isis

        net 39.840F.80.1111.0000.1111.1111.bbbbbbbbbbbb.00

*Figure 9-27     IP-Over-CLNS Tunnel Scenario 2: ONS Node to Router*



CTC 1
10.10.10.100/24

IP
DCN

Router 2
Interface 0/0: 10.10.10.10/24
Interface 0/1: 10.10.20.10/24
39.840F.80.111111.0000.1111.1111.aaaaaaaaaaaa.00

Router 1
Interface 0/0: 10.10.20.20/24
Interface 0/1: 10.10.30.10/24
39.840F.80. 111111.0000.1111.1111.bbbbbbbbbbbb.00

OSI

Other vendor
GNE

GRE or
Cisco IP tunnel

OSI

OSI-only
DCC (LAPD)

OSI

Other vendor
NE

ONS NE 1
10.10.30.30/24
39.840F.80. 111111.0000.1111.1111.dddddddddddd.00
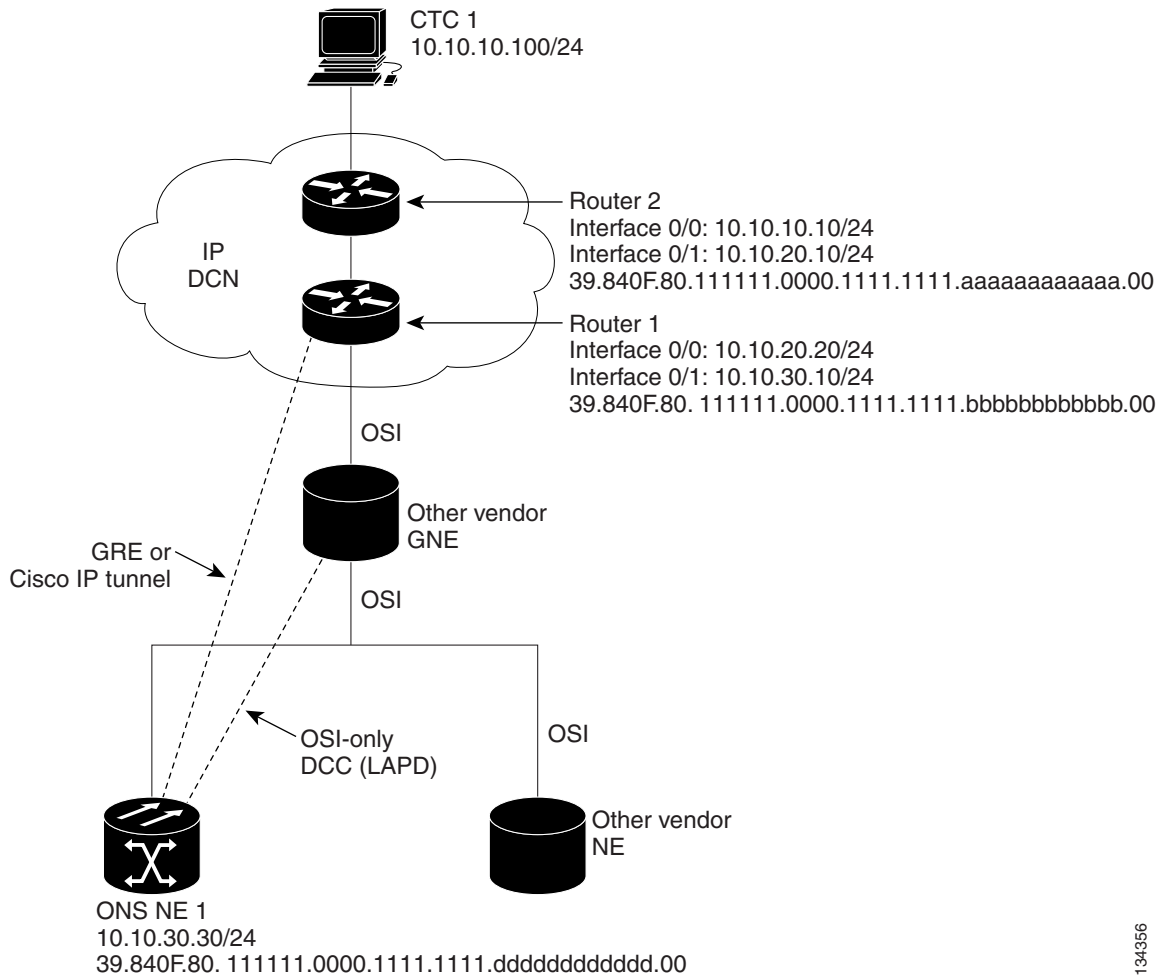
134356

## 9.6.8.4 IP-Over-CLNS Tunnel Scenario 3: ONS Node to Router Across an OSI DCN

Figure 9-28 shows an IP-over-CLNS tunnel from an ONS node to a router across an OSI DCN. The other vendor NE has an OSI connection to an IP DCN to which a CTC computer is attached. An OSI-only (LAP-D) RS-DCC is created between the ONS NE 1 and the other vender GNE. The OSI-over-IP tunnel can be either the Cisco IP tunnel or a GRE tunnel, depending on the tunnel types supported by the router.

IP-over-CLNS tunnel on ONS NE 1:

- Destination: Router 2 IP address
- Mask: 255.255.255.255 for host route (CTC 1 only), or 255.255.255.0 for subnet route (all CTC computers on the same subnet)
- NSAP: Other vender GNE NSAP address
- Metric: 110
- Tunnel Type: Cisco IP

IP over OSI tunnel on Router 2 (sample Cisco IOS provisioning):

```
ip routing
clns routing
interface ctunnel 102
    ip address 10.10.30.30 255.255.255.0
    ctunnel destination 39.840F.80.1111.0000.1111.1111.dddddddddddd.00
interface Ethernet0/1
    clns router isis
router isis
    net 39.840F.80.1111.0000.1111.1111.aaaaaaaaaaaa.00
```

*Figure 9-28*      *IP-Over-CLNS Tunnel Scenario 3: ONS Node to Router Across an OSI DCN*
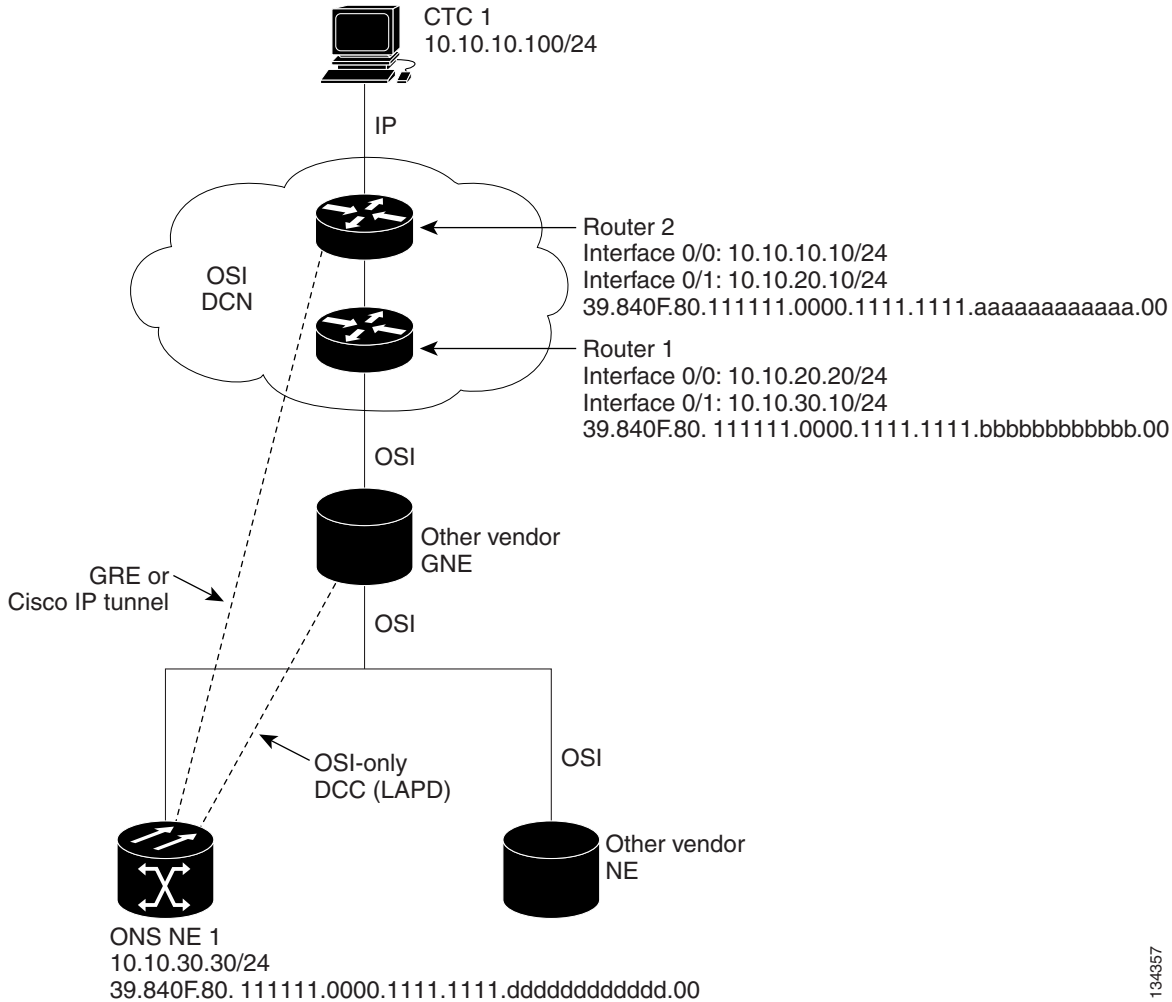


## 9.6.9  OSI/IP Networking Scenarios

The following eight scenarios show examples of ONS 15600 SDHs in networks with OSI-based NEs. The scenarios show ONS 15600 SDHs in a variety of roles. The scenarios assume the following:

- ONS 15600 SDH NEs are configured as dual OSI and IP nodes with both IP and NSAP addresses. They run both OSPF and OSI (IS-IS or ES-IS) routing protocols as "Ships-In-The-Night," with no route redistribution.

- ONS 15600 SDH NEs run TARP, which allows them to resolve a TL1 TID to a NSAP address. A TID might resolve to both an IP and an NSAP address when the destination TID is an ONS 15600 SDH NE that has both IP and NSAP address.

- DCC links between ONS 15600 SDH NEs and OSI-only NEs run the full OSI stack over LAP-D, which includes IS-IS, ES-IS, and TARP.

- DCC links between ONS 15600 SDH NEs run the full OSI stack and IP (OSPF) over PPP.

- All ONS 15600 SDH NEs participating in an OSI network run OSI over PPP between themselves. This is needed so that other vendor GNEs can route TL1 commands to all ONS 15600 SDH NEs participating in the OSI network.

### 9.6.9.1 OSI/IP Scenario 1: IP OSS, IP DCN, ONS GNE, IP DCC, and ONS ENE

Figure 9-29 shows OSI/IP Scenario 1, the current ONS 15600 SDH IP-based implementation, with an IP DCN, IP-over-PPP DCC, and OSPF routing.

*Figure 9-29    OSI/IP Scenario 1: IP OSS, IP DCN, ONS GNE, IP DCC, and ONS ENE*
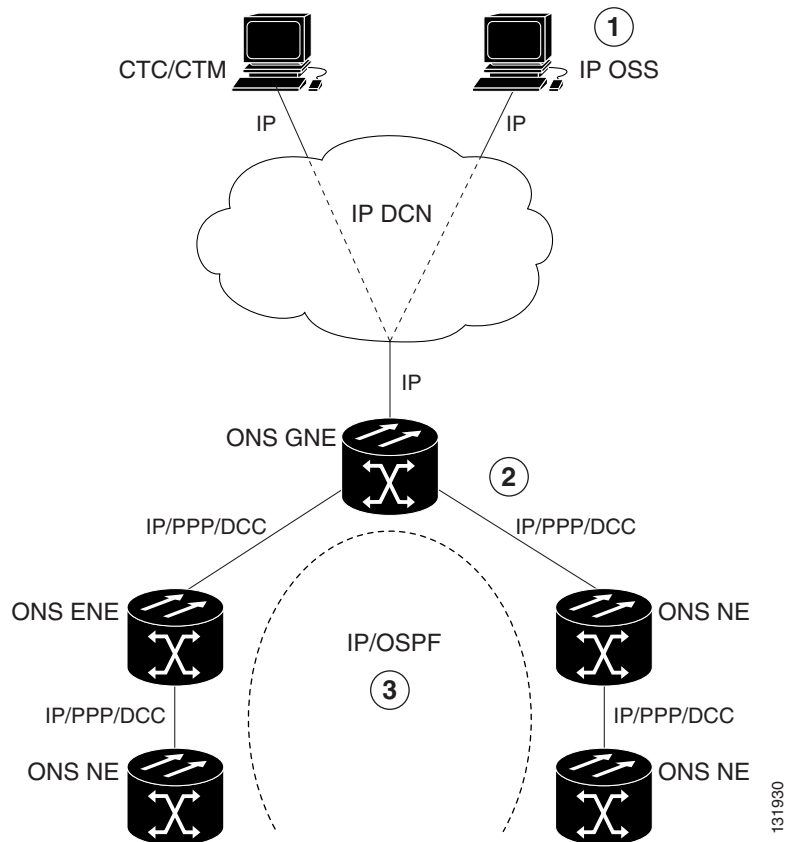


| 1 | IP OSS manages ONS 15600 SDH using TL1 and FTP. |
|---|---|
| 2 | DCCs carry IP over the PPP protocol. |
| 3 | The ONS 15600 SDH network is managed by IP over OSPF. |

### 9.6.9.2 OSI/IP Scenario 2: IP OSS, IP DCN, ONS GNE, OSI DCC, and Other Vendor ENE

OSI/IP Scenario 2 (Figure 9-30) shows an ONS 15600 SDH GNE in a multivendor OSI network. Both the ONS 15600 SDH GNE and the other vendor NEs are managed by an IP OSS using TL1 and FTP. The ONS 15600 SDH is also managed by CTC and Cisco Transport Manager (CTM). Because the other vendor NE only supports TL1 and FTAM over the full OSI stack, the ONS 15600 SDH GNE provides T–TD and FT–TD mediation to convert TL1/IP to TL1/OSI and FTAM/OSI to FTP/IP.

*Figure 9-30* *OSI/IP Scenario 2: IP OSS, IP DCN, ONS GNE, OSI DCC, and Other Vendor ENE*
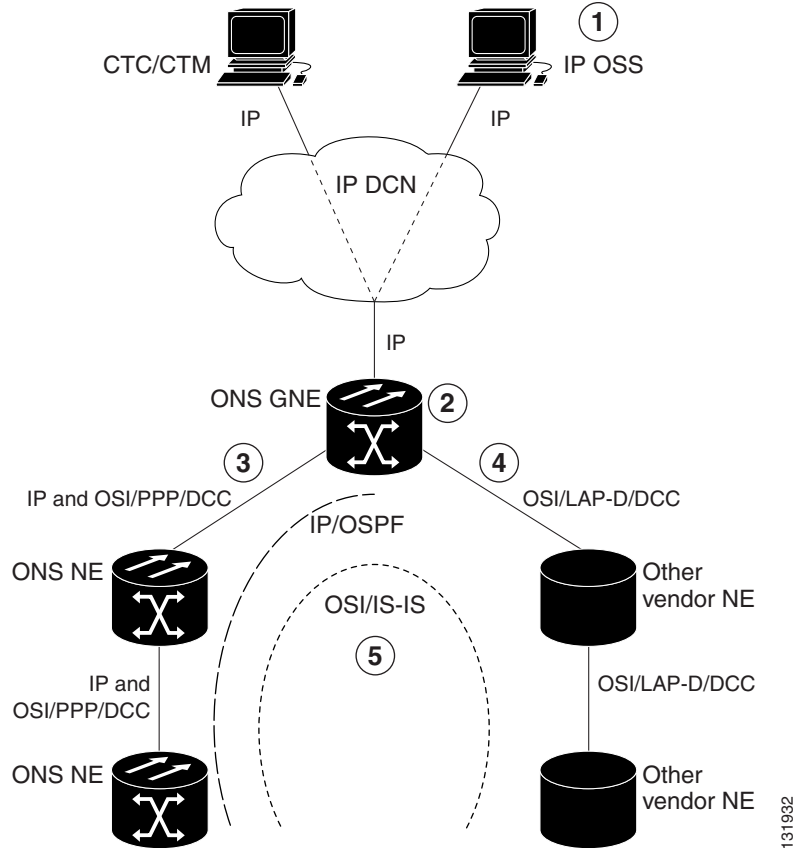


| 1 | The IP OSS manages ONS 15600 SDH and other vendor NEs using TL1 and FTP. |
|---|---|
| 2 | The ONS 15600 SDH GNE performs mediation for other vendor NEs. |
| 3 | DCCs between the ONS 15600 SDH GNE and ONS 15600 SDH NEs are provisioned for IP and OSI over PPP. |
| 4 | DCCs between the ONS 15600 SDH GNE and other vendor NEs are provisioned for OSI over LAP-D. |
| 5 | The ONS 15600 SDH and the other vendor NE network include IP over OSPF and OSI over the IS-IS protocol. |

The ONS 15600 SDH GNE routes TL1 traffic to the correct NE by resolving the TL1 TID to either an IP or NSAP address. For TL1 traffic to other vendor NEs (OSI-only nodes), the TID is resolved to an NSAP address. The ONS 15600 SDH GNE passes the TL1 to the mediation function, which encapsulates it over the full OSI stack and routes it to the destination using the IS-IS protocol.

For TL1 traffic to ONS 15600 SDH NEs, the TID is resolved to both an IP and an NSAP address. The ONS 15600 SDH GNE follows the current TL1 processing model and forwards the request to the destination NE using the TCP/IP stack and OSPF routing.

OSS-initiated software downloads consist of two parts: the OSS to destination NE TL1 download request and the file transfer. The TL1 request is handled the same as described earlier. The ONS 15600 SDH NEs use FTP for file transfers. OSI-only NEs use FTAM to perform file transfers. The FTAM protocol is carried over OSI between the OSI NE and the ONS 15600 SDH GNE. The GNE mediation translates between FTAM to FTP.

## 9.6.9.3  OSI/IP Scenario 3: IP OSS, IP DCN, Other Vendor GNE, OSI DCC, and ONS ENE

In OSI/IP Scenario 3 (Figure 9-31), all TL1 traffic between the OSS and GNE is exchanged over the IP DCN. TL1 traffic targeted for the GNE is processed locally. All other TL1 traffic is forwarded to the OSI stack, which performs IP-to-OSI TL1 translation. The TL1 is encapsulated in the full OSI stack and sent to the target NE over the DCC. The GNE can route to any node within the IS-IS domain because all NEs, ONS 15600 SDH and non-ONS 15600 SDH, have NSAP addresses and support IS-IS routing.

TL1 traffic received by an ONS 15600 SDH NE and not addressed to its NSAP address is forwarded by IS-IS routing to the correct destination. TL1 traffic received by an ONS 15600 SDH NE and addressed to its NSAP is sent up the OSI stack to the mediation function, which extracts the TL1 and passes it to the ONS 15600 SDH TL1 processor.

An OSS initiated software download includes the OSS to destination node TL1 download request and the file transfer. The TL1 request is handled as described earlier. The target node uses FTAM for file transfers because the GNE does not support IP on the DCC and cannot forward FTP. The ONS 15600 SDH NEs therefore must support an FTAM client and initiate file transfer using FTAM when subtended to an OSI GNE.

In this scenario, the GNE has both IP and OSI DCN connections. The GNE only supports TL1 and FTP over IP. Both are translated and then carried over OSI to the destination ENE (ONS 15600 SDH or OSI-only NE). All other IP traffic is discarded by the GNE. The CTC/CTM IP traffic is carried over an IP-over-OSI tunnel to an ONS 15600 SDH NE. The tunnel is created between an external router and an ONS 15600 SDH NE. The traffic is sent to the ONS 15600 SDH terminating the tunnel. That ONS 15600 SDH then forwards the traffic over the tunnel to CTC/CTM by way of the external router.

***Figure 9-31*** *OSI/IP Scenario 3: IP OSS, IP DCN, Other Vendor GNE, OSI DCC, and ONS ENE*
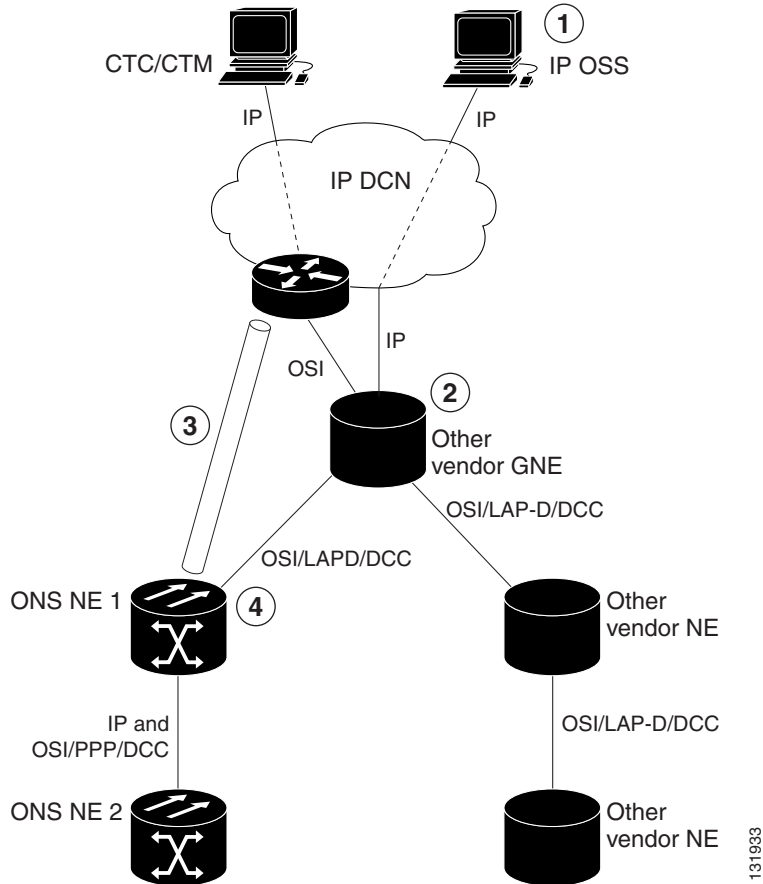


| | |
|---|---|
| **1** | The IP OSS manages the ONS 15600 SDH and other vendor NEs using TL1 and FTP. |
| **2** | The other vendor GNE performs mediation for TL1 and FTP, so the DCCs to the ONS 15600 SDH and other vendor NEs are OSI-only. |
| **3** | CTC/CTM communicates with ONS 15600 SDH NEs over a IP-over-CLNS tunnel. The tunnel is created from the ONS 15600 SDH node to the external router. |
| **4** | The ONS 15600 SDH NE exchanges TL1 over the full OSI stack using FTAM for file transfer. |

Figure 9-32 shows the same scenario, except the IP-over-CLNS tunnel endpoint is the GNE and not the DCN router.

*Figure 9-32 OSI/IP Scenario 3 with OSI/IP-over-CLNS Tunnel Endpoint at the GNE*
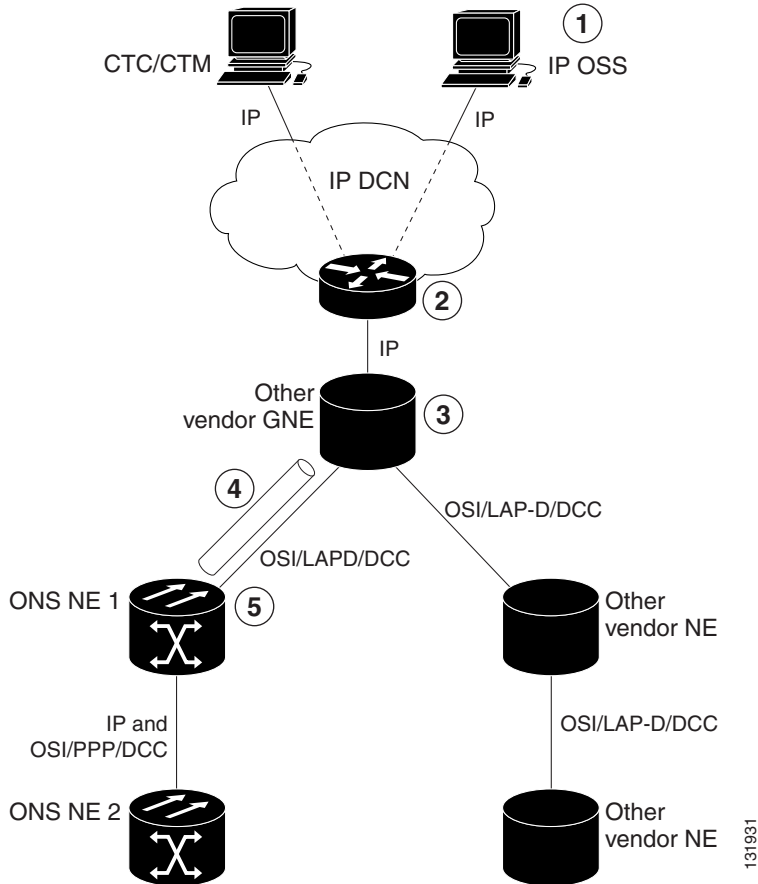


| 1 | The IP OSS manages ONS and other vendor NEs using TL1 and FTP. |
|---|---|
| 2 | The router routes requests to the other vender GNE. |
| 3 | The other vendor GNE performs mediation for TL1 and FTP, so the DCCs to ONS 15600 SDH and other vendor NEs are OSI-only. |
| 4 | CTC/CTM communicates with ONS 15600 SDH NEs over an IP-over-CLNS tunnel between the ONS 15600 SDH and the GNE. |
| 5 | ONS 15600 SDH NEs exchange TL1 over the full OSI stack. FTAM is used for file transfer. |

## 9.6.9.4 OSI/IP Scenario 4: Multiple ONS DCC Areas

OSI/IP Scenario 4 (Figure 9-33) is similar to OSI/IP Scenario 3 except that the OSI GNE is subtended by multiple isolated ONS 15600 SDH areas. A separate IP-over-CLNS tunnel is required to each isolated ONS 15600 SDH OSPF area. An alternate approach is to create a single IP-over-CLNS tunnel from CTC/CTM to an ONS 15600 SDH NE, and then to configure a tunnel from that NE to an NE in each isolated OSPF area. This approach requires additional static routes.

*Figure 9-33      OSI/IP Scenario 4: Multiple ONS DCC Areas*
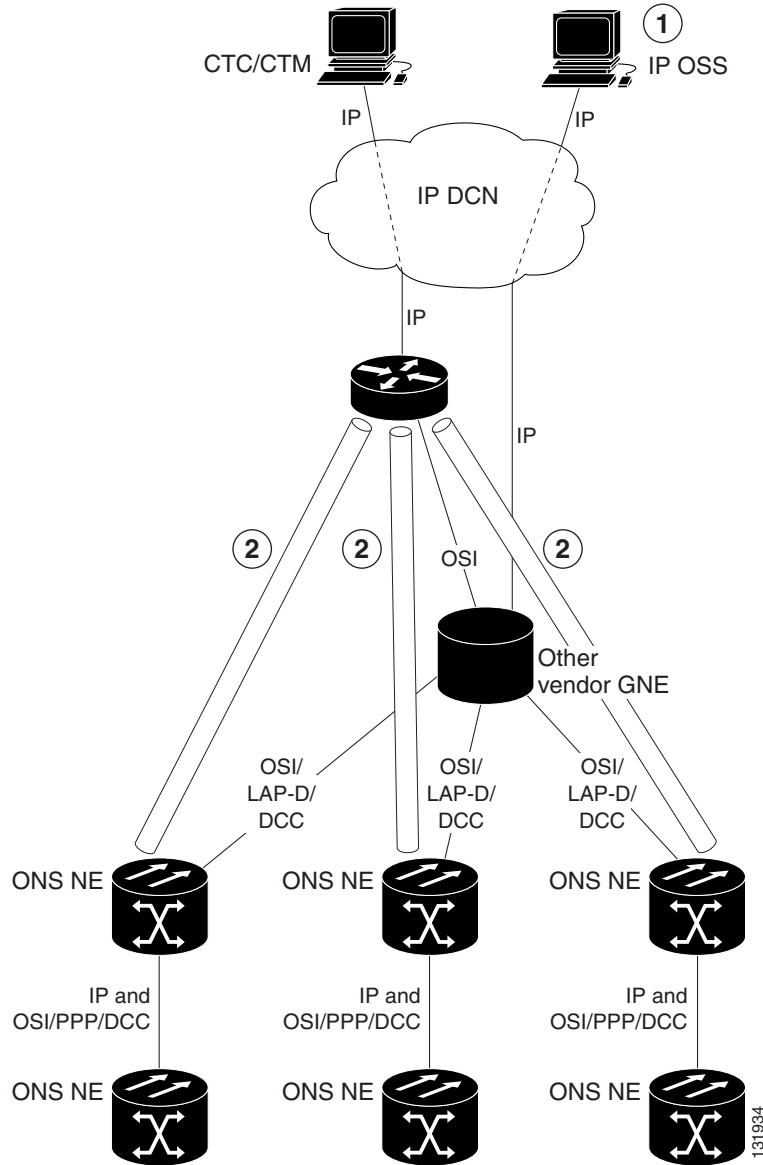


| **1** | The IP OSS manages ONS 15600 SDH and other vendor NEs using TL1 and FTP. |
|---|---|
| **2** | A separate tunnel is created for each isolated ONS 15600 SDH DCC area. |

## 9.6.9.5  OSI/IP Scenario 5: GNE Without an OSI DCC Connection

OSI/IP Scenario 5 (Figure 9-34) is similar to OSI/IP Scenario 3 except that the OSI GNE only has an IP connection to the DCN. It does not have an OSI DCN connection to carry CTC/CTM IP traffic through an IP-over-OSI tunnel. A separate DCN to ONS 15600 SDH NE connection is created to provide CTC/CTM access.

*Figure 9-34      OSI/IP Scenario 5: GNE Without an OSI DCC Connection*
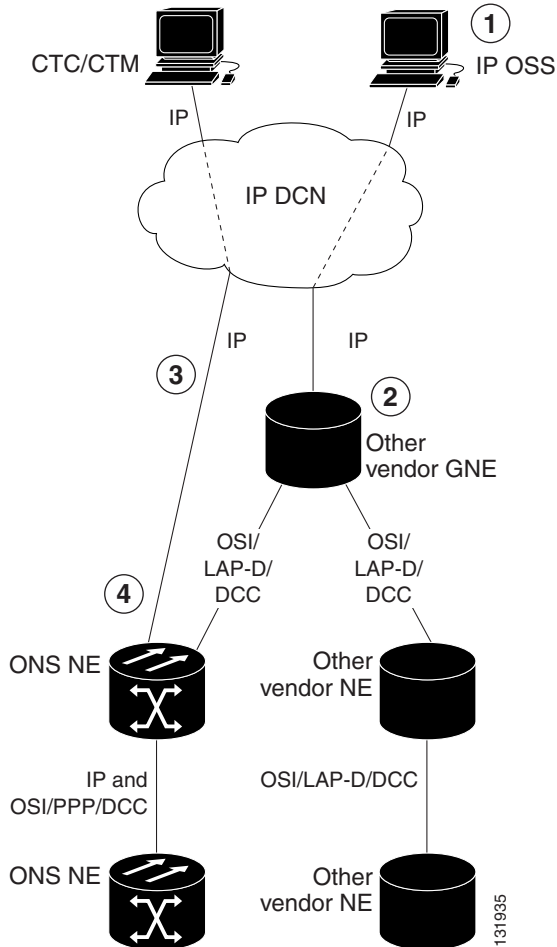


| 1 | The IP OSS manages ONS 15600 SDH and other vendor NEs using TL1 and FTP. |
|---|---|
| 2 | The other vendor GNE performs mediation on TL1 and FTP, so DCCs are OSI-only. |
| 3 | CTC/CTM communicates with ONS 15600 SDH NEs over a separate IP DCN connection. |
| 4 | ONS 15600 SDH NE exchanges TL1 over the full OSI stack. FTAM is used for file transfers. |

## 9.6.9.6  OSI/IP Scenario 6: IP OSS, OSI DCN, ONS GNE, OSI DCC, and Other Vendor ENE

OSI/IP Scenario 6 (Figure 9-35) shows how the ONS 15600 SDH supports OSI DCNs. The OSI DCN has no impact on the ONS 15600 SDH because all IP traffic (CTC/CTM, FTP, and TL1) is tunneled through the OSI DCN.

*Figure 9-35    OSI/IP Scenario 6: IP OSS, OSI DCN, ONS GNE, OSI DCC, and Other Vendor ENE*
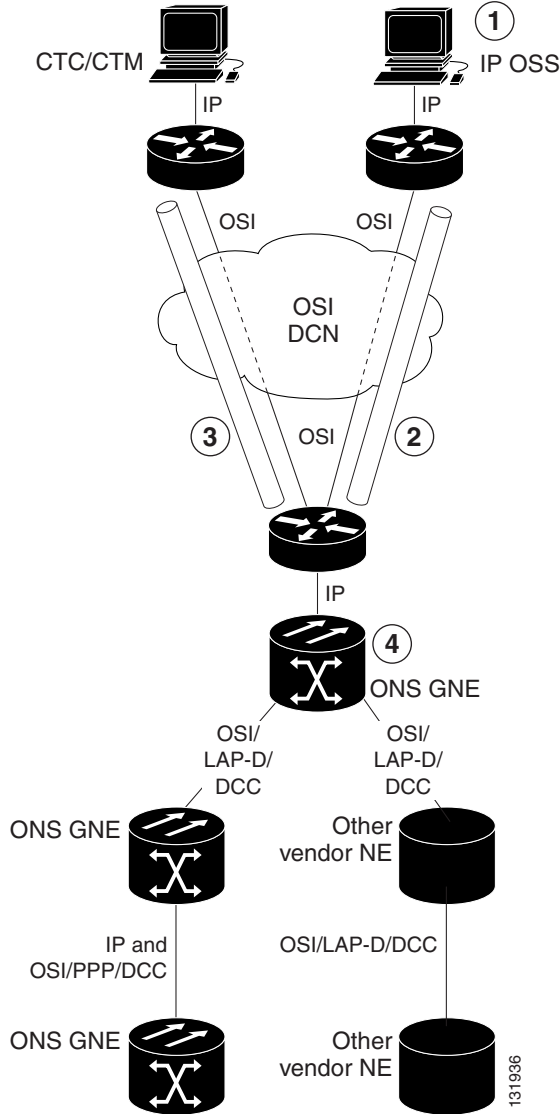


| 1 | The IP OSS manages ONS 15600 SDH and other vendor NEs using TL1 and FTP. |
|---|---|
| 2 | OSS IP traffic is tunneled through the DCN to the ONS 15600 SDH GNE. |
| 3 | CTC/CTM IP traffic is tunneled through the DCN to the ONS 15600 SDH GNE. |
| 4 | The GNE performs mediation for other vendor NEs. |

## 9.6.9.7  OSI/IP Scenario 7: OSI OSS, OSI DCN, Other Vender GNE, OSI DCC, and ONS NEs

OSI/IP Scenario 7 (Figure 9-36) shows an example of a European network.

*Figure 9-36    OSI/IP Scenario 7: OSI OSS, OSI DCN, Other Vender GNE, OSI DCC, and ONS NEs*
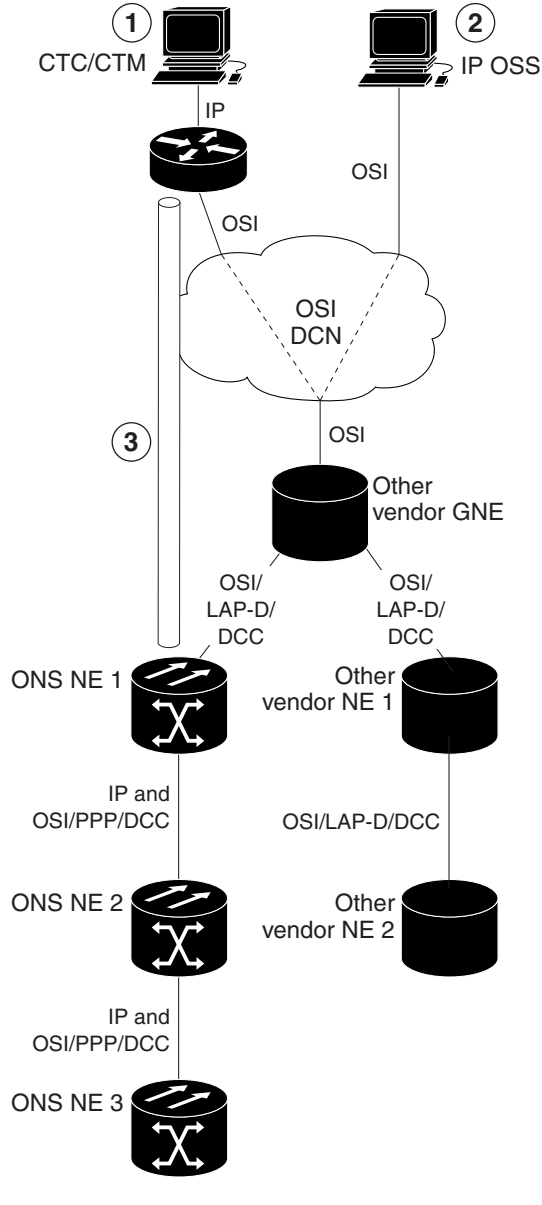


| 1 | ONS 15600 SDH NEs are managed by CTC/CTM only (TL1/FTP is not used). |
|---|---|
| 2 | The OSI OSS manages other vendor NEs only. |
| 3 | CTC/CTM communicates with the ONS 15600 SDH over a IP-over-CLNS tunnel between the ONS 15600 SDH NE and external router. |

In European networks:

- CTC and CTM are used for management only.
- IP-over-CLNS tunnels are widely accepted and deployed.

- TL1 management is not required.

- FTP file transfer is not required.

- TL1 and FTAM to FTP mediation is not required.

Management traffic between CTC/CTM and ONS 15600 SDH NEs is carried over an IP-over-CLNS tunnel. A static route is configured on the ONS 15600 SDH that terminates the tunnel (ONS 15600 SDH NE 1) so that downstream ONS 15600 SDH NEs (ONS 15600 SDH NE 2 and 3) know how to reach CTC/CTM.

## 9.6.9.8 OSI/IP Scenario 8: OSI OSS, OSI DCN, ONS GNE, OSI DCC, and Other Vender NEs

OSI/IP Scenario 8 (Figure 9-37) is another example of a European network. Similar to OSI/IP Scenario 7, the ONS 15600 SDH NEs are solely managed by CTC/CTM. The CTC/CTM IP traffic is carried over a IP-over-OSI tunnel between an external router and the ONS 15600 SDH GNE. The GNE extracts the IP from the tunnel and forwards it to the destination ONS 15600 SDH. Management traffic between the OSS and other vendor NEs is routed by the ONS 15600 SDH GNE and NEs. This is possible because all ONS 15600 SDH NEs run dual stacks (OSI and IP).

*Figure 9-37      OSI/IP Scenario 8: OSI OSS, OSI DCN, ONS GNE, OSI DCC, and Other Vender NEs*
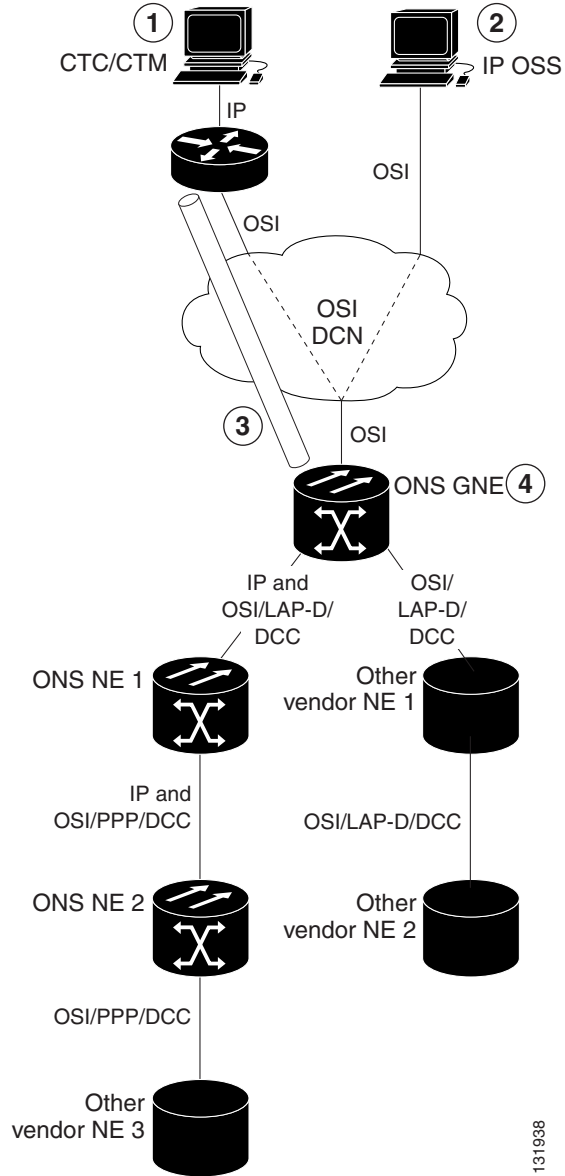


| 1 | The ONS NEs are managed by CTC/CTM only (TL1/FTP is not used). |
|---|---|
| 2 | The OSI OSS manages other vendor NEs only. |
| 3 | CTC/CTM communicates with the ONS 15600 SDH over an IP-over-CLNS tunnel between the ONS 15600 SDH NE and the external router. A static route is needed on the GNE. |
| 4 | The ONS 15600 SDH GNE routes OSI traffic to other vendor NEs. No IP-over-CLNS tunnel is needed. |

## 9.6.10 OSI Provisioning in CTC

Table 9-15 shows the OSI actions that are performed from the node view Provisioning tab. Refer to the *Cisco ONS 15600 SDH Procedure Guide* for OSI procedures and tasks.

*Table 9-15     OSI Actions from the CTC Provisioning Tab*

| Tab | Actions |
|-----|---------|
| OSI > Main Setup | • View and edit Primary Area Address.<br>• Change OSI routing mode.<br>• Change LSP buffers. |
| OSI > TARP > Config | Configure the TARP parameters:<br>• PDU L1/L2 propagation and origination.<br>• TARP data cache and loop detection buffer.<br>• LAN storm suppression.<br>• Type 4 PDU on startup.<br>• TARP timers: LDB, T1, T2, T3, T4. |
| OSI > TARP > Static TDC | Add and delete static TARP data cache entries. |
| OSI > TARP > MAT | Add and delete static manual area table entries. |
| OSI > Routers > Setup | • Enable and disable routers.<br>• Add, delete, and edit manual area addresses. |
| OSI > Routers > Subnets | Edit RS-DCC, MS-DCC, and LAN subnets that are provisioned for OSI. |
| OSI > Tunnels | Add, delete, and edit Cisco and IP-over-CLNS tunnels. |
| Comm Channels > RS-DCC | • Add OSI configuration to an RS-DCC.<br>• Choose the data link layer protocol, PPP or LAP-D. |
| Comm Channels > MS-DCC | • Add OSI configuration to an RS-DCC. |

Table 9-16 shows the OSI actions that are performed from the node view Maintenance tab.

*Table 9-16     OSI Actions from the CTC Maintenance Tab*

| Tab | Actions |
|-----|---------|
| OSI > ISIS RIB | View the IS-IS routing table. |
| OSI > ESIS RIB | View ESs that are attached to ISs. |
| OSI > TDC | • View the TARP data cache and identify static and dynamic entries.<br>• Perform TID to NSAP resolutions.<br>• Flush the TDC. |

# 9.7 IPv6 Network Compatibility

Cisco ONS 15xxx products can function in an IPv6 network when an internet router that supports Network Address Translation - Protocol Translation (NAT-PT) is positioned between the GNE, such as an ONS 15600 SDH, and the client workstation. NAT-PT is defined in RFC-2766. IPv4 and IPv6 nodes communicate with each other using NAT-PT by allowing both IPv6 and IPv4 stacks to interface between the IPv6 DCN and the IPv4 DCC networks.

NAT-PT binds addresses in IPv6 networks with addresses in IPv4 networks and vice versa to provide transparent routing for the packetss traveling between address types. This requires no changes to end nodes and IP packet routing is completely transparent to end nodes. It does, however, require NAT-PT to track the sessions it supports and mandates that inbound and outbound datagrams pertaining to a session traverse the same NAT-PT router. Protocol translation is used to extend address translation with protocol syntax/semantics translation.

**Note** Only Mozilla 1.7 is supported on clients interfacing with IPv6 networks.

C H A P T E R **10**

# Ethernet Operation

This chapter describes the operation of the Cisco ONS 15600 SDH ASAP Ethernet card.

For Ethernet card specifications, refer to Appendix A, "Hardware Specifications." For step-by-step Ethernet card circuit configuration procedures, refer to the *Cisco ONS 15600 SDH Procedure Guide*. Refer to the *Cisco ONS 15454 and Cisco ONS 15600 SDH TL1 Command Guide* for TL1 provisioning commands.

Chapter topics include:

# 10.1 Any Service Any Port Card Application

The Any Service Any Port (ASAP) Carrier Card plugs into any of the eight available I/O slots for the ONS 15600 SDH. Each ASAP carrier card has four slots available for up to and including four ASAP Pluggable Input/output Modules (PIMs). There are four slots available on the PIM for Pluggable Port Modules (PPM), which are Small Form-factor Pluggable (SFP) optics. Four PPMs per ASAP PIM are allowed, which means that there can be as many as 16 PPM optical network interfaces for each ASAP carrier card. Each PPM can support any of the following single-rate SFP optics:

- OC-3/STM-1 LR-2
- OC-12/STM-4 LR-2
- OC-48/STM-16 LR-2

Each of the PPM ports also supports the following multirate SFP optics:

- OC-3/STM-1-SR-1
- OC-12/STM-4-SR-1
- OC-48/STM-16 IR-1
- GE LX

Each ASAP 4-port I/O (4PIO) and 1-port I/O (1PIO) PIM is hot-pluggable while other ports on other PIMs are functioning. Each SFP is also hot-pluggable.

Layer 1 Ethernet transport is implemented for Gigabit Ethernet (GE) interfaces. GE traffic is encapsulated by generic framing procedure (GFP), ITU X.86, or Cisco high-level data link control/LAN extension (HDLC/LEX) and mapped into an SDH payload.

The data path processing consists of:

- Optical-to-electrical conversion (O/E) and electrical to optical (E/O) on the 4PIO PIM
- Gigabit Ethernet to Ethernet over SDH (EoS) mapping (for the GE ports only)

**Note** For a single flow of Gigabit Ethernet, traffic can be mapped to an VC4-16c. This choice limits maximum usable Ethernet ports to eight when all are mapped to VC4-16c. Any time an VC4-16c is used for an Ethernet connection, one-eighth of the total card bandwidth is consumed on the EoS mapper.

Ethernet facilities on the ASAP card include:

- Ethernet ports can be provisioned on a multirate PPM.
- Encapsulation methods allowed for the Ethernet ports are:
  - Cisco HDLC/LEX
  - GFP
  - ITU X.86
- Provisioning of an Ethernet port automatically provisions a POS port for the connection and circuit.

# 10.2 Transport Functionality

Figure 10-1 shows the transport of Ethernet frames into an SDH path using the ASAP carrier card in the ONS 15600 SDH.

**Figure 10-1      ONS 15600 SDH Ethernet Frame Transport**
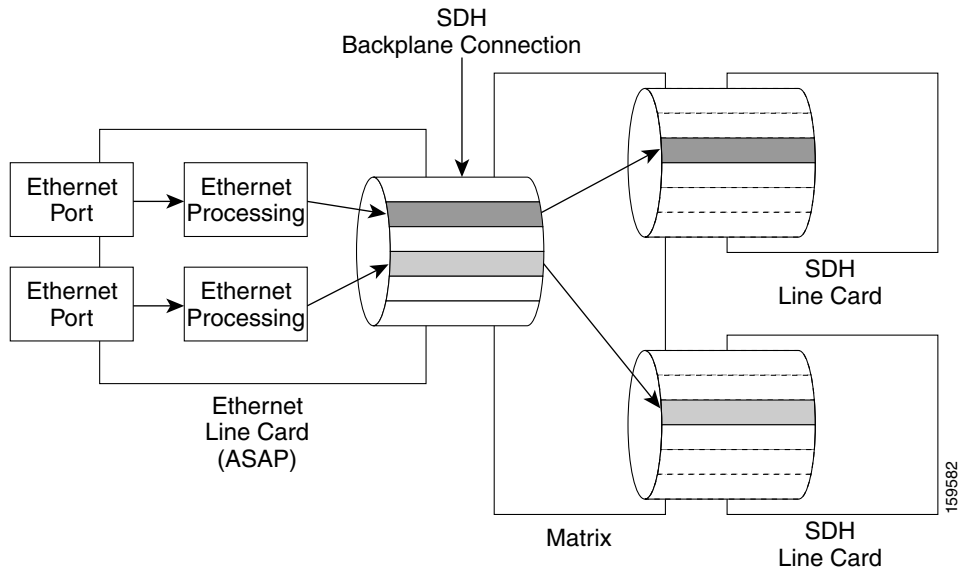


The ONS 15600 SDH provides transport functionality of all frames arriving on the Ethernet interfaces. Frames arriving on each Ethernet interface are mapped onto their own SDH path. In the reverse direction, frames arriving on an SDH path are mapped to one and only one Ethernet interface. Frames arriving on different Ethernet interfaces are not mapped onto the same SDH path.

Valid received Ethernet frames are encapsulated and transported across the SDH network. There are no modifications made to any bits in the frame that is delivered at the destination Ethernet port. Because invalid frames are dropped, this transport is not transparent.

Figure 10-2 shows Ethernet framing with HDLC/GFP header/trailers and mapping into a synchronous payload envelope (SPE) for transport over an SDH network.

**Figure 10-2      Ethernet Framing**
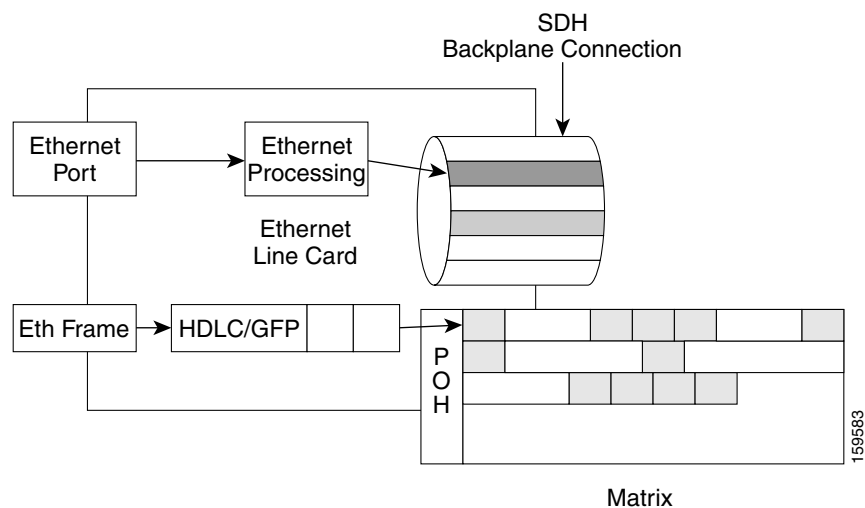


A valid frame is defined as one with the following attributes:

- Valid preamble + synchronization

- Valid size

- Valid cyclic redundancy check (CRC)

- Valid interpacket gap

# 10.3  Ethernet Rates and Mapping

This section explains the Ethernet frame format, encapsulation methods, path and circuit configurations, and oversubscription.

## 10.3.1  Frame Size

The IEEE 802.3 frame format is supported on the GE interfaces. The minimum frame size supported by the system is 64 bytes; the interface drops smaller sized frames. The maximum frame size per interface is 9600 bytes and can be provisioned independently. 9600 bytes is the maximum transmission unit (MTU).

## 10.3.2  Encapsulations

The Ethernet ports can be provisioned for encapsulation in frame-mapped GFP (GFP-F) as per ITU G.7041, Cisco HDLC/LEX as per RFC 1841, or Ethernet over Link Access Protocol over SDH (LAPS) as per ITU X.86. LEX with CRC-32 is the default encapsulation, as it is supported by most Cisco data cards.

The value of the C2 byte in a high-order SDH path is set to the following values for each encapsulation type:

- 0x1B for GFP-F

- 0x18 for X.86

- 0x05 for LEX with CRC-16

- 0x01 for LEX with CRC-32

**Note**    Bridge Control Protocol (BCP), HDLC, LEX, and ITU X.86 are all variations of Point-to-Point Protocol (PPP) in HDLC framing. To the Ethernet processor, the packets look essentially the same. GFP encapsulation is drastically different.

## 10.3.3  Path and Circuit Sizes

GE interfaces can be mapped to all supported SDH paths of sizes VC3, VC4, VC4-2c, VC4-3c, VC4-4c, VC4-8c, and VC4-16c.

**Note**    Mapping depends on the particular concatenation being supported on the card. It also depends on the concatenation being supported on all of the network elements (NEs) that the end-to-end circuit is being built through.

For full line-rate mapping to ensure the VC4-8c rate, the effects of bandwidth expansion due to HDLC/GFP/ITU X.86 encapsulations need to be taken into account to ensure no packet loss.

## 10.3.4  Oversubscription

Oversubscription of data interfaces is the mapping of an interface to a path with a lower bandwidth than the rate of the interface. When oversubscribing, the operator is relying on the fact that on data interfaces, packet transmission rates and utilization is not always 100 percent. For example, a customer with a GE interface might transmit at an average rate of only 100 Mbps.

To ensure that packet loss does not occur or that any ensuing packet loss is minimized, system engineers need to carefully estimate the amount of memory in the NE that is required to sustain any traffic bursts. Traffic bursts are characterized by several different models that take into account such parameters as the mean rate, peak rates, length of burst, and so on. Performing these calculations is more important in switching applications than in transport applications.

In the ONS 15600 SDH, oversubscription of interfaces is supported. This occurs when the GE interface is mapped to any of the VC3, VC4, VC4-2c, VC4-3c, and VC4-4c (c) rates. No guarantees on frame loss or delay due to oversubscription is provided by the system. Actual loss and delay values depend on incoming Ethernet traffic patterns.

# 10.4  Protocols over Ethernet

The ASAP card supports the BCP, PPP Half Bridge, and VLAN protocols, described in the following subsections.

## 10.4.1  Bridge Control Protocol

Support of BCP is relevant between two routers or bridges. An Ethernet card providing transport functionality is neither a router nor a bridge. Therefore, even BCP encapsulation is not supported on the Ethernet ports of the ASAP transport line card.

The ASAP line card Ethernet function is transparent to any Layer 2 and above protocol packets (the entire control plane). Any BCP control packets are transported out to the SDH interface.

## 10.4.2  PPP Half Bridge

For situations in which a routed network needs connectivity to a remote bridged Ethernet network, a serial or integrated services digital network (ISDN) interface can be configured to function as a PPP half-bridge. The line to the remote bridge functions as a virtual Ethernet interface, and the router's serial or ISDN interface functions as a node on the same Ethernet subnetwork as the remote network.

The bridge sends bridge packets to the PPP half-bridge, which converts them to routed packets and forwards them to other router processes. Likewise, the PPP half-bridge converts routed packets to Ethernet bridge packets and sends them to the bridge on the same Ethernet subnetwork.

The ASAP line card is transparent to any Layer 2 and above protocol packets (the entire control plane). Any PPP Half Bridge control packets are transported out to the SDH interface.

## 10.4.3 VLAN

The ASAP line card is transparent to VLAN tag information in the Ethernet frame.

**Note** VLANs are tunneled, and not terminated.

# 10.5 Buffering and Flow Control

Because the VC circuits can often be oversubscribed (have a bandwidth lower than that needed to support the traffic on the Ethernet port), a combination of buffering and local flow control is supported. Initially, frames that arrive on an ingress interface that cannot be transmitted immediately on the egress interface are placed in an ingress buffer. When this buffer starts filling up and is in danger of overflowing, flow control is employed. Local flow control is flow control between the Ethernet interface and the router or switch it is connected to, over the single Ethernet link. This is depicted in Figure 10-3.

*Figure 10-3    Buffering and Flow Control*
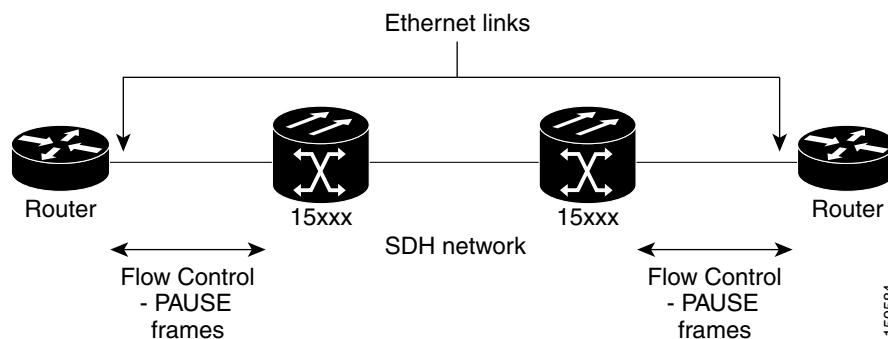


To prevent dropping of frames on an ingress Ethernet interface due to buffer congestion, an Ethernet interface sends a PAUSE frame to its peer on its egress Ethernet interface. An Ethernet interface might be capable of both sending and receiving PAUSE frames (symmetric flow control). On the other hand, it might be capable of performing only one of the two (asymmetric flow control). Two factors determine what an Ethernet interface ultimately ends up supporting:

• Flow control capability of the interface as provisioned by the operator (fixed at OFF or ON)

• Flow control capability of the peer as determined by AutoNegotiation

The Ethernet interfaces are capable of using symmetric or asymmetric flow control to meter packet receptions according to the requirements specified in IEEE 802.3x. This is done to avoid dropping packets internally due to output or input queue congestion. When an Ethernet interface uses symmetric flow control, it generates and obeys pause frames. When it uses asymmetric flow control, it only generates pause frames. Through management control, the Ethernet interface allows an operator to turn flow control ON or OFF (the default is ON).

When an Ethernet interface is set to be capable of generating PAUSE frames, it starts generating them at a rate of X PAUSE frames per second when the ingress buffer passes above a certain level called the High Water Mark. A PAUSE_TIME is specified in each PAUSE frame. The values of the PAUSE_TIME parameter and the rate X parameter are determined by the system and are not user settable.

It is expected that the peer Ethernet interface stops sending new frames after receiving a PAUSE frame for the amount of time as specified in the PAUSE_TIME. When an Ethernet interface is actively generating PAUSE frames, it stops generating them when the ingress buffer passes below a certain level, called the Low Water Mark. It is expected that the peer Ethernet interface starts sending new frames after the PAUSE frames stop.

When an Ethernet interface is set to be capable of receiving PAUSE frames, it temporarily suspends transmission of any new Ethernet frames upon reception of a PAUSE frame from its peer. Note that the transmission of any Ethernet frames already begun are completed.

When an Ethernet interface has temporarily PAUSED transmission of Ethernet frames, it resumes transmission of the frames when no new PAUSE frame is received within the PAUSE_TIME specified in the last received PAUSE frame.

The High Water Mark and Low Water Mark values are both operator provisionable. Legal values are as follows:

- Low Water Mark: from 10 kB to 74 kB
- High Water Mark: from 11 kB to 75 kB

The Low Water Mark is always lower than the High Water Mark.

The ASAP line card utilizes tail drop when frames need to be dropped. This means that the last frames received are the first to be dropped. This is implemented with a Last In First Out (LIFO) buffer.

# 10.6  Autonegotiation

The Ethernet interfaces on the ASAP card are capable of autonegotiating for full duplex (only) operation as per IEEE 802.3z. The default provisioning is to autonegotiate the duplex mode and persists in memory. Autonegotiation can be provisioned to be ON or OFF.

When flow control is turned on (and so is autonegotiation), the Ethernet interface autonegotiates and advertises all modes that it supports. The mode used by the Ethernet interface is the one agreed to by the Ethernet peers. If an agreement on the supported flow control mode cannot be reached, the transmitter is turned off. Autonegotiation is depicted in Figure 10-4.

***Figure 10-4      Autonegotiation***
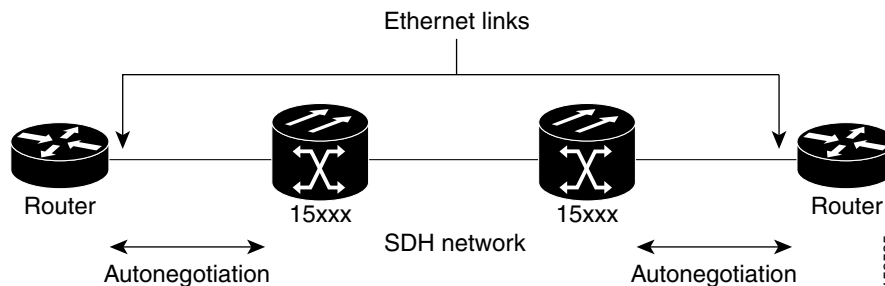
# 10.7  Gigabit EtherChannel/IEEE 802.3ad Link Aggregation

The end-to-end Ethernet link integrity feature can be used in combination with Gigabit EtherChannel (GEC) capability on attached devices. The combination provides an Ethernet traffic restoration scheme that has a faster response time than alternate techniques such as spanning tree rerouting, yet is more bandwidth efficient because spare bandwidth does not need to be reserved.

The ASAP card supports all forms of link aggregation technologies including GEC, which is a Cisco proprietary standard, and the IEEE 802.3ad standard. The end-to-end link integrity feature ASAP card allows a circuit to emulate an Ethernet link. This allows all flavors of Layer 2 and Layer 3 rerouting to work correctly with the ASAP card. Figure 10-5 illustrates GEC support.

*Figure 10-5*      *ASAP Gigabit EtherChannel (GEC) Support*
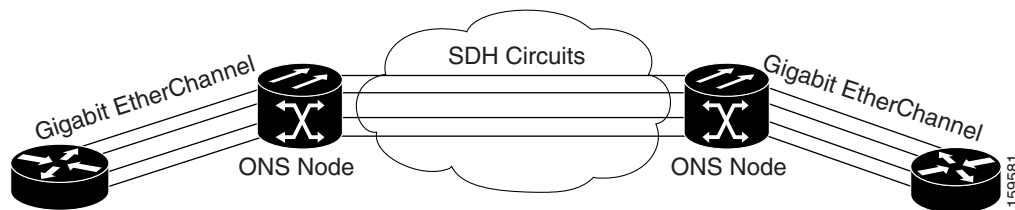


Although the ASAP card does not actively run GEC, it supports the end-to-end GEC functionality of attached Ethernet devices. If two Ethernet devices running GEC connect through the ASAP card to an ONS network, the ONS SDH side network is transparent to the EtherChannel devices. The EtherChannel devices operate as if they are directly connected to each other. Any combination of parallel circuit sizes can be used to support GEC throughput.

GEC provides line-level active redundancy and protection (1:1) for attached Ethernet equipment. It can also bundle parallel data links together to provide more aggregated bandwidth. Spanning Tree Protocol (STP) operates as if the bundled links are one link and permits GEC to utilize these multiple parallel paths. Without GEC, STP permits only a single nonblocked path. GEC can also provide ASAP card-level protection or redundancy because it can support a group of ports on different cards (or different nodes) so that if one port or card has a failure, traffic is rerouted over the other port or card.

# Alarm Monitoring and Management

This chapter explains how to manage alarms with Cisco Transport Controller (CTC), which includes:

- 11.1 Overview, page 11-1
- 11.2 Alarms, Conditions, and History, page 11-1
- 11.3 Alarm Profiles, page 11-10
- 11.4 Alarm Filter, page 11-13
- 11.5 Alarm Suppression, page 11-13
- 11.6 External Alarms and Controls, page 11-14

To troubleshoot specific alarms, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

## 11.1 Overview

CTC detects and reports SDH alarms generated by the Cisco ONS 15600 SDH and the larger SDH network. You can use CTC to monitor and manage alarms at the card, node, or network level. Default alarm severities conform to the ITU-T G.733 standard, but you can set alarm severities in customized alarm profiles or suppress CTC alarm reporting. For a detailed description of the standard Telcordia categories employed by Optical Networking System (ONS) nodes, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* "Alarm Troubleshooting" chapter.

**Note** ONS 15600 SDH alarms can also be monitored and managed through TL1 or a network management system (NMS).

## 11.2 Alarms, Conditions, and History

In the card, node, or network level CTC view, click the Alarms tab to display the alarms for that card, node or network. The Alarms window shows alarms in conformance to ITU-T G.733. This means that if a network problem causes two alarms, such as loss of frame (LOF) and loss of signal (LOS), CTC only shows the LOS alarm in this window because it supersedes LOF. (The LOF alarm can still be retrieved in the Conditions window.)

Table 11-1 describes in the information in the Alarms window.

*Table 11-1        Alarms Column Descriptions*

| Column | Information Recorded |
|---|---|
| Num | Quantity of alarm messages received; incremented automatically as alarms occur to display the current total of received error messages |
| Ref | A unique identification number assigned to each alarm to reference a specific alarm message that is displayed |
| New | Indicates a new alarm if checked[1] |
| Date | Date and time of the alarm |
| Node | Shows the name of the node where the condition or alarm occurred. (Visible in network view.) |
| Object | TL1 access identifier (AID) for the alarmed object |
| Eqpt Type | Card type in this slot |
| Shelf | The shelf where the alarmed object is located. Visible in network view. |
| Slot | Slot where the alarm occurred (appears in the network view and node view) |
| Port | Port where the alarm occurred |
| Path Width | Indicates how many STSs are contained in the alarmed path. This information complements the alarm object notation, which is explained in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15600 SDH Troubleshooting Guide*. |
| Sev | Severity level: Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) |
| ST | Status: Raised (R), Clear (C), Transient (T) |
| SA | When checked, indicates a service-affecting alarm |
| Cond | Error message/alarm name; alphabetically defined in the *Cisco ONS 15600 SDH Troubleshooting Guide* |
| Description | Description of the alarm |

1.   The user can click the Synchronize button to acknowledge the new alarm. Clicking the Delete Cleared Alarms button only deletes cleared alarms on the window.

Figure 11-1 shows the CTC node view Alarms window.

*Figure 11-1* *Viewing Alarms in CTC Node View*



Alarms and conditions appear in one of five background colors, listed in Table 11-2, to communicate severity.

*Table 11-2* *Color Codes for Alarms and Conditions*

| Color | Description |
|---|---|
| Red | Critical alarm |
| Orange | Major alarm |
| Yellow | Minor alarm |
| Magenta (pink) | Event (NA) |
| Blue | Condition (NR) |
| White | Cleared alarm or event (C) |

> **Note** Major and Minor alarms might appear yellow in CTC under certain circumstances. This is not due to a CTC problem but to a workstation memory and color utilization problem. For example, a workstation might run out of colors if many color-intensive applications are running. When using Netscape, you can limit the number of colors used by launching it from the command line with either the -install option or the -ncols 32 option.

Software Releases 7.0 and later have TL1 port-based alarm numbering that identifies an alarmed virtual container (VC) by its VC on a port rather than the VC on the optical card. The numbering is present in the VC alarm TL1 AID. The numbering scheme is described in Table 11-3.

*Table 11-3      TL1 Port-Based Alarm Numbering Scheme*

| MON Object (Optical) | Syntax and Examples |
| --- | --- |
| STM1/4/16/64 VC | Syntax: VC-<Slot>-<Pim>-<Ppm>-<Port>-<STS> <br> Ranges: VC-{1-4,11-14}-{1-4}-{1-4}-{1-$n^1$}-{1-$n^2$} |
| | Example: VC-1-1-1-1-6 |

1. Port number range varies by card type with a maximum of four.

2. Maximum VC number depends on the rate and size of the VC.

## 11.2.1 Alarm Window

Table 11-4 shows the actions you can perform in the Alarms window.

*Table 11-4      Alarm Window*

| Button | Action |
| --- | --- |
| Filter | Allows you to change the display on the Alarms window to show only alarms that meet a certain severity level, occur in a specified time frame, and/or reflect specific conditions. For example, you can set the filter so that only Critical alarms appear on the window. |
| | If you enable the Filter feature by clicking the Filter icon button in one CTC view, such as node view, it is enabled in the others as well (card view and network view). |
| Synchronize | Updates the alarm display. Although CTC displays alarms in real time, the Synchronize button verifies that CTC and the ONS 15600 SDH agree on current alarms. This is particularly useful during provisioning or troubleshooting. |
| Delete Cleared Alarms | Deletes alarms that have been cleared. |
| AutoDelete Cleared Alarms | If checked, CTC automatically deletes cleared alarms. |

## 11.2.2 Alarm-Affected Circuits

You can determine which ONS 15600 SDH circuits are affected by a specific alarm by positioning the cursor over the alarm in the Alarm window and right-clicking. A shortcut menu appears (Figure 11-2).

*Figure 11-2 Select the Affected Circuits Option for an Alarm*
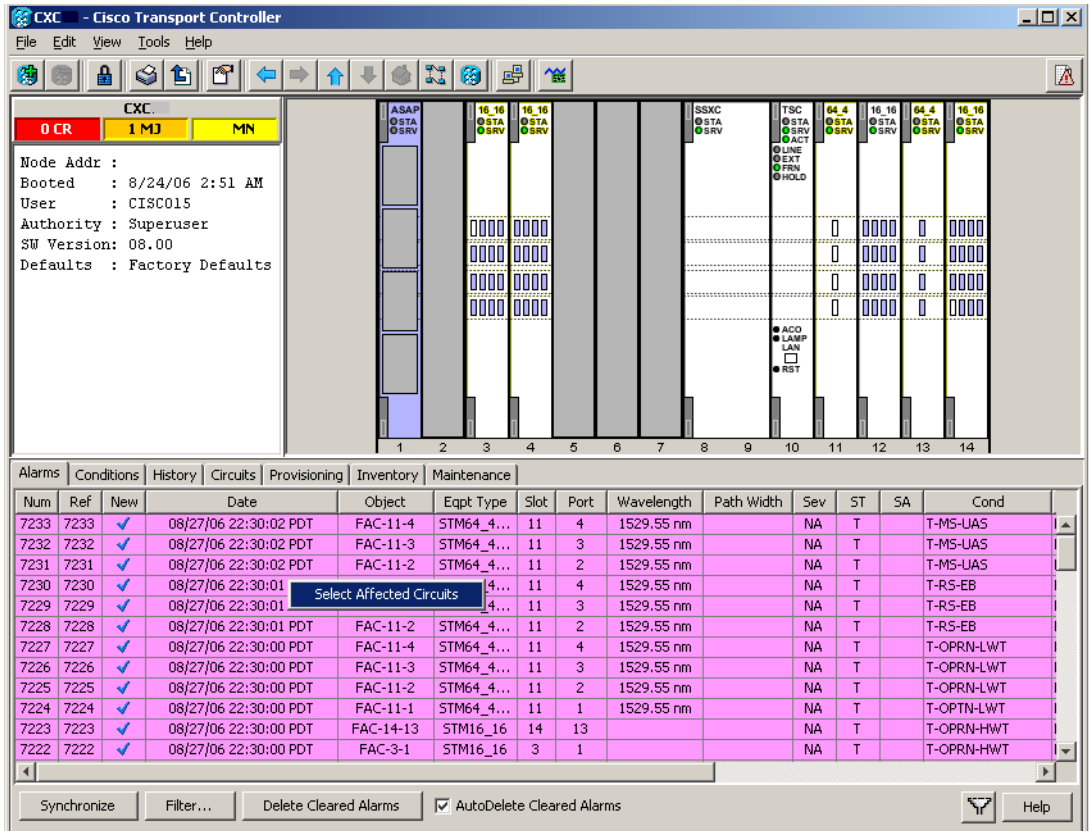


When the user selects the Select Affected Circuits option, the Circuits window opens to show the circuits that are affected by the alarm.

## 11.2.3 Conditions Window

The Conditions window displays retrieved fault conditions. A condition is a fault or status detected by ONS 15600 SDH hardware or software. When a condition occurs and continues for a minimum period, CTC raises a condition, which is a flag showing that this particular condition currently exists on the ONS 15600 SDH.

The Conditions window shows all conditions that occur, including those that are superseded by alarms. For instance, if a network problem causes two alarms, such as LOF and LOS, CTC shows both the LOF and LOS conditions in this window. Having all conditions visible can be helpful when troubleshooting the ONS 15600 SDH. If you want to retrieve conditions that obey a root-cause hierarchy (that is, LOS supersedes and replaces LOF), you can exclude the same root causes.

Fault conditions include reported alarms and Not Reported or Not Alarmed conditions. Refer to the trouble notifications information in the *Cisco ONS 15600 SDH Troubleshooting Guide* "Alarm Troubleshooting" chapter for more information about alarm and condition classifications.

# 11.2.4 Conditions Window Actions

Table 11-5 shows the actions you can perform in the Conditions window.

*Table 11-5*        *Conditions Display*

| Button | Action |
|--------|--------|
| Retrieve | Retrieves the current set of all existing fault conditions, as maintained by the alarm manager, from the ONS 15600 SDH. |
| Filter | Allows you to change the Conditions window display to only show the conditions that meet a certain severity level or occur in a specified time. For example, you can set the filter so that only Critical conditions display on the window. |
| | There is a Filter icon button in the lower-right corner of the window that allows you to enable or disable the filter feature. |

The current set of all existing conditions maintained by the alarm manager appears when you click the Retrieve button. The set of conditions retrieved is relative to the view. For example, if you click the button in the node view, node-specific conditions appear (Figure 11-3). If you click the Retrieve button in the network view, all conditions for the network (including ONS 15600 SDH nodes and other connected nodes such as ONS 15454 SDHs) appear, and the card view shows only card-specific conditions.

**Figure 11-3    Viewing Conditions in the Conditions Window**



Table 11-6 lists the Conditions window column headings and the information recorded in each column.

**Table 11-6    Conditions Column Description**

| Column | Information Recorded |
| --- | --- |
| Date | Date and time of the condition |
| Node | Shows the name of the node where the condition or alarm occurred. (Visible in network view.) |
| Object | TL1 AID for the alarmed object |
| Eqpt Type | Card type in this slot (only displayed in the network view and node view) |
| Shelf | The shelf where the alarmed object is located. Visible in network view. |
| Slot | Slot where the condition occurred (only displayed in the network view and node view) |
| Port | Port where the condition occurred |
| Path Width | Width of the data path |
| Sev | Severity level: CR, MJ, MN, NA, NR |
| SA | When checked, indicates a service-affecting alarm |
| Cond | Condition name; alphabetically listed and defined in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15600 SDH Troubleshooting Guide* |
| Description | Description of the condition |

# 11.2.5 History Window

The History window displays historical alarm data. It also displays conditions, which are Not Alarmed activities such as timing changes and threshold crossings. For example, protection-switching events or performance-monitoring threshold crossings appear here. The ONS 15600 SDH can store up to 3,000 total alarms and conditions: 750 Critical alarms, 750 Major alarms, 750 Minor alarms, and 750 conditions. When the limit is reached, the ONS 15600 SDH begins replacing the oldest items. The History window presents several alarm history views:

- The History > Session window appears in network view, node view, and card view (Figure 11-4). It shows alarms and conditions that have occurred during the current user CTC session.

- The History > Shelf window appears only in node view. It shows the alarms and conditions that have occurred on the node since CTC software was originally activated for that node.

- The History > Card window appears only in the card view. It shows the alarms and conditions that have occurred on the card since CTC software was installed on the node.

**Note** In the Preference dialog box General tab, the Maximum History Entries value applies to only the Session window.

**Tip** Double-click an alarm in the History window to display the corresponding view. 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.

*Figure 11-4        Viewing All Alarms Reported for a Node*
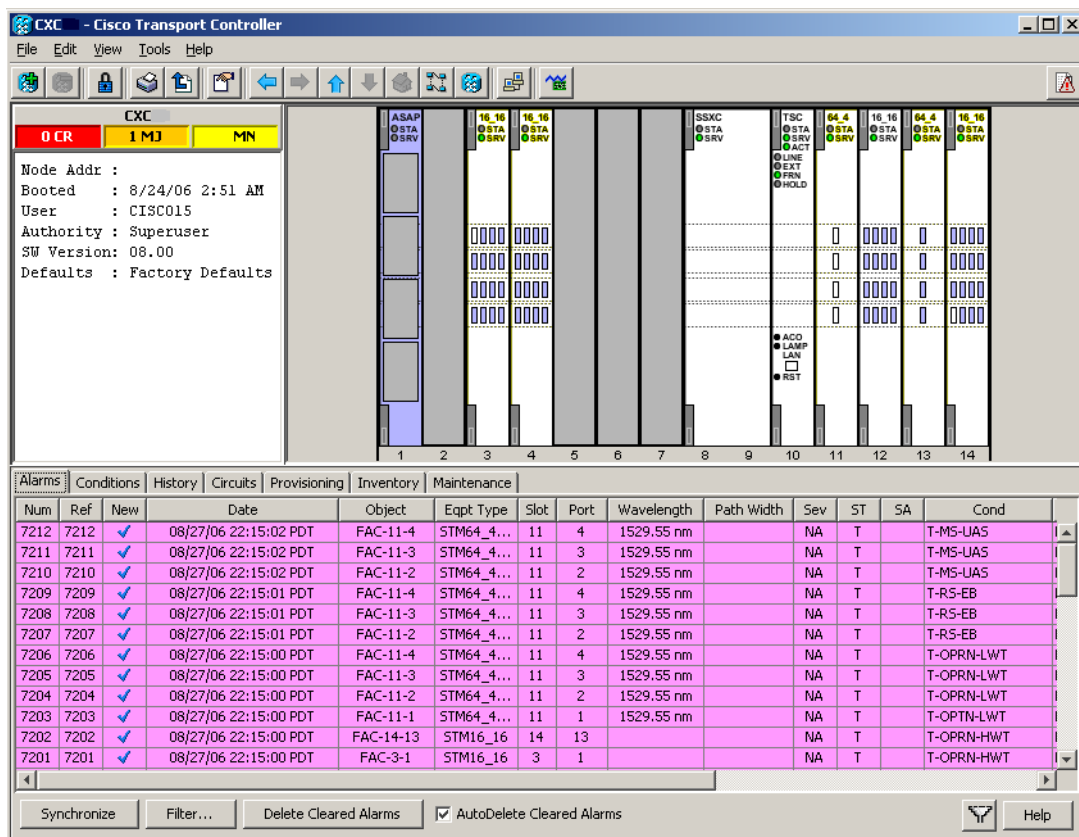


Table 11-7 describes the information in the History window.

*Table 11-7        History Column Description*

| Column | Information Recorded |
| --- | --- |
| Num | An incrementing count of alarm or condition messages. (The column is hidden by default; to view it, right-click a column and choose **Show Column > Num**.) |
| Ref | The reference number assigned to the alarm or condition. (The column is hidden by default; to view it, right-click a column and choose **Show Column > Ref**.) |
| Date | Date and time of the alarm |
| Node | Shows the name of the node where the condition or alarm occurred. (Visible in network view.) |
| Object | TL1 AID for the alarmed object |
| Eqpt Type | Card type in this slot (only displays in network view and node view) |
| Shelf | The shelf where the alarmed object is located. Visible in network view. |
| Slot | Slot where the condition occurred (only displays in network view and node view) |
| Port | Port where the condition occurred |
| Path Width | Width of the data path |
| Sev | Severity level: CR, MJ, MN, NA, NR |

*Table 11-7      History Column Description (continued)*

| Column | Information Recorded |
|---|---|
| SA | When checked, indicates a service-affecting alarm |
| ST | Status: R (raised), C (cleared), T (transient) |
| Description | Description of the condition |
| Cond | Condition name |

# 11.2.6  Alarm History Actions

You can retrieve and view the history of alarms and conditions, as well as Transient conditions (passing notifications of processes as they occur) in the CTC History window. The information in this window is specific to the view where it is shown (that is, network history in the network view, node history in the node view, and card history in the card view). For more information about Transient conditions, refer to the "Transient Conditions" chapter in the *Cisco ONS 15600 SDH Troubleshooting Guide*.

The node and card history views are each divided into two tabs. In node view, when you click the Retrieve button, you can see the history of alarms, conditions, and transients that have occurred on the node in the History > Shelf window, and the history of alarms, conditions, and transients that have occurred on the node during your login session in the History > Session window. When you retrieve the card history, you can see the history of alarms, conditions, and transients on the card in the History > Card window, or a history of alarms, conditions, and transients that have occurred during your login session in the History > Session window. You can also filter the severities and occurrence period in these history windows.

# 11.3  Alarm Profiles

The alarm profiles feature allows you to change default alarm severities by creating unique alarm profiles for individual ONS 15600 SDH ports, cards, or nodes. A created alarm profile can be applied to any node on the network. Alarm profiles can be saved to a file and imported elsewhere in the network, but the profile must be stored locally on a node before it can be applied to the node, cards, or ports.

CTC can store up to ten active alarm profiles at any time to apply to the node. Custom profiles can take eight of these active profile positions. Two other profiles, Default profile and Inherited profile, are reserved by the network element (NE), and cannot be edited. The reserved Default profile contains ITU-T G.733 severities. The reserved Inherited profile allows port alarm severities to be governed by the card-level severities or card alarm severities to be determined by the node-level severities.

If one or more alarm profiles have been stored as files from elsewhere in the network onto the local PC or server hard drive where CTC resides, you can utilize as many profiles as you can physically store by deleting and replacing them locally in CTC so that only eight are active at any given time.

# 11.3.1  Alarm Profile Window

Alarm profiles are created in the network view using the Provisioning > Alarm Profiles tab. A default alarm profile (in the Default column) is preprovisioned for every alarm. After loading the default profile on the node, you can use the Clone feature to create new profiles based on the default alarm profile. After the new profile is created, the Alarm Profiles window shows the default profile and the new profile (Figure 11-5).

*Figure 11-5        Node View Alarm Profiles Window Showing the Default Profiles of Listed Alarms*
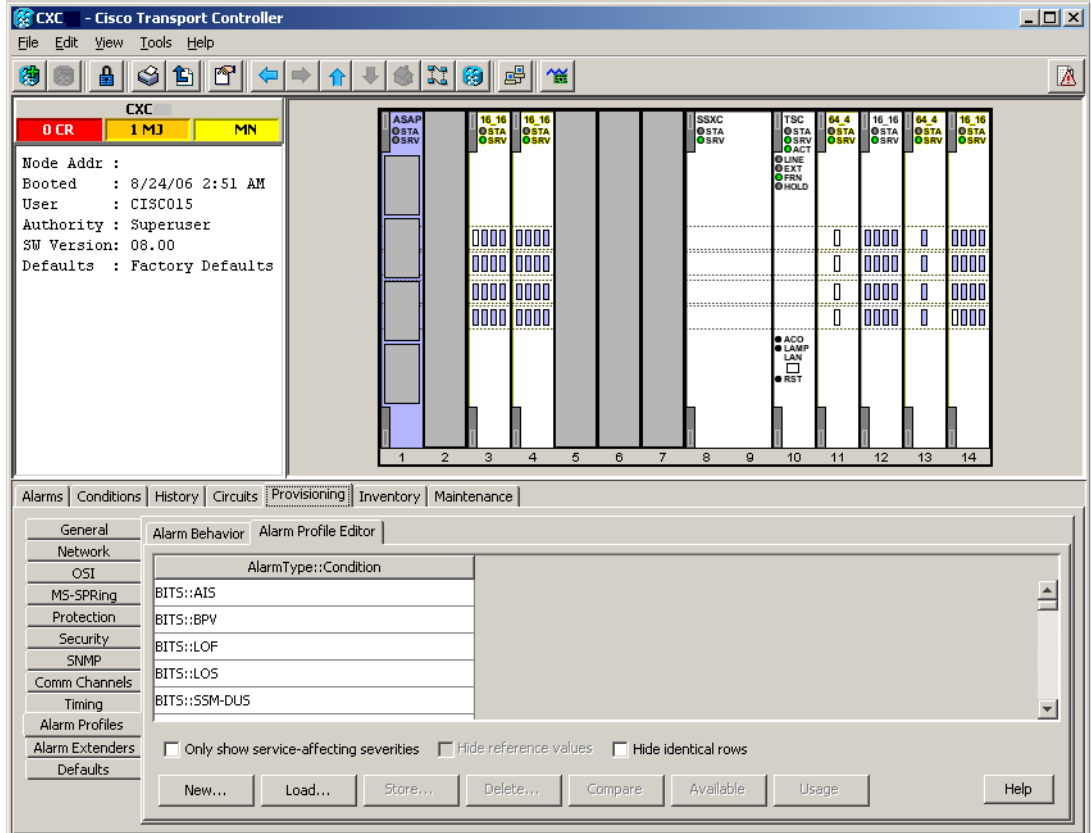


## 11.3.2  Alarm Profile Buttons

The Alarm Profiles window has six buttons at the bottom. Table 11-8 describes each of the alarm profile buttons.

*Table 11-8        Alarm Profile Buttons*

| Button | Description |
| --- | --- |
| New | Adds a new alarm profile. |
| Load | Loads a profile to a node or a file. |
| Store | Saves profiles on a node (or nodes) or in a file. |
| Delete | Deletes profiles from a node. |
| Compare | Displays differences between alarm profiles (individual alarms that are not configured equivalently between profiles). |
| Available | Displays all profiles available on each node. |
| Usage | Displays all entities (nodes and alarm subjects) present in the network and which profiles contain the alarm (can be printed). |

## 11.3.3 Alarm Profile Editing

Table 11-9 describes the five profile-editing options available when you right-click an alarm item in the profile column (such as Default).

*Table 11-9      Alarm Profile Editing Options*

| Button | Description |
|--------|-------------|
| Store | Saves a profile in a node or in a file. |
| Rename | Changes a profile name. |
| Clone | Creates a new profile that contains the same alarm severity settings as the profile being cloned. |
| Reset | Restores a profile to its previous state or to the original state (if it has not yet been applied). |
| Remove | Removes a profile from the table editor. |

## 11.3.4 Alarm Severity Option

To change or assign alarm severity, left-click the alarm severity you want to change in the alarm profile column. Seven severity levels appear for the alarm:

- Not Reported (NR)
- Not Alarmed (NA)
- Minor (MN)
- Major (MJ)
- Critical (CR)
- Use Default
- Transient (T)

Transient and Use Default severity levels only appear in alarm profiles. They do not appear when you view alarms, history, or conditions.

## 11.3.5 Row Display Options

In the network view, the Alarm Profiles window has two check boxes at the bottom of the window:

- Hide reference values—Highlights alarms with nondefault severities by clearing alarm cells with default severities. This check box is normally unavailable. It becomes active only when more than one profile is listed in the Alarm Profile Editor window. (The check box text changes to "Hide Values matching profile Default" in this case.)
- Hide identical rows—Hides rows of alarms that contain the same severity for each profile.

## 11.3.6 Alarm Profile Actions

In CTC node view, the Provisioning > Alarm Profiles > Alarm Profile Editor window displays alarm profiles for the node, and in card view this windows displays the alarm profiles for the selected card.

Alarm profiles form a hierarchy. A node-level alarm profile applies to all cards in the node except cards that have their own profiles. A card-level alarm profile applies to all ports on the card except ports that have their own profiles.

At the node level, you can apply profile changes on a card-by-card basis or set a profile for the entire node. At the card-level view, you can apply profile changes on a port-by-port basis for all ports on that card. Figure 11-6 shows an STM-16 card view of an alarm profile.

*Figure 11-6        Alarm Profile on an STM-16 Card*
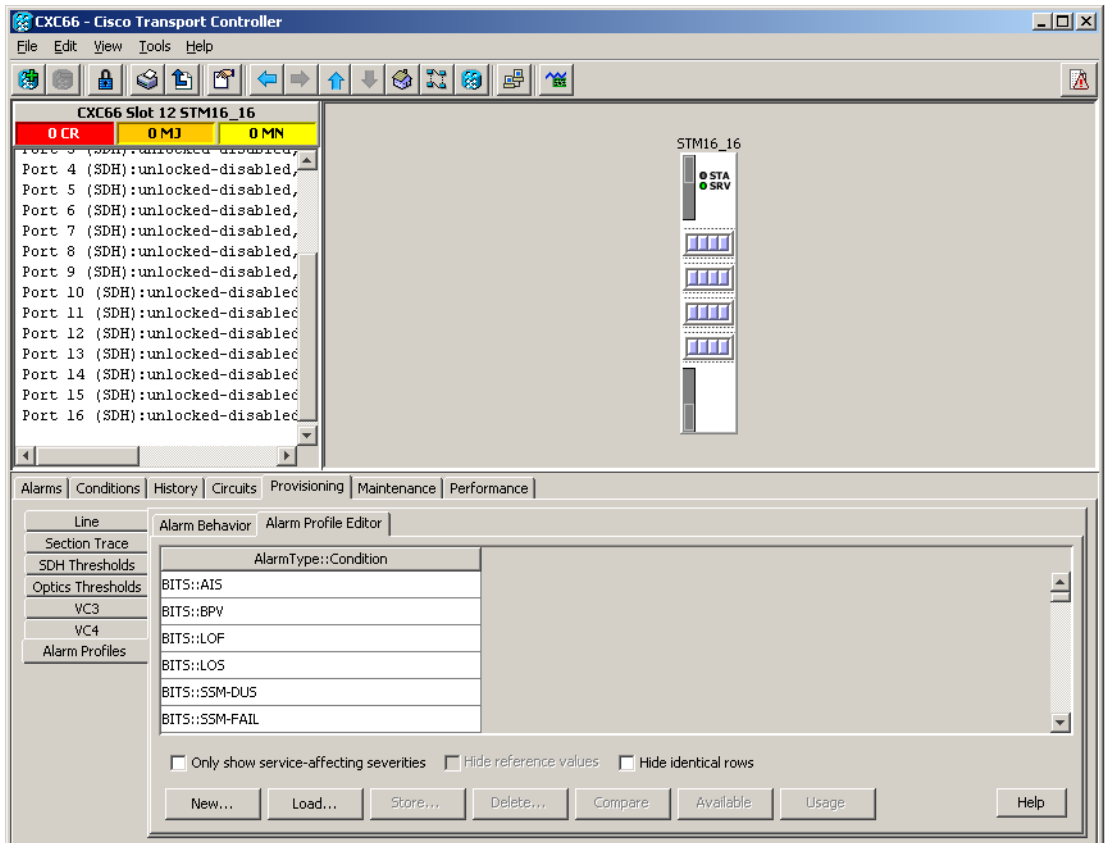


## 11.4  Alarm Filter

Alarm display can be filtered to keep particular alarm severities, or alarms that occur between certain dates, from appearing in the Alarms window (Figure 11-2 on page 11-5). You can set the parameters of the filter by clicking Filter at the bottom-left of the Alarms window. You can turn the filter on or off by clicking the Filter icon button at the bottom-right of the window. CTC retains your filter activation setting. For example, if you turn the filter on and then log out, CTC makes the filter active the next time your user ID is activated.

## 11.5  Alarm Suppression

The following sections explain alarm suppression features for the ONS 15600 SDH.

## 11.5.1 Alarms Suppressed for Maintenance

When you place a port in Locked,maintenance administrative state, this raises the alarm suppressed for maintenance (AS-MT) alarm in the Conditions and History windows and causes subsequently raised alarms for that port to be suppressed.

While the facility is in the Locked,maintenance state, any alarms or conditions that are raised and suppressed on it (for example, a transmit failure [TRMT] alarm) are reported in the Conditions window and show their normal severity in the Sev column. The suppressed alarms are not shown in the Alarms and History windows. (These windows only show AS-MT). When you place the port back into Unlocked,automaticInService administrative state, the AS-MT alarm is resolved in all three windows. Suppressed alarms remain raised in the Conditions window until they are cleared.

## 11.5.2 Alarms Suppressed by User Command

In the Provisioning > Alarm Profiles > Alarm Behavior tab, the ONS 15600 SDH has an alarm suppression option that clears raised alarm messages for the node, chassis, one or more slots (cards), or one or more ports. Using this option raises the alarms suppressed by user command, or AS-CMD alarm. The AS-CMD alarm, like the AS-MT alarm, appears in the Conditions, and History windows. Suppressed conditions (including alarms) appear only in the Conditions window--showing their normal severity in the Sev column. When the Suppress Alarms check box is unchecked, the AS-CMD alarm is cleared from all three windows.

**Note**   AS-MT can be seen in the Alarms window if you set the Filter dialog box to show NA severity events.

A suppression command applied at a higher level does not supersede a command applied at a lower level. For example, applying a node-level alarm suppression command makes all raised alarms for the node appear to be cleared, but it does not cancel out card-level or port-level suppression. Each of these conditions can exist independently and must be cleared independently.

**Caution**   Use alarm suppression with caution. If multiple CTC or TL1 sessions are open, suppressing the alarms in one session suppresses the alarms in all other open sessions.

**Note**   When an entity is put in the Locked,maintenance administrative state, the ONS 15600 SDH suppresses all standing alarms on that entity. All alarms and events appear on the Conditions tab. You can change this behavior for the LPBKFACILITY and LPBKTERMINAL alarms. To display these alarms on the Alarms tab, set the NODE.general.ReportLoopbackConditionsOnPortsIn Locked,maintenance to TRUE on the NE Defaults tab.

# 11.6 External Alarms and Controls

External alarm inputs are used for external sensors such as open doors and flood sensors, temperature sensors, and other environmental conditions. External control outputs allow you to drive external visual or audible devices such as bells and lights. They can control other devices such as generators, heaters, and fans.

You provision external alarms and controls in the node view Maintenance > Alarm Extenders window. Up to 16 external alarm inputs and 16 external controls are available. The external input/output contacts are located on the CAP/CAP2 attached to the ONS 15600 SDH backplane.

## 11.6.1 External Alarm Input

You can provision each alarm input separately. Provisionable characteristics of external alarm inputs include:

- Alarm type
- Alarm severity (CR, MJ, MN, NA, and NR)
- Alarm-trigger setting (open or closed)
- Virtual wire associated with the alarm
- CTC alarm log description (up to 63 characters)

## 11.6.2 External Control Output

You can provision each alarm output separately. Provisionable characteristics of alarm outputs include:

- Control type
- Trigger type (alarm or virtual wire)
- Description for CTC
- Closure setting (manually or by trigger). If you provision the output closure to be triggered, the following characteristics can be used as triggers:
  - Local NE alarm severity—A chosen alarm severity (for example, Major) and any higher-severity alarm (in this case, Critical) causes output closure.
  - Remote NE alarm severity—Similar to local NE alarm severity trigger setting, but applies to remote alarms.
  - Virtual wire entities—You can provision an alarm that is input to a virtual wire to trigger an external control output.

## 11.6.3 Virtual Wires for External Alarms in Mixed Networks

Virtual wires route external alarms to one or more alarm collection centers in a network. External alarms can be assigned to virtual wires in networks containing only ONS 15600 SDHs or in mixed networks containing ONS 15600 SDHs and ONS 15454 SDHs. You can view virtual wires in the CTC node view Maintenance > Alarm Extenders > Virtual Wires window.

When using virtual wires, you can:

- Assign different external devices to the same virtual wire.
- Assign virtual wires as the trigger type for different external controls.

The ONS 15600 SDH supports 16 virtual wires. The ONS 15454 SDH support four virtual wires. In mixed ONS 15600 SDH/15454 SDH networks, CTC displays the virtual wire information differently based upon where it is viewed.

Figure 11-7 shows an ONS 15600 SDH Virtual Wires window with a DCC connection to an
ONS 15454 SDH node. The Virtual Wires window shows 10 virtual wire columns, but 16 are available.
The first 12 are available for other ONS 15600 SDHs. Only the last four are available for the ONS 15454
SDH, because it can only support four virtual wires.

*Figure 11-7*      *Virtual Wires Seen from an ONS 15600 SDH*

C H A P T E R **12**
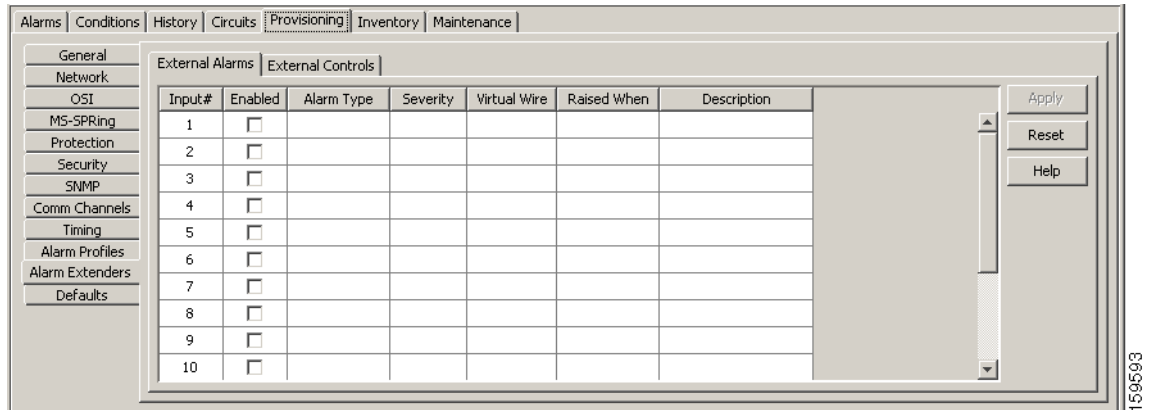
# Performance Monitoring

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

This chapter defines PM parameters and concepts for Cisco ONS 15600 SDH optical cards. You can use performance monitoring (PM) parameters to gather, store, threshold, and report performance data for early detection of problems.

> **Note** For additional information regarding PM parameters, refer to ITU-T G.826, G.827, G.828, G.829, M2101, and M2102, or Telcordia documents GR-1230-CORE, GR-820-CORE, GR-499-CORE, and GR-253-CORE and the ANSI T1.231 document entitled *Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*.

For information about enabling and viewing PM values, refer to the *Cisco ONS 15600 SDH Procedure Guide.*

Chapter topics include:

## 12.1 Threshold Performance Monitoring

Thresholds are used to set error levels for each PM. You can program PM threshold ranges from the Provisioning > SDH Thresholds tabs on the Cisco Transport Controller (CTC) card view. To provision card thresholds, such as line, path, and SDH thresholds, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

During the accumulation cycle, if the current value of a performance monitoring parameter reaches or exceeds its corresponding threshold value, a threshold crossing alert (TCA) is generated by the node and sent to CTC. TCAs provide early detection of performance degradation. When a threshold is crossed, the node continues to count the errors during a given accumulation period. If 0 is entered as the threshold value, the performance monitoring parameter is disabled.

Change the threshold if the default value does not satisfy your error monitoring needs. For example, customers with a critical VC3 installed for on-demand emergency calls must guarantee the best quality of service on the line; therefore, they lower all thresholds so that the slightest error raises a TCA.

# 12.2 Intermediate-Path Performance Monitoring

Intermediate-path performance monitoring (IPPM) allows a nonterminating node to transparently monitor a constituent channel of an incoming transmission signal. ONS 15600 SDH networks only use line terminating equipment (LTE), not path terminating equipment (PTE). The following cards are LTE equipment in the ONS 15600 SDH system:

- OC48/STM16 SR/SH 16 Port 1310
- OC48/STM16 LR/LH 16 Port 1550
- OC192/STM64 SR/SH 4 Port 1310
- OC192/STM64 LR/LH 4 Port 1550
- OC192LR/STM64 4 Port ITU C-Band

IPPM enables LTE cards to monitor near-end path PM data on individual virtual containers (VC) payloads. After enabling IPPM on provisioned VC3 or VC4 ports, service providers can monitor large amounts of VC traffic through intermediate nodes, thus making troubleshooting and maintenance activities more efficient.

IPPM occurs only on VC4 paths that have IPPM enabled, and TCAs are raised only for PM parameters on the selected IPPM paths. The monitored IPPMs are VC4 HP-EB, VC4 HP-ES, VC4 HP-SES, VC4 HP-UAS, and VC4 HP-BBE. The following ratio parameters are provided: VC4 HP-BBER, VC4 HP-ESR, and VC4 HP-SESR. To enable IPPM, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

The ONS 15600 SDH performs IPPM by examining the overhead in the monitored path and reading all of the near-end path performance monitoring parameters in the incoming transmission direction. The IPPM process allows the path overhead to pass bidirectionally through the node completely unaltered.

For detailed information about specific performance monitoring parameters, see the .

# 12.3 Pointer Justification Count

Pointers are used to compensate for frequency and phase variations. Pointer justification counts indicate timing differences on SDH networks. When a network is not synchronized, frequency and phase variations occur on the transported signal. Excessive frequency and phase variations can cause terminating equipment to slip. These variations also cause slips at the SDH and plesiosynchronous digital hierarchy (PDH) boundaries.

Slips cause different effects in service. Voice service has intermittent audible clicks. Compressed voice technology has short transmission errors or dropped calls. Fax machines lose scanned lines or experience dropped calls. Digital video transmission has distorted pictures or frozen frames. Encryption service loses the encryption key, which causes data to be transmitted again.

Pointers align the phase variations in VC4 and TU payloads. The VC4 payload pointer is located in the H1 and H2 bytes of the line overhead. Clocking differences are measured by the offset in bytes from the pointer to the first byte of the VC4 virtual container (VC) called the J1 byte. A small number of pointer justification counts per day is not cause for concern. If the pointer justification count continues to rise or becomes large, action must be taken to correct the problem.

You can enable positive pointer justification count (PPJC) and negative pointer justification count (NPJC) performance monitoring parameters for LTE cards.

PPJC is a count of path-detected (PPJC-Pdet) or path-generated (PPJC-Pgen) positive pointer justifications depending on the specific PM name. NPJC is a count of path-detected (NPJC-Pdet) or path-generated (NPJC-Pgen) negative pointer justifications depending on the specific PM name.

A consistent pointer justification count indicates clock synchronization problems between nodes. A difference between the counts means the node transmitting the original pointer justification has timing variations with the node detecting and transmitting this count. Positive pointer adjustments occur when the frame rate of the VC is too slow in relation to the rate of the VC4.

For pointer justification count definitions, see the "12.4  Performance-Monitoring Parameter Definitions" section on page 12-3. In CTC, the PM count fields for PPJC and NPJC appear white and blank unless IPPM is enabled.

# 12.4  Performance-Monitoring Parameter Definitions

Table 12-1 gives definitions for each type of performance-monitoring parameter found in this chapter.

*Table 12-1*       ***Performance Monitoring Parameters***

| Parameter | Definition |
|---|---|
| MS-EB | Multiplex Section Errored Block (MS-EB) indicates that one or more bits are in error within a block. |
| MS-ES | Multiplex Section Errored Second (MS-ES) is a one-second period with one or more errored blocks or at least one defect. |
| MS-SES | Multiplex Section Severely Errored Second (MS-SES) is a one-second period which contains 30 percent or more errored blocks or at least one defect. SES is a subset of ES. For more information, see ITU-T G.829 Section 5.1.3. |
| MS-BBE | Multiplex Section Background Block Error (MS-BBE) is an errored block not occurring as part of an SES. |
| MS-UAS | Multiplex Section Unavailable Seconds (MS-UAS) is a count of the seconds when the section was unavailable. A section becomes unavailable when ten consecutive seconds occur that qualify as MS-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as MS-SESs. When the condition is entered, MS-SESs decrement and then count toward MS-UAS. |
| MS-FC | Count of the number of occurrences of near-end failure events, and is incremented by one each time a near-end failure event begins. Failure counts are incremented during unavailable time. |

*Table 12-1*     *Performance Monitoring Parameters (continued)*

| Parameter | Definition |
|-----------|-----------|
| MS-ESR | Multiplex Section Errored Second Ratio (MS-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval. |
| MS-SESR | Multiplex Section Severely Errored Second ratio (MS-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval. |
| MS-BBER | Multiplex Section Background Block Error Ratio (MS-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs. |
| MS-PSC-W | For a working line in a 2-fiber MS-SPRing, Multiplex Section Protection Switching Count-Working (MS-PSC-W) is a count of the number of times traffic switches away from the working capacity in the failed line and back to the working capacity after the failure is cleared. MS-PSC-W increments on the failed working line and MS-PSC increments on the active protect line. For a working line in a 4-fiber MS-SPRing, MS-PSC-W is a count of the number of times service switches from a working line to a protection line plus the number of times it switches back to the working line. MS-PSC-W increments on the failed line and MS-PSC-R or MS-PSC-S increments on the active protect line. |
| MS-PSD-W | For a working line in a two-fiber MS-SPRing, Multiplex Section Protection Switching Duration-Working (MS-PSD-W) is a count of the number of seconds that service was carried on the protection line. MS-PSD-W increments on the failed working line and MS-PSD increments on the active protect line. |
| HP-EB | High-Order Path Errored Block (HP-EB) indicates that one or more bits are in error within a block. |
| HP-ES | High-Order Path Errored Second (HP-ES) is a one-second period with one or more errored blocks or at least one defect. |
| HP-SES | High-Order Path Severely Errored Seconds (HP-SES) is a one-second period containing 30 percent or more errored blocks or at least one defect. SES is a subset of ES. |
| HP-BBE | High-Order Path Background Block Error (HP-BBE) is an errored block not occurring as part of an SES. |
| HP-UAS | High-Order Path Unavailable Seconds (HP-UAS) is a count of the seconds when the VC path was unavailable. A high-order path becomes unavailable when ten consecutive seconds occur that qualify as HP-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as HP-SESs. |
| HP-FC | Count of the number of occurrences of near-end failure events, and is incremented by one each time a near-end failure event begins. Failure counts are incremented during unavailable time. |
| RS-EB | Regenerator Section Errored Block (RS-EB) indicates that one or more bits are in error within a block. |
| RS-ES | Regenerator Section Errored Second (RS-ES) is a one-second period with one or more errored blocks or at least one defect. |
| RS-SES | Regenerator Section Severely Errored Second (RS-SES) is a one-second period which contains 30 percent or more errored blocks or at least one defect. SES is a subset of ES. |

*Table 12-1* *Performance Monitoring Parameters (continued)*

| Parameter | Definition |
|---|---|
| RS-BBE | Regenerator Section Background Block Error (RS-BBE) is an errored block not occurring as part of an SES. |
| RS-ESR | Regenerator Section Errored Second Ratio (RS-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval. |
| RS-SESR | Regenerator Section Severely Errored Second Ratio (RS-SES) is the ratio of SES to total seconds in available time during a fixed measurement interval. |
| RS-BBER | Regenerator Section Background Block Error Ratio (RS-BBE) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs. |
| RS-UAS | Regenerator Section Unavailable Second (RS-UAS) is a count of the seconds when the regenerator section was unavailable. A section becomes unavailable when ten consecutive seconds occur that qualify as RS-UASs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as RS-UASs. |

# 12.5 Optical Card Performance Monitoring

The following sections define performance monitoring parameters for the OC-48/STM16, and OC-192/STM64 optical cards.

## 12.5.1 OC-48/STM16, and OC-192/STM64 Card Performance Monitoring Parameters

Figure 12-1 shows where overhead bytes detected on the Application-Specific Integrated Circuits (ASICs) produce performance monitoring parameters for the OC-48/STM16, and OC-192/STM64 optical cards.

*Figure 12-1*      *PM Read Points on the OC-48/STM16, and OC-192/STM64 Cards*
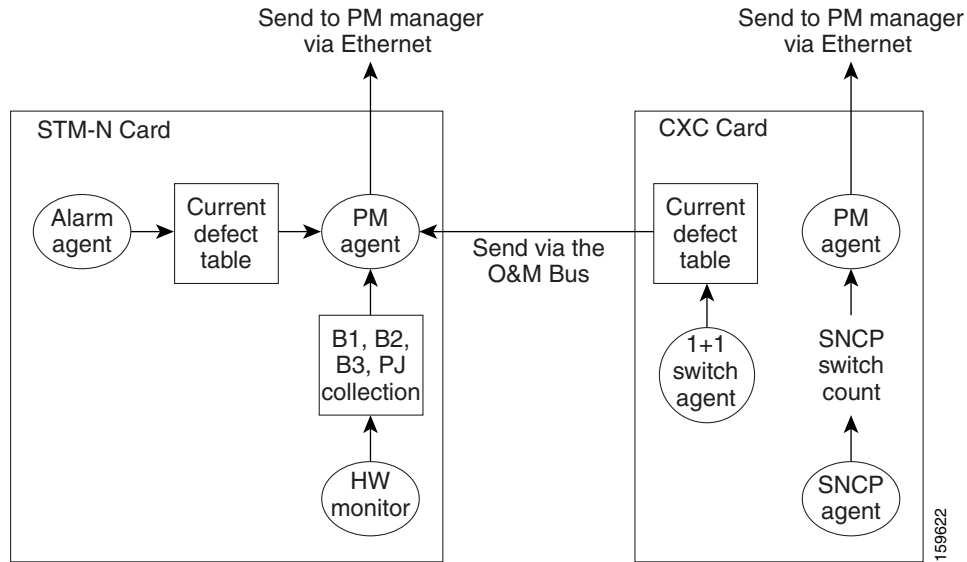


**Note**    For PM locations relating to protection switch counts, see the Telcordia GR-1230-CORE document.

Table 12-2 lists the near-end and far-end section layer PMs.

*Table 12-2*      *OC48/STM16, and OC-192/STM64 Card PMs*

| RS (NE/FE) | MS (NE/FE) | PSC (NE)[1, 2] | PJC (NE) | VC4 and VC4-Xc HP Path (NE) |
|---|---|---|---|---|
| RS-EB | MS-EB | MS-PSC | HP-PPJC-Pdet | HP-BBE |
| RS-ES | MS-ES | MS-PSD | HP-NPJC-Pdet | HP-BBER |
| RS-SES | MS-SES | MS-PSC-W | HP-PPJC-Pgen | HP-EB |
| RS-OFS | MS-UAS | MS-PSD-W | HP-NPJC-Pgen | HP-ES |
| RS-BBE | MS-FC | | HP-PJCDiff | HP-ESR |
| | MS-BBE | | HP-PJCS-Pdet | HP-SES |
| | | | HP-PJCS-Pgen | HP-SESR |
| | | | | HP-UAS |

1. SDH path performance monitoring parameters increment only if IPPM is enabled. For additional information, see the "12.2 Intermediate-Path Performance Monitoring" section on page 12-2. To monitor SDH path performance monitoring parameters, log into the far-end node directly.

2. For information about troubleshooting path protection configurations (path protection) switch counts, refer to the *Cisco ONS 15600 SDH Reference Manual f*or information about creating circuits with protection switching.

## 12.5.2 Physical Layer Parameters

The ONS 15600 SDH retrieves the OPR, OPT, and LBC from the line card and stores these values with the PM counts for the 15-minute and 1-day periods. You can retrieve current OPR, OPT, and LBC values for each port by displaying the card view in CTC and clicking the Maintenance > Transceiver tabs.

The physical layer performance parameters consist of normalized and non-normalized values of LBC, OPT, and OPR. Table 12-3 defines the non-normalized values.

*Table 12-3 Non-Normalized Transceiver Physical Optics for the OC-48/STM16, and OC-192/STM64 Cards*

| Parameter | Definition |
|---|---|
| Non-normalized LBC (mA)[1] | The actual operating value of laser bias current (mA) for the specified card port. |
| Non-normalized OPR (dbm)[2] | The actual operating value of optical power received (dBm) for the specified card port. |
| Non-normalized OPT (dbm)[1] | The actual operating value of optical power transmitted (dBm) for the specified card port. |

1. This value should be somewhat consistent from port to port and cannot be configured.

2. This value will vary from port to port because of received optical signal power differences. This value can be configured by calibrating the nominal value to the initial receive power level when the port is put in service.

# 12.6 ASAP Card Performance Monitoring

The following sections define performance monitoring parameters for the Any Service Any Port (ASAP) card.

## 12.6.1 ASAP Card Optical Performance Monitoring Parameters

Table 12-4 lists the near-end and far-end section layer PMs.

*Table 12-4 ASAP Card PMs*

| RS (NE/FE) | MS (NE/FE) | PSC (NE)[1] | PJC (NE)[2] | VC4 and VC4-Xc HP Path (NE)[3] |
|---|---|---|---|---|
| RS-EB | MS-EB | MS-PSC | HP-PPJC-Pdet | HP-BBE |
| RS-ES | MS-ES | MS-PSD | HP-NPJC-Pdet | HP-BBER |
| RS-SES | MS-SES | MS-PSC-W | HP-PPJC-Pgen | HP-EB |
| RS-OFS | MS-OFS | MS-PSD-W | HP-NPJC-Pgen | HP-ES |
| RS-BBE | MS-BBE | | HP-PJCDiff | HP-ESR |
| | | | HP-PJCS-Pdet | HP-SES |
| | | | HP-PJCS-Pgen | HP-SESR |
| | | | | HP-UAS |

1. SDH path performance monitoring parameters increment only if IPPM is enabled. For additional information, see the "12.2 Intermediate-Path Performance Monitoring" section on page 12-2. To monitor SDH path performance monitoring parameters, log into the far-end node directly.

2. In CTC, the count fields for HP-PPJC and HP-NPJC PM parameters appear white and blank unless they are enabled on the Provisioning > Line tab. See the "12.3 Pointer Justification Count" section on page 12-2.

3. SDH path PM parameters do not increment unless IPPM is enabled. See the "12.2 Intermediate-Path Performance Monitoring" section on page 12-2.

# 12.6.2 ASAP Card Ethernet Performance Monitoring Parameters

CTC provides Ethernet performance information, including line-level parameters, port bandwidth consumption, and historical Ethernet statistics. The ASAP card Ethernet performance information is divided into Ether Ports and POS Ports windows within the card view Performance tab window.

## 12.6.2.1 ASAP Card Ether Port Statistics Window

The Ethernet Ether Ports statistics window lists Ethernet parameters at the line level. The Statistics window provides buttons to change the statistical values. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs. The ASAP Statistics window also has a Clear button. The Clear button sets the values on the card to zero, but does not reset the ASAP card.

During each automatic cycle, whether auto-refreshed or manually refreshed (using the Refresh button), statistics are added cumulatively and are not immediately adjusted to equal total received packets until testing ends. To see the final PM count totals, allow a few moments for the PM window statistics to finish testing and update fully. PM counts are also listed in the ASAP card Performance > History window.

Table 12-5 defines the ASAP card statistics parameters.

*Table 12-5      ASAP Ethernet Statistics Parameters*

| Parameter | Meaning |
|---|---|
| Time Last Cleared | A time stamp indicating the last time statistics were reset. |
| Link Status | Indicates whether the Ethernet link is receiving a valid Ethernet signal (carrier) from the attached Ethernet device; up means present, and down means not present. |
| ifInOctets | Number of bytes received since the last counter reset. |
| ifInUcastPkts | Number of unicast packets received since the last counter reset. |
| ifInMulticastPkts | Number of multicast packets received since the last counter reset. |
| ifInBroadcastPkts | Number of broadcast packets received since the last counter reset. |
| 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. Note that for tagged interfaces, this number becomes 1522 bytes. |
| dot3StatsFCSErrors | A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. |
| etherStatsUndersizePkts | The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed. |

*Table 12-5    ASAP Ethernet Statistics Parameters (continued)*

| Parameter | Meaning |
|---|---|
| etherStatsJabbers | The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). |
| dot3StatsAlignmentErrors | A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. |
| ifOutOctets | Number of bytes transmitted since the last counter reset. |
| ifOutUcastPkts | Number of unicast packets transmitted. |
| ifOutMulticastPkts | Number of multicast packets transmitted. |
| ifOutBroadcastPkts | Number of broadcast packets transmitted. |
| etherStatsDropEvents | Number of received frames dropped at the port level. |
| rxPauseFrames | Number of received Ethernet IEEE 802.3z pause frames. |
| txPauseFrames | Number of transmitted IEEE 802.3z pause frames. |
| etherStatsOctets | The total number of bytes of data (including those in bad packets) received on the network (excluding framing bits but including FCS bytes. |
| etherStatsBroadcastPkts | The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets. |
| etherStatsMulticastPkts | The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address. |
| etherStatsFragments | The total number of packets received that were less than 64 bytes in length (excluding framing bits but including FCS bytes) and had either a bad FCS with an integral number of bytes (FCS error) or a bad FCS with a nonintegral number of bytes (alignment error).<br><br>**Note**    It is entirely normal for etherStatsFragments to increment. This is because it counts both runts (which are normal occurrences due to collisions) and noise hits. |
| etherStatsPkts64Octets | The total number of packets (including bad packets) received that were 64 bytes in length (excluding framing bits but including FCS bytes). |
| etherStatsPkts65to127Octets | The total number of packets (including bad packets) received that were between 65 and 127 bytes in length inclusive (excluding framing bits but including FCS bytes). |
| etherStatsPkts128to255Octets | The total number of packets (including bad packets) received that were between 128 and 255 bytes in length inclusive (excluding framing bits but including FCS bytes). |

*Table 12-5*      *ASAP Ethernet Statistics Parameters (continued)*

| Parameter | Meaning |
|---|---|
| etherStatsPkts256to511Octets | The total number of packets (including bad packets) received that were between 256 and 511 bytes in length inclusive (excluding framing bits but including FCS bytes). |
| etherStatsPkts512to1023Octets | The total number of packets (including bad packets) received that were between 512 and 1023 bytes in length inclusive (excluding framing bits but including FCS bytes). |
| etherStatsPkts1024to1518Octets | The total number of packets (including bad packets) received that were between 1024 and 1518 bytes in length inclusive (excluding framing bits but including FCS bytes). |
| ifInDiscards | The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. |
| ifOutDiscards | The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. |
| ifInErrors | The number of inbound packets (or transmission units) that contained errors preventing them from being deliverable to a higher-layer protocol. |
| dot3StatsFrameTooLongs | A count of frames received on a particular interface that exceed the maximum permitted frame size. |
| etherStatsPkts | The total number of packets (including bad packets, broadcast packets, and multicast packets) received. |
| ifOutErrors | The number of outbound packets (or transmission units) that could not be transmitted because of errors. |
| dot3StatsInternalMacTxErrors | A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsFrameTooLongs object, the dot3StatsAlignmentErrors object, or the dot3StatsFCSErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted. |

*Table 12-5 ASAP Ethernet Statistics Parameters (continued)*

| Parameter | Meaning |
|---|---|
| dot3StatsInternalMacRxErrors | A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsFrameTooLongs object, the dot3StatsAlignmentErrors object, or the dot3StatsFCSErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted. |
| dot3StatsSymbolErrors | A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object might represent a count of transmission errors on a particular interface that are not otherwise counted. |

## 12.6.2.2 ASAP Card Ether Ports Utilization Window

The Ether Ports Utilization window shows the percentage of Tx and Rx line bandwidth used by the Ethernet ports during consecutive time segments. The Utilization window provides an Interval menu that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100% interval * maxBaseRate

Tx = (outOctets + outPkts * 20) * 8 / 100% interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the Ethernet port (that is,1 Gbps). Table 12-6 provides the maxBaseRate for ASAP cards.

*Table 12-6 maxBaseRate for VC Circuits*

| VC | maxBaseRate |
|---|---|
| VC3 | 51840000 |
| VC4 | 155000000 |
| VC4-2c | 311000000 |
| VC4-4c | 622000000 |

**Note** Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

## 12.6.2.3  ASAP Card Ether Ports History Window

The Ethernet Ether Ports History window lists past Ethernet statistics for the previous time intervals. The History window displays the statistics for each port for the number of previous time intervals as shown in Table 12-7. The listed parameters are defined in Table 12-5 on page 12-8.

*Table 12-7      Ethernet History Statistics per Time Interval*

| Time Interval | Number of Intervals Displayed |
|---|---|
| 1 minute | 60 previous time intervals |
| 15 minutes | 32 previous time intervals |
| 1 hour | 24 previous time intervals |
| 1 day (24 hours) | 7 previous time intervals |

## 12.6.2.4  ASAP Card POS Ports Statistics Parameters

The Ethernet POS Ports statistics window lists Ethernet POS parameters at the line level.

Table 12-8 defines the ASAP card Ethernet POS Ports parameters.

*Table 12-8      ASAP Card POS Ports Parameters*

| Parameter | Meaning |
|---|---|
| Time Last Cleared | A time stamp indicating the last time statistics were reset. |
| Link Status | Indicates whether the Ethernet link is receiving a valid Ethernet signal (carrier) from the attached Ethernet device; up means present, and down means not present. |
| gfpStatsRxFrame | Number of received GFP frames. |
| gfpStatsTxFrame | Number of transmitted GFP frames. |
| gfpStatsRxOctets | Number of GFP bytes received. |
| gfpStatsTxOctets | Number of GFP bytes transmitted. |
| gfpStatsRxCRCErrors | Number of packets received with a payload FCS error. |
| gfpStatsRxMBitErrors | Sum of all the multiple bit errors. In the GFP CORE HDR at the GFP-T receiver these are uncorrectable. |
| gfpStatsRxSBitErrors | Sum of all the single bit errors. In the GFP CORE HDR at the GFP-T receiver these are correctable. |
| gfpStatsRxTypeInvalid | Number of receive packets dropped due to Client Data Frame UPI error. |
| hdlcInOctets | Number of bytes received (from the SONET/SDH path) prior to the bytes undergoing HLDC decapsulation by the policy engine. |
| hdlcOutOctets | Number of bytes transmitted (to the SONET/SDH path) after the bytes undergoing HLDC encapsulation by the policy engine. |
| rxTotalPkts | Number of received packets. |
| txTotalPkts | Number of transmitted packets |
| hdlcRxAborts | Number of received packets aborted on input. |

*Table 12-8      ASAP Card POS Ports Parameters (continued)*

| Parameter | Meaning |
|---|---|
| mediaIndStatsRxFramesBadCRC | Number of received frames with CRC error. |
| rxPktsDroppedInternalCongestion | Number of received packets dropped due to overflow in frame buffer. |
| mediaIndStatsRxShortPkts | Number of received packets that are too small. |
| mediaIndStatsRxFramesTruncated | Number of received frames with length of 36 bytes or less. |
| mediaIndStatsRxFramesTooLong | Number of received frames that are too long. The maximum is the programmed max frame size (for VSAN support); if the max frame size is set to default, then the max is 2112 byte payload plus 36 byte header, which is 2148. |

## 12.6.2.5  ASAP Card POS Ports Utilization Window

The POS Ports Utilization window shows the percentage of Tx and Rx line bandwidth used by the POS ports during consecutive time segments. The Utilization window provides an Interval menu that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets * 8) / interval * maxBaseRate

Tx = (outOctets * 8) / interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the Ethernet port (that is,1 Gbps). The maxBaseRate for ASAP cards is shown in Table 12-6 on page 12-11.

**Note**    Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

## 12.6.2.6  ASAP Card POS Ports History Window

The Ethernet POS Ports History window lists past Ethernet POS Ports statistics for the previous time intervals. The History window displays the statistics for each port for the number of previous time intervals as shown in Table 12-7. The listed parameters are defined in Table 12-8 on page 12-12.

**12.6.2 ASAP Card Ethernet Performance Monitoring Parameters**

**C H A P T E R 13**

# SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by the Cisco ONS 15600 SDH.

For SNMP setup information, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Chapter topics include:

## 13.1 SNMP Overview

SNMP is an application-layer communication protocol that allows ONS 15600 SDH network devices to exchange management information among these systems and with other devices outside the network. Through SNMP, network administrators can manage network performance, find and solve network problems, and plan network growth. Up to 10 SNMP trap destinations and five concurrent Cisco Transport Controller (CTC) user sessions are allowed per node.

The ONS 15600 SDH uses SNMP for asynchronous event notification to a network management system (NMS). ONS SNMP implementation uses standard Internet Engineering Task Force (IETF) management information bases (MIBs) to convey node-level inventory, fault, and performance management information for SDH read-only management. SNMP allows a generic SNMP manager such as HP OpenView Network Node Manager (NNM) or Open Systems Interconnection (OSI) NetExpert to be utilized for limited management functions.

The Cisco ONS 15600 SDH supports SNMP Version 1 (SNMPv1) and SNMP Version 2c (SNMPv2c). These versions share many features, but SNMPv2c includes additional protocol operations and 64-bit performance monitoring support. This chapter describes both versions and gives SNMP configuration parameters for the ONS 15600 SDH.

**Note**  It is recommended that the SNMP Manager timeout value be set to 60 seconds. Under certain conditions, if this value is lower than the recommended time, the TCC card can reset. However, the response time depends on various parameters such as object being queried, complexity, and number of hops in the node, etc.

**Note**  The CERENT-MSDWDM-MIB.mib, CERENT-FC-MIB.mib, and CERENT-GENERIC-PM-MIB.mib in the CiscoV2 directory support 64-bit performance monitoring counters. The SNMPv1 MIB in the CiscoV1 directory does not contain 64-bit performance monitoring counters, but supports the lower and higher word values of the corresponding 64-bit counter. The other MIB files in the CiscoV1 and CiscoV2 directories are identical in content and differ only in format.

**Note**  When you switch multiplex-section shared protection ring (MS-SPRing) traffic from working to protect, the intermediate path performance monitoring (IPPM) TCAs and SDH near-end path PM values are available on the protect path. The protect TCA and PM values will not be available after the switch is cleared. Note that the protection channel access (PCA) TCAs and PM values are collected when the protect is not active.

Figure 13-1 illustrates the basic layout idea of an SNMP-managed network.

*Figure 13-1*      *Basic Network Managed by SNMP*
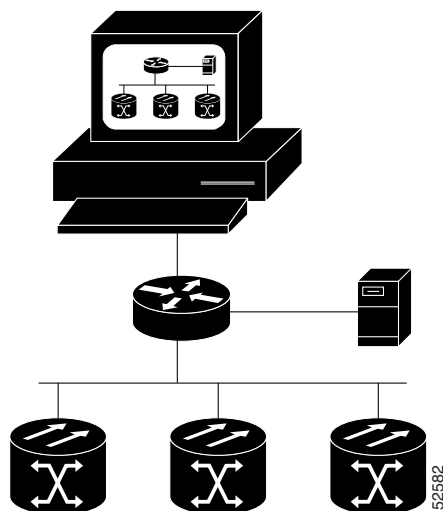


# 13.2  Basic SNMP Components

In general terms, an SNMP-managed network consists of a management system, agents, and managed devices.

A network might be managed by one or several management systems. A management system such as HP OpenView executes monitoring applications and controls managed devices. Management systems execute most of the management processes and provide the bulk of memory resources used for network management. Figure 13-2 illustrates the relationship between the network manager, SNMP agent, and the managed devices.

*Figure 13-2      Example of the Primary SNMP Components*
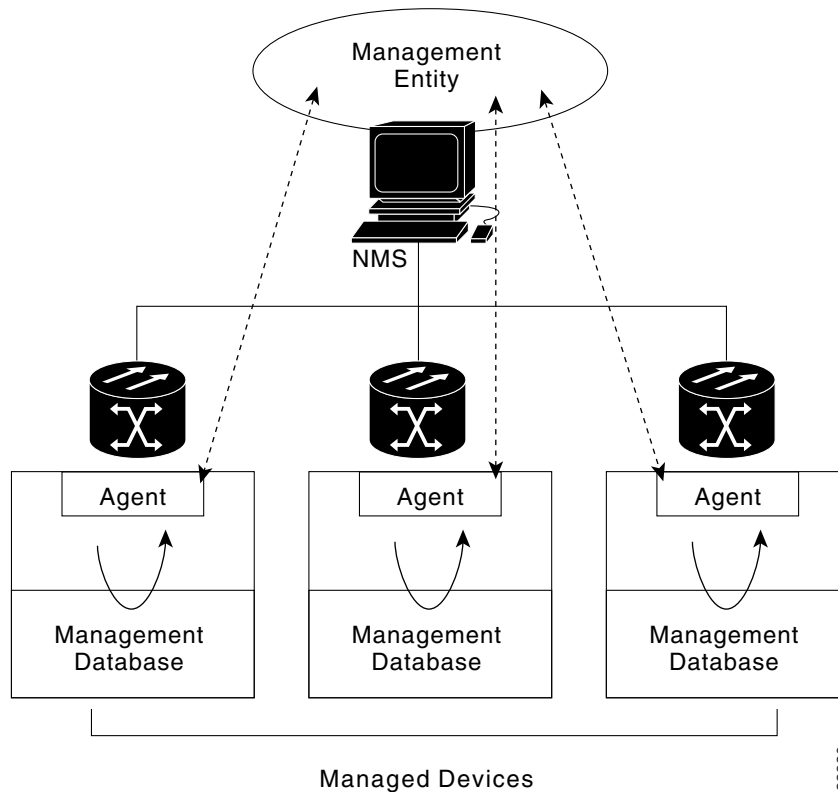


An agent (such as SNMP) residing on each managed device translates local management information data—such as performance information or event and error information—caught in software traps, into a readable form for the management system. Figure 13-3 illustrates SNMP agent get-requests that transport data to the network management software.

*Figure 13-3      Agent Gathering Data from a MIB and Sending Traps to the Manager*
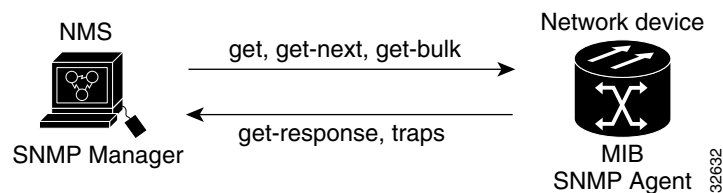


The SNMP agent captures data from MIBs, which are device parameter and network data repositories, or from error or change traps.

A managed element—such as a router, access server, switch, bridge, hub, computer host, or network element (such as an ONS 15600 SDH)—is accessed through the SNMP agent. Managed devices collect and store management information, making it available through SNMP to other management systems having the same protocol compatibility.

# 13.3 SNMP External Interface Requirement

Since all SNMP requests come from a third-party application, the only external interface requirement is that a third-part SNMP client application can upload RFC 3273 SNMP MIB variables in the etherStatsHighCapacityTable, etherHistoryHighCapacityTable, or mediaIndependentTable.

# 13.4 SNMP Version Support

The ONS 15600 SDH supports SNMPv1 and SNMPv2c traps and get requests. The ONS 15600 SDH SNMP MIBs define alarms, traps, and status. Through SNMP, NMS applications can query a management agent for data from functional entities such as Ethernet switches and SDH multiplexers using a supported MIB.

**Note** ONS 15600 SDH MIB files in the CiscoV1 and CiscoV2 directories are almost identical in content except for the difference in 64-bit performance monitoring features. The CiscoV2 directory contains three MIBs with 64-bit performance monitoring counters: CERENT-MSDWDM-MIB.mib, CERENT-FC-MIB.mib, and CERENT-GENERIC-PM-MIB.mib. The CiscoV1 directory does not contain any 64-bit counters, but it does support the lower and higher word values used in 64-bit counters. The two directories also have somewhat different formats.

# 13.5 SNMP Message Types

The ONS 15600 SDH SNMP agent communicates with an SNMP management application using SNMP messages. Table 13-1 describes these messages.

*Table 13-1    ONS 15600 SDH SNMP Message Types*

| Operation | Description |
| --- | --- |
| get-request | Retrieves a value from a specific variable. |
| get-next-request | Retrieves the value following the named variable; this operation is often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable name. The SNMP manager searches sequentially to find the needed variable from within the MIB. |
| get-response | Replies to a get-request, get-next-request, get-bulk-request, or set-request sent by an NMS. |
| get-bulk-request | Fills the get-response with up to the max-repetition number of get-next interactions, similar to a get-next-request. |

*Table 13-1        ONS 15600 SDH SNMP Message Types (continued)*

| Operation | Description |
|-----------|-------------|
| set-request | Provides remote network monitoring (RMON) MIB. |
| trap | Indicates that an event has occurred. An unsolicited message is sent by an SNMP agent to an SNMP manager. |

# 13.6  SNMP Management Information Bases

A managed object, sometimes called a MIB object, is one of many specific characteristics of a managed device. The MIB consists of hierarchically organized object instances (variables) that are accessed by network-management protocols such as SNMP. Section 13.6.1 lists the IETF standard MIBs implemented in the ONS 15600 SDH SNMP agent. Section 13.6.2 lists the proprietary MIBs implemented in the ONS 15600 SDH.

## 13.6.1  IETF-Standard MIBs for ONS 15600 SDH

Table 13-2 lists the IETF-standard MIBs implemented in the ONS 15600 SDH SNMP agents.

First compile the MIBs in Table 13-2. Next, compile the MIBs in the order given in Table 13-3.

⚠ **Caution**    If you do not compile MIBs in the correct order, one or more might not compile correctly.

*Table 13-2        IETF Standard MIBs Implemented in the ONS 15600 SDH System*

| RFC[1] Number | Module Name | Title/Comments |
|-----------|-------------|----------------|
| — | IANAifType-MIB.mib | Internet Assigned Numbers Authority (IANA) ifType |
| 1213 | RFC1213-MIB-rfc1213.mib | Management Information Base for Network |
| 1907 | SNMPV2-MIB-rfc1907.mib | Management of TCP/IP-based Internet: MIB-II Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2) |
| 1253 | RFC1253-MIB-rfc1253.mib | OSPF Version 2 Management Information Base |
| 1493 | BRIDGE-MIB-rfc1493.mib | Definitions of Managed Objects for Bridges (This defines MIB objects for managing MAC bridges based on the IEEE 802.1D-1990 standard between Local Area Network [LAN] segments.) |
| 2819 | RMON-MIB-rfc2819.mib | Remote Network Monitoring Management Information Base |
| 2737 | ENTITY-MIB-rfc2737.mib | Entity MIB (Version 2) |
| 2233 | IF-MIB-rfc2233.mib | Interfaces Group MIB using SNMPv2 |
| 2358 | EtherLike-MIB-rfc2358.mib | Definitions of Managed Objects for the Ethernet-like Interface Types |

*Table 13-2* **IETF Standard MIBs Implemented in the ONS 15600 SDH System (continued)**

| RFC[1] Number | Module Name | Title/Comments |
|---|---|---|
| 2493 | PerfHist-TC-MIB-rfc2493.mib | (Not applicable to the ONS 15600 SDH) Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals |
| 2495 | DS1-MIB-rfc2495.mib | Not applicable to the ONS 15600 SDH |
| 2496 | DS3-MIB-rfc2496.mib | Not applicable to the ONS 15600 SDH |
| 2558 | SDH-MIB-rfc2558.mib | Definitions of Managed Objects for the SONET/SDH Interface Type |
| 2674 | P-BRIDGE-MIB-rfc2674.mib Q-BRIDGE-MIB-rfc2674.mib | Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions |
| 3273 | HC-RMON-MIB | The MIB module for managing RMON device implementations, augmenting the original RMON MIB as specified in RFC 2819 and RFC 1513, and RMON-2 MIB as specified in RFC 2021 |

1. RFC = Request for Comment

## 13.6.2 Proprietary ONS 15600 SDH MIBs

Each ONS 15600 SDH is shipped with a software CD containing applicable proprietary MIBs. The MIBs in Table 13-3 lists the proprietary MIBs for the ONS 15600 SDH.

*Table 13-3* **ONS 15600 SDH Proprietary MIBs**

| MIB Number | Module Name |
|---|---|
| 1 | CERENT-GLOBAL-REGISTRY.mib |
| 2 | CERENT-TC.mib |
| 3 | CERENT-600.mib |
| 4 | CERENT-GENERIC.mib |

**Note** If you cannot compile the proprietary MIBs correctly, log into the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/techsupport or call Cisco TAC (800) 553-2447.

# 13.7 SNMP Trap Content

The ONS 15600 SDH uses SNMP traps to generate all alarms and events, such as raises and clears. The traps contain the following information:

- Object IDs that uniquely identify each event with information about the generating entity (the slot or port; virtual container [VC], or MS-SPRing).

- Severity and service effect of the alarm (Critical [CR], Major [MJ], Minor [MN], or event; Service-Affecting [SA] or Non Service Affecting [NSA]).

• Date and time stamp showing when the alarm occurred.

# 13.7.1 Generic and IETF Traps

Table 13-4 contains information about the generic threshold and performance monitoring MIBs that can be used to monitor any network element (NE) contained in the network. The ONS 15600 SDH supports the generic IETF traps listed in Table 13-4.

*Table 13-4        Supported Generic IETF Traps*

| Trap | From RFC No. MIB | Description |
|------|------------------|-------------|
| coldStart | RFC1213-MIB | Agent up, cold start. |
| warmStart | RFC1213-MIB | Agent up, warm start. |
| entConfigChange | RFC2037/ ENTITY-MIB | The entLastChangeTime value has changed. |

# 13.7.2 Variable Trap Bindings

Each SNMP trap contains variable bindings that are used to create the MIB tables. Variable bindings for the ONS 15600 SDH are listed in Table 13-5. For each group (such as Group A), all traps within the group are associated with all of the group's variable bindings.

*Table 13-5        Supported ONS 15600 SDH SNMPv2 Trap Variable Bindings*

| Group | Associated Trap Name(s) | (Variable Binding Number) | SNMPv2 Variable Bindings | Description |
|-------|-------------------------|---------------------------|--------------------------|-------------|
| A | dsx1LineStatusChange (from RFC 2495, not applicable to ONS 15600 SDH but applicable to other platforms) | (1) | dsx1LineStatus | This variable indicates the line status of the interface. It contains loopback, failure, received alarm and transmitted alarm information. |
| | | (2) | dsx1LineStatusLastChange | The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last proxy-agent re-initialization, the value of this object is zero. |
| | | (3) | cerentGenericNodeTime | The time that an event occurred. |
| | | (4) | cerentGenericAlarmState | The alarm severity and service-affecting status. Severities are Minor (MN), Major (MJ), and Critical (CR). Service-affecting statuses are Service-Affecting (SA) and Non-Service Affecting (NSA). |
| | | (5) | snmpTrapAddress | The address of the SNMP trap. |

*Table 13-5*        *Supported ONS 15600 SDH SNMPv2 Trap Variable Bindings (continued)*

| Group | Associated Trap Name(s) | (Variable Binding Number) | SNMPv2 Variable Bindings | Description |
|---|---|---|---|---|
| B | dsx3LineStatusChange (from RFC 2496, not applicable to ONS 15600 SDH but applicable to other platforms) | (1) | dsx3LineStatus | This variable indicates the line status of the interface. It contains loopback state information and failure state information. |
| | | (2) | dsx3LineStatusLastChange | The value of MIB II's sysUpTime object at the time this DS3/E3 entered its current line status state. If the current state was entered prior to the last reinitialization of the proxy-agent, then the value is zero. |
| | | (3) | cerentGenericNodeTime | The time that an event occurred. |
| | | (4) | cerentGenericAlarmState | The alarm severity and service-affecting status. Severities are Minor (MN), Major (MJ), and Critical (CR). Service-affecting statuses are Service-Affecting and Non-Service Affecting. |
| | | (5) | snmpTrapAddress | The address of the SNMP trap. |
| C | coldStart (from RFC 1907) | (1) | cerentGenericNodeTime | The time that an event occurred. |
| | warmStart (from RFC 1907) | (2) | cerentGenericAlarmState | The alarm severity and service-affecting status. Severities are Minor (MN), Major (MJ), and Critical (CR). Service-affecting statuses are Service-Affecting (SA) and Non-Service Affecting (NSA). |
| | newRoot (from RFC) | (3) | snmpTrapAddress | The address of the SNMP trap (not supported for ONS 15600 SDH). |
| | topologyChange (from RFC) | — | — | (Not supported for ONS 15600 SDH) |
| | entConfigChange (from RFC 2737) | — | — | — |
| | authenticationFailure (from RFC 1907) | — | — | — |

*Table 13-5* **Supported ONS 15600 SDH SNMPv2 Trap Variable Bindings (continued)**

| Group | Associated Trap Name(s) | (Variable Binding Number) | SNMPv2 Variable Bindings | Description |
|-------|------------------------|---------------------------|--------------------------|-------------|
| D | failureDetectedExternal ToTheNE (from CERENT-600-mib) | (1) | cerentGenericNodeTime | The time that an event occurred. |
| | | (2) | cerentGenericAlarmState | The alarm severity and service-affecting status. Severities are Minor (MN), Major (MJ), and Critical (CR). Service-affecting statuses are Service-Affecting (SA) and Non-Service Affecting (NSA). |
| | | (3) | cerentGenericAlarmObject Type | The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm. |
| | | (4) | cerentGenericAlarmObject Index | Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table. |
| | | (5) | cerentGenericAlarmSlot Number | The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero. |
| | | (6) | cerentGenericAlarmPort Number | The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero. |
| | | (7) | cerentGenericAlarmLine Number | The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero. |
| | | (8) | cerentGenericAlarmObject Name | The TL1-style user-visible name that uniquely identifies an object in the system. |
| | | (9) | cerentGenericAlarm AdditionalInfo | Additional information for the alarm object. In the current version of the MIB, this object contains provisioned description for alarms that are external to the NE. If there is no additional information, the value is zero. |
| | | (10) | snmpTrapAddress | The address of the SNMP trap. |

*Table 13-5* *Supported ONS 15600 SDH SNMPv2 Trap Variable Bindings (continued)*

| Group | Associated Trap Name(s) | (Variable Binding Number) | SNMPv2 Variable Bindings | Description |
|---|---|---|---|---|
| E | performanceMonitorThresholdCrossingAlert (from CERENT-600-mib) | (1) | cerentGenericNodeTime | The time that an event occurred. |
| | | (2) | cerentGenericAlarmState | The alarm severity and service-affecting status. Severities are Minor (MN), Major (MJ), and Critical (CR). Service-affecting statuses are Service-Affecting (SA) and Non-Service Affecting (NSA). |
| | | (3) | cerentGenericAlarmObjectType | The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm. |
| | | (4) | cerentGenericAlarmObjectIndex | Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table. |
| | | (5) | cerentGenericAlarmSlotNumber | The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero. |
| | | (6) | cerentGenericAlarmPortNumber | The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero. |
| | | (7) | cerentGenericAlarmLineNumber | The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero. |
| | | (8) | cerentGenericAlarmObjectName | The TL1-style user-visible name that uniquely identifies an object in the system. |
| | | (9) | cerentGenericThresholdMonitorType | This object indicates the type of metric being monitored. |
| | | (10) | cerentGenericThresholdLocation | Indicates whether the event occurred at the near or far end. |
| | | (11) | cerentGenericThresholdPeriod | Indicates the sampling interval period. |
| | | (12) | cerentGenericThresholdSetValue | The value of this object is the threshold provisioned by the NMS. |
| | | (13) | cerentGenericThresholdCurrentValue | — |
| | | (14) | cerentGenericThresholdDetectType | — |
| | | (15) | snmpTrapAddress | The address of the SNMP trap. |

*Table 13-5* *Supported ONS 15600 SDH SNMPv2 Trap Variable Bindings (continued)*

| Group | Associated Trap Name(s) | (Variable Binding Number) | SNMPv2 Variable Bindings | Description |
|---|---|---|---|---|
| F | All other traps (from CERENT-600-MIB) not listed above | (1) | cerentGenericNodeTime | The time that an event occurred. |
| | | (2) | cerentGenericAlarmState | The alarm severity and service-affecting status. Severities are Minor (MN), Major (MJ), and Critical (CR). Service-affecting statuses are Service-Affecting (SA) and Non-Service Affecting (NSA). |
| | | (3) | cerentGenericAlarmObject Type | The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm. |
| | | (4) | cerentGenericAlarmObject Index | Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table. |
| | | (5) | cerentGenericAalrmSlot Number | The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero. |
| | | (6) | cerentGenericAlarmPort Number | The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero. |
| | | (7) | cerentGenericAlarmLine Number | The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero. |
| | | (8) | cerentGenericAlarmObject Name | The TL1-style user-visible name that uniquely identifies an object in the system. |
| | | (9) | snmpTrapAddress | The address of the SNMP trap. |

# 13.8 Proxy Over Firewalls

SNMP and NMS applications have traditionally been unable to cross firewalls used for isolating security risks inside or outside networks. CTC enables network operations centers (NOCs) to access performance monitoring data such as remote monitoring (RMON) statistics or autonomous messages across firewalls by using an SNMP proxy element installed on a firewall.

The application-level proxy transports SNMP protocol data units (PDU) between the NMS and NEs, allowing requests and responses between the NMS and NEs and forwarding NE autonomous messages to the NMS. The proxy agent requires little provisioning at the NOC and no additional provisioning at the NEs.

The firewall proxy is intended for use in a gateway network element-end network element (GNE-ENE) topology with many NEs through a single NE gateway. Up to 64 SNMP requests (such as get, getnext, or getbulk) are supported at any time behind single or multiple firewalls. The proxy interoperates with common NMS such as HP OpenView.

For security reasons, the SNMP proxy feature must be enabled at all receiving and transmitting NEs to function. For instructions to do this, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

# 13.9  Remote Monitoring

The ONS 15600 SDH incorporates RMON to allow network operators to monitor Ethernet facility performance and events. Software Releases 7.0 and later provide remote data communications channel (DCC) monitoring using 64-bit RMON over the DCC to gather historical and statistical Ethernet data. In general, the ONS 15600 SDH system RMON is based on the IETF-standard MIB RFC 2819 and includes the following five groups from the standard MIB: Ethernet Statistics, History Control, Ethernet History, Alarm, and Event.

✎ **Note**    Typical RMON operations, other than threshold provisioning, are invisible to the CTC user.

## 13.9.1  64-Bit RMON Monitoring over DCC

The ONS 15600 SDH DCC is implemented over the IP protocol, which is not compatible with Ethernet. The system monitors Ethernet equipment history and statistics using RMON. RMON DCC monitoring for IP and Ethernet is used to check the health of remote DCC connections.

RMON DCC contains two MIBs for DCC interfaces. They are:

- cMediaIndependentTable—Standard, RFC 3273; the proprietary extension of the HC-RMON MIB used for reporting statistics
- cMediaIndependentHistoryTable—Proprietary MIB used to support history

### 13.9.1.1  Row Creation in MediaIndependentTable

The mediaIndependentTable is created automatically when the Ethernet facility is created on the ONS 15600 SDH ASAP card.

### 13.9.1.2  Row Creation in cMediaIndependentHistoryControlTable

SNMP row creation and deletion for the cMediaIndependentHistoryControlTable follows the same processes as for the MediaIndependentTable; only the variables differ.

In order to create a row, the SetRequest PDU should contain the following:

- cMediaIndependentHistoryControlDataSource and its desired value
- cMediaIndependentHistoryControlOwner and its desired value
- cMediaIndependentHistoryControlStatus with a value of createRequest (2)

## 13.9.2  HC-RMON-MIB Support

For the ONS 15600 SDH, the implementation of the high-capacity remote monitoring information base (HC-RMON-MIB, or RFC 3273) enables 64-bit support of existing RMON tables. This support is provided with the etherStatsHighCapacityTable and the etherHistoryHighCapacityTable. An additional table, the mediaIndependentTable, and an additional object, hcRMONCapabilities, are also added for

this support. All of these elements are accessible by any third-party SNMP client should have the ability to upload RFC 3273 SNMP MIB variables in the etherStatsHighCapacityTable, etherHistoryHighCapacityTable, or mediaIndependentTable.

# 13.9.3 Ethernet Statistics RMON Group

The Ethernet Statistics group contains the basic statistics monitored for each subnetwork in a single table called the etherStatsTable.

## 13.9.3.1 Row Creation in etherStatsTable

The SetRequest PDU for creating a row in this table should contain all the values needed to activate a row in a single set operation, and an assigned status variable to createRequest. The SetRequest PDU object ID (OID) entries must all carry an instance value, or type OID, of 0.

In order to create a row, the SetRequest PDU should contain the following:

- The etherStatsDataSource and its desired value
- The etherStatsOwner and its desired value (size of this value is limited to 32 characters)
- The etherStatsStatus with a value of createRequest (2)

The etherStatsTable creates a row if the SetRequest PDU is valid according to the above rules. When the row is created, the SNMP agent decides the value of etherStatsIndex. This value is not sequentially allotted or contiguously numbered. It changes when an Ethernet interface is added or deleted. The newly created row will have etherStatsStatus value of valid (1).

If the etherStatsTable row already exists, or if the SetRequest PDU values are insufficient or do not make sense, the SNMP agent returns an error code.

**Note** EtherStatsTable entries are not preserved if the SNMP agent is restarted.

## 13.9.3.2 Get Requests and GetNext Requests

Get requests and getNext requests for the etherStatsMulticastPkts and etherStatsBroadcastPkts columns return a value of zero because the variables are not supported by ONS 15600 SDH Ethernet facilities.

## 13.9.3.3 Row Deletion in etherStatsTable

To delete a row in the etherStatsTable, the SetRequest PDU should contain an etherStatsStatus value of 4 (invalid). The OID marks the row for deletion. If required, a deleted row can be recreated.

# 13.9.4 History Control RMON Group

The History Control group defines sampling functions for one or more monitor interfaces in the historyControlTable. The values in this table, as specified in RFC 2819, are derived from the historyControlTable and etherHistoryTable.

### 13.9.4.1 History Control Table

The RMON is sampled at one of four possible intervals. Each interval, or period, contains specific history values (also called buckets). Table 13-6 lists the four sampling periods and corresponding buckets.

The historyControlTable maximum row size is determined by multiplying the number of ports on a card by the number of sampling periods.

*Table 13-6        RMON History Control Periods and History Categories*

| Sampling Periods (historyControlValue Variable) | Total Values, or Buckets (historyControl Variable) |
|---|---|
| 15 minutes | 32 |
| 24 hours | 7 |
| 1 minute | 60 |
| 60 minutes | 24 |

### 13.9.4.2 Row Creation in historyControlTable

The etherStats table and historyControl table are automatically created when the Ethernet facility is created. History size is based upon the default history bucket located in Table 13-6.

### 13.9.4.3 Get Requests and GetNext Requests

These PDUs are not restricted.

### 13.9.4.4 Row Deletion in historyControl Table

To delete a row from the table, the SetRequest PDU should contain a historyControlStatus value of 4 (invalid). A deleted row can be recreated.

### 13.9.4.5 Ethernet History RMON Group

The ONS 15600 SDH implements the etherHistoryTable as defined in RFC 2819. The group is created within the bounds of the historyControlTable and does not deviate from the RFC in its design.

### 13.9.4.6 64-Bit etherHistoryHighCapacityTable

64-bit Ethernet history for the HC-RMON-MIB is implemented in the etherHistoryHighCapacityTable, which is an extension of the etherHistoryTable. The etherHistoryHighCapacityTable adds four columns for 64-bit performance monitoring data. These two tables have a one-to-one relationship. Adding or deleting a row in one table will effect the same change in the other.

# 13.9.5 Alarm RMON Group

The Alarm group consists of the alarmTable, which periodically compares sampled values with configured thresholds and raises an event if a threshold is crossed. This group requires the implementation of the event group, which follows this section.

## 13.9.5.1 Alarm Table

The NMS uses the alarmTable to determine and provision network performance alarmable thresholds.

## 13.9.5.2 Get Requests and GetNext Requests

These PDUs are not restricted.

## 13.9.5.3 Row Deletion in alarmTable

To delete a row from the table, the SetRequest PDU should contain an alarmStatus value of 4 (invalid). A deleted row can be recreated. Entries in this table are preserved if the SNMP agent is restarted.

# 13.9.6 Event RMON Group

The event group controls event generation and notification. It consists of two tables: the eventTable, which is a read-only list of events to be generated, and the logTable, which is a writable set of data describing a logged event. The ONS 15600 SDH implements the logTable as specified in RFC 2819.

## 13.9.6.1 Event Table

The eventTable is read-only and unprovisionable. The table contains one row for rising alarms and another for falling ones. This table has the following restrictions:

- The eventType is always "log-and-trap (4)".
- The eventCommunity value is always a zero-length string, indicating that this event causes the trap to be sent to all provisioned destinations.
- The eventOwner column value is always "monitor."
- The eventStatus column value is always "valid(1)".

## 13.9.6.2 Log Table

The logTable is implemented exactly as specified in RFC 2819. The logTable is based upon data that is locally cached in a controller card. If there is a controller card protection switch, the existing logTable is cleared and a new one is started on the newly active controller card. The table contains as many rows as provided by the alarm controller.

# Hardware Specifications

This appendix provides detailed shelf assembly hardware specifications for the Cisco ONS 15600 SDH. It includes the following sections:

# A.1 Shelf Specifications

This section provides bandwidth specifications; slot assignments; lists of cards and topologies; shelf dimensions; Cisco Transport Controller (CTC) specifications; the LAN, TL1, modem, and alarm interface specifications; and timing, database, environmental, and power specifications.

## A.1.1 Bandwidth

The ONS 15600 SDH has the following bandwidth specifications:

- Total bandwidth: 320 Gbps
- Optical bandwidth: 40 Gbps per slot

## A.1.2 Slot Assignments

The ONS 15600 SDH has the following slot assignments:

- Total card slots: 14
- Optical cards: Slots 1 to 4, 11 to 14
- TSC: Slots 5, 10
- SSXC: Slots 6/7, 8/9

## A.1.3 Cards

The ONS 15600 SDH has the following cards:

- TSC

- SSXC
- ASAP
- OC48/STM16 LR16 1550
- OC48/STM16 SR16 1310
- OC192/STM64 LR4 1550
- OC192/STM64 SR4 1310
- OC192/STM64 4 Port ITU C-Band

# A.1.4  Configurations

The ONS 15600 SDH has the following configurations:

- 1+1 automatic protections switching (APS) for point-to-point and linear configurations
- Two-fiber subnetwork connection protection ring (SNCP)
- Path-protected mesh network (PPMN)
- Two-fiber multiplex section-shared protection ring (MS-SPRing)
- Four-fiber multiplex section-shared protection ring (MS-SPRing)
- Unprotected

# A.1.5  Dimensions

The ONS 15600 SDH has the following dimensions:

- Height: 83.9 inches (2130 mm)
- Width: 23.6 inches (600 mm)
- Depth: 23.6 inches (600 mm)
- Weight: 500 lb (226.8 kg) (without cards)

# A.1.6  Cisco Transport Controller

CTC has the following specifications:

- 10/100BaseT
- TSC access: RJ-45 connector
- Backplane access: RJ-45 connector

# A.1.7  External LAN Interface

The external LAN interface has the following specifications:

- 10/100BaseT Ethernet
- Backplane access: RJ-45 connector

# A.1.8 TL1 Craft Interface

The TL1 craft interface has the following specifications:

- Speed: 9600 bps
- Backplane (CAP/CAP2) access: EIA/TIA-232 DB-9 type connector

# A.1.9 Modem Interface

The modem interface has the following specifications:

- Hardware flow control
- Backplane (CAP/CAP2) access: EIA/TIA-232 DB-9 type connector

# A.1.10 Alarm Interface

The alarm interface has the following specifications:

- Visual: Critical, Major, Minor, Remote
- Audible: Critical, Major, Minor, Remote
- Alarm contacts: 0.045 mm, –48 VDC, 50 mA
- Backplane (CAP/CAP2) access: Alarm pin fields

# A.1.11 BITS Interface

The building integrated timing supply (BITS) interface has the following specifications:

- 2 DS-1 BITS inputs
- 2 derived STM-N outputs

# A.1.12 System Timing

The ONS 15600 SDH has the following system timing specifications:

- Holdover stability: Stratum 3E per Telcordia GR-253-CORE
- Free running accuracy: +/– 4.6 ppm
- Reference: External BITS, line, internal

# A.1.13 Database Storage

The ONS 15600 SDH has the following database storage specifications:

- Nonvolatile memory: 512 MB, IDE FLASH memory

# A.1.14 Environmental Specifications

The ONS 15600 SDH has the following environmental specifications:

- Operating temperature: 23 to 122 degrees Fahrenheit (–5 to +50 degrees Celsius)
- Operating humidity: 5 to 95 percent, noncondensing

# A.1.15 Power Specifications

The ONS 15600 SDH has the following power specifications:

- Input voltage: –48 VDC
- Input current: 80 A per channel (six channels provided)
- Power terminals: Lug

Table A-1 lists the power requirements for each card.

*Table A-1      Power Requirements for Individual Cards*

| Card Type | Card Name | Watts |
|---|---|---|
| Control Cards | TSC | 58 |
| | SSXC | 165 |
| Optical Cards | OC48/STM16 LR16 1550 | 170 |
| | OC48/STM16 SR16 1310 | 180 |
| | OC192/STM64 LR4 1550 | 180 |
| | OC192/STM64 SR4 1310 | 165 |
| | OC192/STM64 4 Port ITU C-Band | 180 |
| Multifunction Cards | ASAP | 170 |

Table A-2 lists the power requirements for an individual fan in the fan-tray assembly.

*Table A-2      Power Requirements for Individual Fans*

| Condition | Watts | Amps | BTU/Hr. |
|---|---|---|---|
| Minimum. at 48 V (ambient temperature less than 25 degrees Celsius (77 degrees Fahrenheit) | 12 | 0.25 | 41 |
| Maximum at 48 V (ambient temperature greater than 25 degrees Celsius (77 degrees Fahrenheit) | 46 | 0.95 | 157 |

# A.2 Card Specifications

This section provides specifications for the following cards:

- TSC
- SSXC

- OC48/STM16 LR/LH 16 Port 1550

- OC48/STM16 SR/SH 16 Port 1310

- OC192/STM64 LR/LH 4 Port 1550

- OC192/STM64 SR/SH 4 Port 1310

- OC192/STM64 4 Port ITU C-BandASAP

- Filler

# A.2.1 TSC Card Specifications

Table A-3 shows the TSC card specifications.

*Table A-3       TSC Card Specifications*

| Specification Type | Description |
|---|---|
| CTC software | Interface: 10/100BaseT LAN |
| | Backplane (CAP/CAP2) access: RJ-45 |
| TL1 craft interface | Speed: 10/100BaseT LAN |
| | Front panel access: RJ-45 type connector |
| | Backplane access: RJ-45 and EIA/TIA-232 DB-9 type connector |
| Synchronization | Stratum 3E, per Telcordia GR-1244 |
| | Free running access: Accuracy 4.6 ppm |
| | Holdover stability: 3.7 x$10^{-7}$ ppm/day including temperature (< 255 slips in first 24 hours) |
| | Reference: External BITS, line, internal |
| Operating temperature | 23 to 122 degrees Fahrenheit (–5 to +50 degrees Celsius) |
| Operating humidity | 5 to 95 percent, noncondensing |
| Dimensions | Height: 16.50 in. (419 mm) |
| | Width: 1.10 in. (28 mm) |
| | Depth: 18.31 in. (465 mm) |
| | Card weight: 4.0 lb (1.81 kg) |
| Compliance | When installed in a node, ONS 15600 SDH cards comply with these safety standards: UL 60950, CSA C22.2 No. 950, EN 60950, IEC 60950 |

# A.2.2  SSXC Specifications

Table A-4 shows the SSXC card specifications.

*Table A-4*        *SSXC Card Specifications*

| Specification Type | Description |
|---|---|
| Cross-connect | Connection setup time: 7 microseconds |
| | Latency: 0.5 microseconds |
| Operating temperature | 23 to 122 degrees Fahrenheit (–5 to +50 degrees Celsius) |
| Operating humidity | 5 to 95 percent, noncondensing |
| Dimensions | Height: 16.50 in. (419 mm) |
| | Width: 2.36 in. (60 mm) |
| | Depth: 18.31 in. (465 mm) |
| | Card weight: 5.0 lb (2.27 kg) |
| Compliance | When installed in a node, ONS 15600 SDH cards comply with these safety standards: UL 60950, CSA C22.2 No. 950, EN 60950, IEC 60950 |

# A.2.3  OC48/STM16 LR/LH 16 Port 1550 Specifications

Table A-5 shows the OC48/STM16 LR/LH 16 Port 1550 card specifications.

*Table A-5*        *OC48/STM16 LR/LH 16 Port 1550 Card Specifications*

| Specification Type | Description |
|---|---|
| Line | Bit rate: 2.49 Gbps |
| | Code: Scrambled nonreturn to zero (NRZ) |
| | Fiber: 1550 nm single-mode |
| | Loopback mode: Facility |
| | Connectors: OGI |
| | Compliance: Telcordia GR-253 |
| Transmitter | Max. transmitter output power: +3 dBm |
| | Min. transmitter output power: –2 dBm |
| | Center wavelength: 1500 nm to 1580 nm |
| | Nominal wavelength: 1550 nm |
| | Transmitter: Distributed feedback (DFB) laser |
| | **Note**  The CTC Maintenance > Transceiver tab shows the optical power transmitted (OPT) levels. CTC might show OPT levels at 1 dBm greater or less than the actual card OPT level. |

*Table A-5* **OC48/STM16 LR/LH 16 Port 1550 Card Specifications (continued)**

| Specification Type | Description |
|---|---|
| Receiver | Max. receiver level: –9 dBm |
| | Min. receiver level: –28 dBm |
| | Receiver: InGaAs Avalanche Photo Diode (APD) photo detector |
| | Link loss budget: 26 dB minimum, with 1 dBm dispersion penalty |
| Loopback mode | Facility (Line) |
| | **Note** Use a 19 to 24 dBm fiber attenuator (15 to 20 dBm is recommended) when connecting a fiber loopback to an OC48/STM16 LR/LH 16 Port 1550 card. Never connect a direct fiber loopback. |
| Operating temperature | 23 to 122 degrees Fahrenheit (–5 to +50 degrees Celsius) |
| Operating humidity | 5 to 95 percent, noncondensing |
| Dimensions | Height: 16.50 in. (419 mm) |
| | Width: 1.50 in. (38 mm) |
| | Depth: 18.31 in. (465 mm) |
| | Card weight: 5.0 lb (2.27 kg) |
| Compliance | Telcordia GR-253 |
| | When installed in a node, ONS 15600 SDH cards comply with these safety standards: UL 60950, CSA C22.2 No. 950, EN 60950, IEC 60950 |
| | Eye safety compliance: Class 1 (21 CFR 1040.10 and 1040.11) and Class 1 (IEC 60825) laser products |

## A.2.4  OC48/STM16 SR/SH 16 Port 1310 Specifications

Table A-6 shows the OC48/STM16 SR/SH 16 Port 1310 card specifications.

*Table A-6*　　*OC48/STM16 SR/SH 16 Port 1310 Card Specifications*

| Specification Type | Description |
|---|---|
| Line | Bit rate: 2.49 Gbps |
| | Code: Scrambled NRZ |
| | Fiber: 1310 nm single-mode |
| | Loopback mode: Facility |
| | Connectors: OGI |
| | Compliance: Telcordia GR-253 |
| Transmitter | Max. transmitter output power: –3 dBm |
| | Min. transmitter output power: –10 dBm |
| | Center wavelength: 1266 nm to 1360 nm |
| | Nominal wavelength: 1310 nm |
| | Transmitter: Fabry Perot laser |
| | **Note**　The CTC Maintenance > Transceiver tab shows the OPT levels. CTC might show OPT levels at 1 dBm greater or less than the actual card OPT level. |
| Receiver | Max. receiver level: –3 dBm |
| | Min. receiver level: –18 dBm |
| | Receiver: Positive-intrinsic-negative (PIN) diode |
| | Link loss budget: 8 dBm min., with 1 dBm dispersion penalty |
| Loopback mode | Facility (Line) |
| | **Note**　You must use a 3-dBm fiber attenuator when connecting a fiber loopback to an OC48/STM16 SR/SH 16 port 1310 card. Never connect a direct fiber loopback. |
| Operating temperature | 23 to 122 degrees Fahrenheit (–5 to +50 degrees Celsius) |
| Operating humidity | 5 to 95 percent, noncondensing |
| Dimensions | Height: 16.50 in. (419 mm) |
| | Width: 1.50 in. (38 mm) |
| | Depth: 18.31 in. (465 mm) |
| | Card weight: 5.0 lb (2.27 kg) |
| Compliance | Telcordia GR-253 |
| | When installed in a node, ONS 15600 SDH cards comply with these safety standards: UL 60950, CSA C22.2 No. 950, EN 60950, IEC 60950 |
| | Eye safety compliance: Class 1 (21 CFR 1040.10 and 1040.11) and Class 1 (IEC 60825) laser products |

## A.2.5  OC192/STM64 LR/LH 4 Port 1550 Specifications

Table A-7 shows the OC192/STM64 LR/LH 4 Port 1550 card specifications.

***Table A-7***      ***OC192/STM64 LR/LH 4 Port 1550 Card Specifications***

| Specification Type | Description |
|---|---|
| Line | Bit rate: 9.96 Gbps |
| | Code: Scrambled NRZ |
| | Fiber: 1550 nm single mode |
| Transmitter | Max. transmitter output power: +7 dBm |
| | Min. transmitter output power: +4 dBm |
| | Center wavelength: 1530 nm to 1565 nm |
| | Nominal wavelength: 1550 nm |
| | Transmitter: Lithium niobate (LN) external modulator transmitter |
| Receiver | Max. receiver level: –9 dBm |
| | Min. receiver level: –22 dBm |
| | Receiver: APD/TIA |
| | Link loss budget: 24 dB min., with no dispersion or 22 dB optical path loss at BER = $1^{-12}$ including dispersion |
| Loopback mode | Payload |
| | **Note**    Use a 19 to 24 dB fiber attenuator (15 to 20 is recommended) when connecting a fiber loopback to an OC192/STM64 LR/LH 4 Port 1550 card. Never connect a direct fiber loopback. |
| Connectors | OGI |
| Operating temperature | 23 to 122 degrees Fahrenheit (–5 to +50 degrees Celsius) |
| Operating humidity | 5 to 95 percent, noncondensing |
| Dimensions | Height: 16.50 in. (419 mm) |
| | Width: 1.50 in. (38 mm) |
| | Depth: 18.31 in. (465 mm) |
| | Card weight: 12.0 lb (5.44 kg) |
| Compliance | Telcordia GR-253 |
| | When installed in a node, ONS 15600 SDH cards comply with these safety standards: UL 60950, CSA C22.2 No. 950, EN 60950, IEC 60950 |
| | Eye safety compliance: Class 1 (21 CFR 1040.10 and 1040.11) and Class 1 (IEC 60825) laser products |

## A.2.6 OC192/STM64 SR/SH 4 Port 1310 Specifications

Table A-8 shows the OC192/STM64 SR/SH 4 Port 1310 card specifications.

*Table A-8      OC192/STM64 SR/SH 4 Port 1310 Card Specifications*

| Specification Type | Description |
|---|---|
| Line | Bit rate: 9.96 Gbps |
| | Code: Scrambled NRZ |
| | Fiber: 1310 nm single mode |
| Transmitter | Max. transmitter output power: –1 dBm |
| | Min. transmitter output power: –6 dBm |
| | Center wavelength: 1290 nm to 1330 nm |
| | Nominal wavelength: 1310 nm |
| Receiver | Max. receiver level: –1 dBm |
| | Min. receiver level: –11 dBm |
| | Link loss budget: –5 dB min., with no dispersion or 4 dB optical path loss at BER = $1^{-12}$ including dispersion |
| Loopback mode | Payload |
| | **Note** You must use a 3-dBm fiber attenuator when connecting a fiber loopback to an OC192/STM64 SR/SH 4 Port 1310 card. Never connect a direct fiber loopback. |
| Connectors | OGI |
| Operating temperature | 23 to 122 degrees Fahrenheit (–5 to +50 degrees Celsius) |
| Operating humidity | 5 to 95 percent, noncondensing |
| Dimensions | Height: 16.50 in. (419 mm) |
| | Width: 1.50 in. (38 mm) |
| | Depth: 18.31 in. (465 mm) |
| | Card weight: 12.0 lb (5.44 kg) |
| Compliance | Telcordia GR-253 |
| | When installed in a node, ONS 15600 SDH cards comply with these safety standards: UL 60950, CSA C22.2 No. 950, EN 60950, IEC 60950 |
| | Eye safety compliance: Class 1 (21 CFR 1040.10 and 1040.11) and Class 1 (IEC 60825) laser products |

## A.2.7 ASAP Specifications

Table A-9 shows the ASAP card specifications.

*Table A-9*        *ASAP Card Specifications*

| Specification Type | Description |
|---|---|
| Carrier Card (CC) | Contains slots for four pluggable ASAP I/O cards, which can be used to provide a variety of optical line interfaces. The CC provides 4 electrical VC4-16c or Gigabit Ethernet signals to each ASAP I/O card (for 16 total) and 16 redundant electrical VC4-16c matrix interfaces to the backplane. For SDH interfaces, the CC card provides pointer processing and overhead extraction/insertion. |
| 4PIO Pluggable I/O card | The ASAP 4PIO module is a four-port multirate optical interface card. It has four slots for Small Form-factor Pluggable (SFP) optics. The four ports can be provisioned on a per-port basis as STM-1, STM-4, STM-16, or Gigabit Ethernet interfaces. |
| 1PIO Pluggable I/O card | The ASAP 1PIO module is a single-port single-rate optical interface card. It has one slot for XFP optics. The port can be provisioned for one STM-64 interface. |
| Payloads | Nonconcatenated and/or concatenated payloads at VC3, VC4, VC4-2c, VC4-3c, VC4-4c, VC4-8c, VC4-16c, and VC4-64c are supported. For Gigabit Ethernet interfaces, Layer 1 Ethernet transport is also implemented. |
| SFP support | ONS-SE-Z1: Supports STM-1 SR-1, STM-4 SR-1, STM-16 IR-1 or GE LX |
| | ONS-SI-155-L2: Supports STM-1 LR-2 |
| | ONS-SI-622-L2: Supports STM-4 LR-2 |
| | ONS-SE-2G-L2: Supports STM-16 LR-2 |
| | ONS-SI-2G-S1: Supports STM-16, LR-2 |
| XFP support | ONS-XC-10G-S1: Supports STM-64 SR-1 |
| | ONS-XC-10G-L2: Supports STM-64 LR-2 |
| Connectors | Up to 16 SFP connectors (4 per 4PIO module) or 4 XFP connectors (1 per 1PIO module), at front edge of card |
| Power | 130 W to 180 W (maximum) |
| Operating temperature | 23 to 131 degrees Fahrenheit (–5 to +55 degrees Celsius) |
| Operating humidity | 5 to 95 percent, noncondensing |
| Dimensions | Height: 16.50 in. (419 mm) |
| | Width: 1.50 in. (38 mm) |
| | Depth: 18.31 in. (465 mm) |
| | Card weight: approximately 6 pound = 2.72155422 kilograms |
| Compliance | Telcordia GR-253 |
| | When installed in a system, ONS 15600 SDH cards comply with these safety standards: UL 60950, CSA C22.2 No. 950, EN 60950, IEC 60950 |
| | Eye safety compliance: Class 1 (21 CFR 1040.10 and 1040.11) and Class 1 (IEC 60825) laser products |

## A.2.8  Filler Card Specifications

Table A-10 shows the Filler card specifications.

*Table A-10      Filler Card Specifications*

| Specification Type | Description |
|---|---|
| Dimensions | Height: 16.50 in. (419 mm) |
| | Width:1.50 in. (38 mm) |
| | Depth: 18.31 in. (465 mm) |
| | Card weight: 2.5 lb (1.134 kg) |

# A.3  SFP/XFP Specifications

Table A-11 and Table A-12 list the specifications for Cisco ONS 15600 SDH SFPs and XFPs.

*Table A-11      SFP Specifications (4PIO Only)*

| SFP Product ID | Interface | Transmitter Output Power Min/Max (dBm) | Receiver Input Power Min/Max (dBm) |
|---|---|---|---|
| ONS-SI-622-L2 | OC-12, STM-4 | –3.0 to 2.0 | –28 to –8 |
| ONS-SI-155-L2 | OC-3, STM-1 | –5.0 to 0.0 | –34 to –10 |
| ONS-SE-2G-L2 | OC-48, STM-16 | –2.0 to 3.0 | –28 to –9 |
| ONS-SE-Z1 | OC-3, STM-1, OC-12, STM-4, OC-48, STM -16 | –5.0 to 0 | –23 to –3 (155.52/ 622.08 Mbps) –19 to –3 (1250 Mbps) –18 to 0 (2488.32 Mbps) |
| ONS-SI-2G-S1 | OC-48, STM-16 | –2.0 to 3.0 | –9 |

*Table A-12      XFP Specifications (1PIO Only)*

| SFP Product ID | Interface | Transmitter Output Power Min/Max (dBm) | Receiver Input Power Min/Max (dBm) |
|---|---|---|---|
| ONS-XC-10G-S1 | OC-192, STM-64 | –6.0 to –1.0 | –11.0 to –1.0 |
| ONS-XC-10G-L2 | OC-192, STM-64 | 0.0 to 4.0 | –24.0 to –7.0 |

The OC-48/STM16 also supports 32-channel SFPs for DWDM applications; 32-channel SFPs can be plugged into the four-port ASAP card 4PIO module.

Some of the parameters common across all 32 DWDM SFPs include:

- Receiver wavelength: 1260 to 1620 nm
- Minimum overload: –9 dBm
- Maximum reflectance of receiver, measured at Rupees: –27 dB
- Maximum receiver power, damage threshold: +5 dBm

- Transmitter output power min/max : 0 to +4 dBm

Table A-13 lists the available DWDM SFPs.

*Table A-13*      ***ASAP Card 4PIO DWDM SFP Specifications***

| SFP Product ID | Interface | Wavelength[1] |
|---|---|---|
| ONS-SC-2G-30.3 | OC-48/STM16 | 1530.3 nm |
| ONS-SC-2G-31.1 | OC-48/STM16 | 1531.1 nm |
| ONS-SC-2G-31.9 | OC-48/STM16 | 1531.9 nm |
| ONS-SC-2G-32.6 | OC-48/STM16 | 1532.6 nm |
| ONS-SC-2G-34.2 | OC-48/STM16 | 1534.2 nm |
| ONS-SC-2G-35.0 | OC-48/STM16 | 1535.0 nm |
| ONS-SC-2G-35.8 | OC-48/STM16 | 1535.8 nm |
| ONS-SC-2G-36.6 | OC-48/STM16 | 1536.6 nm |
| ONS-SC-2G-38.1 | OC-48/STM16 | 1538.1 nm |
| ONS-SC-2G-38.9 | OC-48/STM16 | 1538.9 nm |
| ONS-SC-2G-39.7 | OC-48/STM16 | 1539.7 nm |
| ONS-SC-2G-40.5 | OC-48/STM16 | 1540.5 nm |
| ONS-SC-2G-42.1 | OC-48/STM16 | 1542.1 nm |
| ONS-SC-2G-42.9 | OC-48/STM16 | 1542.9 nm |
| ONS-SC-2G-43.7 | OC-48/STM16 | 1543.7 nm |
| ONS-SC-2G-44.5 | OC-48/STM16 | 1544.5 nm |
| ONS-SC-2G-46.1 | OC-48/STM16 | 1546.1 nm |
| ONS-SC-2G-46.9 | OC-48/STM16 | 1546.9 nm |
| ONS-SC-2G-47.7 | OC-48/STM16 | 1547.7 nm |
| ONS-SC-2G-48.5 | OC-48/STM16 | 1548.5 nm |
| ONS-SC-2G-50.1 | OC-48/STM16 | 1550.1 nm |
| ONS-SC-2G-50.9 | OC-48/STM16 | 1550.9 nm |
| ONS-SC-2G-51.7 | OC-48/STM16 | 1551.7 nm |
| ONS-SC-2G-52.5 | OC-48/STM16 | 1552.5 nm |
| ONS-SC-2G-54.1 | OC-48/STM16 | 1554.1 nm |
| ONS-SC-2G-54.9 | OC-48/STM16 | 1554.9 nm |
| ONS-SC-2G-55.7 | OC-48/STM16 | 1555.7 nm |
| ONS-SC-2G-56.5 | OC-48/STM16 | 1556.5 nm |
| ONS-SC-2G-58.1 | OC-48/STM16 | 1558.1 nm |
| ONS-SC-2G-58.9 | OC-48/STM16 | 1558.9 nm |
| ONS-SC-2G-59.7 | OC-48/STM16 | 1559.7 nm |
| ONS-SC-2G-60.6 | OC-48/STM16 | 1560.6 nm |

1.  Typical loss on a 1310-nm wavelength Single-mode fiber is 0.6 dB/km.

Table A-14 describes the power and noise limited performances parameters for the OC-SC-2G series SFPs.

*Table A-14      Power and Noise Limited Performances*

| Parameter | Power Limited Performances | | Noise Limited Performances | |
|---|---|---|---|---|
| Input power range | –9 to –28 dBm | At BER = $10^{-12}$ with SONET framed PRBS23<br><br>622 Mbps – 2.0 Gbps at OSNR[1] of 20 dB, 0.1 nm bandwidth<br><br>2.0Gbps – 2.7Gbps at OSNR of 21dB, 0.1 nm bandwidth | –9 to –22 dBm | At BER = $10^{-12}$ with SONET framed PRBS23<br><br>At OSNR of 16 dB at 0.1 nm bandwidth |
| Dispersion tolerance | –800 to 3600 dBm | 622 Mbps – 2.0 Gbps<br><br>Power penalty = 3 dB<br><br>OSNR = 20 dB at 0.1 nm bandwidth (Noise penalty = 0 dB) | –800 to 3600 dBm | 622 Mbps – 2.0 Gbps<br><br>Noise penalty = 2 dB<br><br>OSNR = 18 dB at 0.1 nm bandwidth (Power penalty = 0 dB) |
| | –800 to 2400 dBm | 2.0 Gbps – 2.7 Gbps<br><br>Power penalty = 3 dB<br><br>OSNR = 21 dB at 0.1 nm bandwidth (Noise penalty = 0 dB) | –800 to 2400 dBm | 2.0 Gbps – 2.7 Gbps<br><br>Noise penalty = 3 dB<br><br>OSNR = 19 dB at 0.1 nm bandwidth (Power penalty = 0 dB) |

1. OSNR

Table A-15 provides cabling specifications for the single-mode fiber (SMF) SFPs/XFPs. The ports of the listed SFPs/XFPs have LC-type connectors and the minimum cable distance for all SFPs/XFPs listed is 6.5 feet (2 m). Maximum cable distance for all SFPs/XFPs listed is 328 ft (100 m).

*Table A-15      Single-Mode Fiber SFP/XFP Port Cabling Specifications*

| SFP Product ID | Wavelength[1] | Fiber Type | Cable Distance |
|---|---|---|---|
| ONS-SI-622-L2 Long Reach | 1550 nm | 9 micron SMF | 80 km (49.71 mi.) |
| ONS-SE-2G-L2 | 1550 nm | 9 micron SMF | 80 km (49.71 mi.) |
| ONS-SE-Z1 | 1310 nm | 9 micron SMF | 15 km (9.3 mi.) |
| ONS-SI-155-L2 | 1550 nm | 9 micron SMF | 80 km (49.71 mi.) |
| ONS-XC-10G-S1 | 1310 nm | 9 micron SMF | 2 km (1.2 mi.) |
| ONS-XC-10G-L2 | 1550 nm | 9 micron SMF | 80 km (49.71 mi.) |
| ONS-SI-2G-S1 | 1310 nm | 9 micron SMF | 80 km (49.71 mi.) |

1. Typical loss on a 1310-nm wavelength SMF is 0.6 dB/km.

APPENDIX **B**

# Administrative and Service States

This appendix describes administrative and service states for Cisco ONS 15600 SDH cards, ports, and cross-connects. For circuit state information, see Chapter 7, "Circuits and Tunnels." Entity states are based on the generic state model defined in Telcordia GR-1093-CORE, Issue 2 and ITU-T X.731. The following sections are included:

- B.1  Service States, page B-1
- B.2  Administrative States, page B-2
- B.3  Service State Transitions, page B-3

## B.1  Service States

Service states include a Primary State (PST), a Primary State Qualifier (PSTQ), and one or more Secondary States (SST). Table B-1 lists the service state PSTs and PSTQs supported by the ONS 15600 SDH.

*Table B-1        ONS 15600 SDH Service State Primary States and Primary State Qualifiers*

| Primary State, Primary State Qualifier | Definition |
|---|---|
| Unlocked-enabled | The entity is fully operational and will perform as provisioned. |
| Unlocked-disabled | The entity is not operational because of an autonomous event. |
| Locked-disabled | The entity is not operational because of an autonomous event and has also been manually removed from service. |
| Locked-enabled | The entity has been manually removed from service. |

Table B-2 defines the SSTs supported by the ONS 15600 SDH.

*Table B-2        ONS 15600 SDH Secondary States*

| Secondary State | Definition |
|---|---|
| automaticInService | The entity is delayed before transitioning to the Unlocked-enabled service state. The transition to the Unlocked-enabled state depends on the correction of conditions, or on a soak timer. Alarm reporting is suppressed, but traffic is carried. 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. |
| disabled | The entity was manually removed from service and does not provide its provisioned functions. All services are disrupted; the entity is unable to carry traffic.<br><br>**Note**    STM-N ports and connections in the disabled state continue to send an Alarm Indication Signal Line (AIS-L). |
| failed | The entity has a raised alarm or condition. |
| loopback | The entity is in loopback mode. |
| mismatchOfEquipment | An improper card is installed, a cross-connect card does not support an installed card, or an incompatible backplane is installed. For example, an installed card is not compatible with the card preprovisioning or the slot. This SST applies only to cards. |
| maintenance | The entity has been manually removed from service for a maintenance activity but still performs its provisioned functions. Alarm reporting is suppressed, but traffic is carried. 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. |
| softwareDownload | The card is involved in a software download. This SST applies only to cards. |
| unassigned | The card is not provisioned in the database. This SST applies only to cards. |
| notInstalled | The card is not physically present (that is, an empty slot). This SST applies only to cards. |

# B.2   Administrative States

Administrative states are used to manage service states. Administrative states consist of a PST and an SST. Table B-3 lists the administrative states supported by the ONS 15600 SDH. See Table B-2 for SST definitions.

**Note**    A change in the administrative state of an entity does not change the service state of supporting or supported entities.

*Table B-3        ONS 15600 SDH Administrative States*

| Administrative State (PST,SST) | Definition |
|---|---|
| Unlocked | Puts the entity in service. |
| Unlocked,automaticInservice | Puts the entity in automatic in-service. |

*Table B-3        ONS 15600 SDH Administrative States (continued)*

| Administrative State (PST,SST) | Definition |
|---|---|
| Locked,disabled | Removes the entity from service and disables it. |
| Locked,maintenance | Removes the entity from service for maintenance. |

# B.3  Service State Transitions

This section describes the transition from one service state to the next for cards, ports, and cross-connects. A service state transition is based on the action performed on the entity.

**Note**       When an entity is put in the Locked,maintenance administrative state, the ONS 15600 SDH suppresses all standing alarms on that entity. All alarms and events appear on the Conditions tab. You can change this behavior for the LPBKFACILITY and LPBKTERMINAL alarms. To display these alarms on the Alarms tab, set the NODE.general.ReportLoopbackConditionsOnUnlocked,MaintenancePorts to TRUE on the NE Defaults tab.

## B.3.1  Card Service State Transitions

Table B-4 lists card service state transitions.

*Table B-4        ONS 15600 SDH Card Service State Transitions*

| Current Service State | Action | Next Service State |
|---|---|---|
| Unlocked-enabled | Change the administrative state to Locked,maintenance. | Locked-enabled,maintenance |
|  | Delete the card. | Locked-disabled,unassigned |
|  | Pull the card. | Unlocked-disabled,notInstalled |
|  | Reset the card. | Unlocked-disabled,softwareDownload |
|  | Alarm/condition is raised. | Unlocked-disabled,failed |
| Unlocked-disabled,automaticInService and mismatchOfEquipment | Pull the card. | Unlocked-disabled,automaticInService & notInstalled |
|  | Delete the card. | Locked-disabled,unassigned if the card is valid |
|  |  | Locked-disabled,mismatchOfEquipment & unassigned if the card is invalid |
| Unlocked-disabled,automaticInService & softwareDownload | Restart completed. | Unlocked-enabled |
|  | Pull the card. | Unlocked-disabled,automaticInService & notInstalled |

*Table B-4* **ONS 15600 SDH Card Service State Transitions (continued)**

| Current Service State | Action | Next Service State |
|---|---|---|
| Unlocked-disabled,automaticInService & notInstalled | Insert a valid card. | Unlocked-disabled,automaticInService & softwareDownload |
| | Insert an invalid card. | Unlocked-disabled,automaticInService & mismatchOfEquipment |
| | Delete the card. | Locked-disabled,unassigned & notInstalled |
| Unlocked-disabled,failed | Pull the card. | Unlocked-disabled,unequipped |
| | Delete the card. | Locked-disabled,unassigned |
| | Change the administrative state to Locked,maintenance. | Locked-disabled,failed & maintenance |
| | Reset the card. | Unlocked-disabled,softwareDownload |
| | Alarm/condition is cleared. | Unlocked-enabled |
| Unlocked-disabled,mismatchOfEquipment | Pull the card. | Unlocked-disabled,notInstalled |
| | Delete the card. | Locked-disabled,unassigned if the card is valid |
| | | Locked-disabled,mismatchOfEquipment & unassigned if the card is invalid |
| | Change the administrative state to Locked,maintenance. | Locked-disabled,mismatchOfEquipment & maintenance |
| Unlocked-disabled,softwareDownload | Restart completed. | Unlocked-enabled |
| | Pull the card. | Unlocked-disabled,notInstalled |
| Unlocked-disabled,notInstalled | Insert a valid card. | Unlocked-disabled,softwareDownload |
| | Insert an invalid card. | Unlocked-disabled,mismatchOfEquipment |
| | Delete the card. | Locked-disabled,unassigned & notInstalled |
| | Change the administrative state to Locked,maintenance. | Locked-disabled,maintenance & notInstalled |
| Locked-disabled,failed & maintenance | Pull the card. | Locked-disabled,maintenance & notInstalled |
| | Delete the card. | Locked-disabled,unassigned |
| | Change the administrative state to Unlocked. | Unlocked-disabled,failed |
| | Reset the card. | Locked-disabled,maintenance & softwareDownload |
| | Alarm/condition is cleared. | Unlocked-enabled |

*Table B-4* **ONS 15600 SDH Card Service State Transitions (continued)**

| Current Service State | Action | Next Service State |
|---|---|---|
| Locked-disabled,mismatchOfEquipment & maintenance | Change the administrative state to Unlocked. | Unlocked-disabled,mismatchOfEquipment |
| | Pull the card. | Locked-disabled,maintenance & notInstalled |
| | Delete the card. | Locked-disabled,unassigned if the card is valid |
| | | Locked-disabled,mismatchOfEquipment & unassigned if the card is invalid |
| Locked-disabled,mismatchOfEquipment & unassigned | Pull the card. | Locked-disabled,unassigned & notInstalled |
| | Provision the card. | Unlocked-disabled,mismatchOfEquipment |
| Locked-disabled,maintenance & softwareDownload | Restart completed. | Locked-enabled,maintenance |
| | Pull the card. | Locked-disabled,maintenance & notInstalled |
| Locked-disabled,maintenance & notInstalled | Change the administrative state to Unlocked. | Unlocked-disabled,notInstalled |
| | Insert a valid card. | Locked-disabled,maintenance & softwareDownload |
| | Insert an invalid card. | Locked-disabled,mismatchOfEquipment & maintenance |
| | Delete the card. | Locked-disabled,unassigned & notInstalled |
| Locked-disabled,unassigned | Pull the card. | Locked-disabled,unassigned & notInstalled |
| | Provision an invalid card. | Unlocked-disabled,mismatchOfEquipment |
| | Provision a valid card. | Unlocked-disabled,softwareDownload |
| Locked-disabled,unassigned & notInstalled | Insert a valid card. | Unlocked-disabled,softwareDownload |
| | Insert an invalid card. | Locked-disabled,mismatchOfEquipment & unassigned |
| | Preprovision a card. | Unlocked-disabled,automaticInService & notInstalled |
| Locked-enabled,maintenance | Change the administrative state to Unlocked. | Unlocked-enabled |
| | Delete the card. | Locked-disabled,unassigned |
| | Pull the card. | Locked-disabled,maintenance & notInstalled |
| | Reset the card. | Locked-disabled,maintenance & softwareDownloadunassigned |
| | Alarm/condition is raised. | Locked-disabled,failed & maintenance |

# B.3.2  Port and Cross-Connect Service State Transitions

Table B-5 lists the port and cross-connect service state transitions. Port states do not impact cross-connect states with one exception. A cross-connect in the Unlocked-disabled,automaticInService service state cannot transition autonomously into the Unlocked-enabled service state until the parent port is in the Unlocked-enabled service state.

You cannot transition a port from the Unlocked-enabled service state to the Locked-enabled,disabled state. You must first transition the port to the Locked-enabled,maintenance state. Once a port is in the Locked-enabled,maintenance state, the NODE.general.AllowServiceAffectingPortChangeToDisabled default setting of TRUE allows you to put a port in Locked-enabled,disabled even if the following conditions exist:

 * The port is a timing source.
 * The port is used for line, section, or tunneling data communicatiosn channel (DCC).
 * The port supports 1+1 protection or multidirectional multiplex section-shared protection ring (MS-SPRing).
 * Cross-connects are present on the port.
 * Overhead connections or overhead terminations are in use (such as express orderwire, local orderwire, or user data channels [UDCs]).

To change this behavior so that you cannot put a port in Locked-enabled,disabled if any of these conditions exist, set the NODE.general.AllowServiceAffectingPortChangeToDisabled default setting to FALSE. For the procedure to change node defaults, refer to the "Maintain the Node" chapter in the *Cisco ONS 15600 SDH Procedure Guide.*

**Note**      Deleting a port or cross-connect removes the entity from the system. The deleted entity does not transition to another service state.

*Table B-5        ONS 15600 SDH Port and Cross-Connect Service State Transitions*

| Current Service State | Action | Next Service State |
|---|---|---|
| Unlocked-enabled | Put the port or cross-connect in the Locked,maintenance administrative state. | Locked-enabled,maintenance |
| | Put the port or cross-connect in the Unlocked,automaticInService administrative state. | Unlocked-disabled,automaticInService |
| | (Cross-connect only) Put the cross-connect in the Locked,disabled administrative state. | Locked-enabled,disabled<br><br>Locked-enabled,disabled & outOfGroup for a VCAT cross-connect |

*Table B-5*        *ONS 15600 SDH Port and Cross-Connect Service State Transitions (continued)*

| Current Service State | Action | Next Service State |
|---|---|---|
| Unlocked-disabled,automaticInService | Put the port or cross-connect in the Unlocked administrative state. | Unlocked-enabled |
| | Put the port or cross-connect in the Locked,maintenance administrative state. | Locked-enabled,maintenance |
| | Put the port or cross-connect in the Locked,disabled administrative state. | Locked-enabled,disabled<br>Locked-enabled,disabled & outOfGroup for a VCAT cross-connect |
| | Alarm/condition is raised. | Unlocked-disabled,automaticInService & failed |
| Unlocked-disabled,automaticInService & failed | Alarm/condition is cleared. | Unlocked-disabled,automaticInService |
| | Put the port or cross-connect in the Unlocked administrative state. | Unlocked-disabled,failed |
| | Put the port or cross-connect in the Locked,disabled administrative state. | Locked-enabled,disabled |
| | Put the port or cross-connect in the Locked,maintenance administrative state. | Locked-disabled,failed & maintenance |
| Unlocked-disabled,failed | Alarm/condition is cleared. | Unlocked-enabled |
| | Put the port or cross-connect in the Unlocked,automaticInService administrative state. | Unlocked-disabled,automaticInService & failed |
| | Put the port or cross-connect in the Locked,disabled administrative state. | Locked-enabled,disabled<br>Locked-enabled,disabled & outOfGroup for a VCAT member |
| | Put the port or cross-connect in the Locked,maintenance administrative state | Locked-disabled,failed & maintenance |
| Locked-disabled,failed & loopback & maintenance | Release the loopback. | Locked-disabled,failed & maintenance |
| | Alarm/condition is cleared. | Locked-enabled,loopback & maintenance |

*Table B-5      ONS 15600 SDH Port and Cross-Connect Service State Transitions (continued)*

| Current Service State | Action | Next Service State |
|---|---|---|
| Locked-disabled,failed & maintenance | Alarm/condition is cleared. | Locked-enabled,maintenance |
| | Put the port or cross-connect in the Unlocked administrative state. | Unlocked-disabled,failed |
| | Put the port or cross-connect in the Unlocked,automaticInService administrative state. | Unlocked-disabled,automaticInService & failed |
| | Put the port or cross-connect in the Locked,disabled administrative state. | Locked-enabled,disabled |
| | Put the port or cross-connect in loopback. | Locked-disabled,failed & loopback & maintenance |
| Locked-enabled,disabled | Put the port or cross-connect in the Unlocked administrative state. | Unlocked-enabled |
| | Put the port or cross-connect in the Unlocked,automaticInService administrative state. | Unlocked-disabled,automaticInService |
| | Put the port or cross-connect in the Locked,maintenance. | Locked-enabled,maintenance |
| Locked-enabled,loopback & maintenance | Release the loopback. | Locked-enabled,maintenance |
| | Alarm/condition is raised. | Locked-disabled,failed & loopback & maintenance |
| Locked-enabled,maintenance | Put the port or cross-connect in the Unlocked administrative state. | Unlocked-enabled |
| | Put the port or cross-connect in the Unlocked,automaticInService administrative state. | Unlocked-disabled,automaticInService |
| | Put the port or cross-connect in the Locked,disabled. | Locked-enabled,disabled |
| | Put the port or cross-connect in loopback. | Locked-enabled,loopback & maintenance |
| | Alarm/condition is raised. | Locked-disabled,failed & maintenance |

# B.3.3  Pluggable Equipment Service State Transitions

The service state transitions for pluggable equipment are the same as for other equipment with the exceptions listed in Table B-6.

Note    Pluggable equipment (pluggable interface modules [PIMs] and pluggable port modules [PPMs]) will transition out of the unassigned state when inserted if the software can read the EEPROM and identify information on the pluggable equipment. If the software cannot read the pluggable equipment, the equipment is considered invalid and will not transition out of the unassigned state.

*Table B-6        ONS 15600 SDH Pluggable Equipment Service State Transitions*

| Current Service State | Action | Next Service State |
|---|---|---|
| Unlocked-enabled | Reset the pluggable equipment. | Unlocked-enabled |
| | Provision an unsupported service rate. | Unlocked-disabled,mismatchOfEquipment |
| | Pluggable equipment does not work with the board configuration. | |
| Unlocked-disabled,automaticInService & notInstalled | Insert valid pluggable equipment. | Unlocked-enabled |
| | Insert pluggable equipment with the incorrect rate. | Unlocked-disabled,mismatchOfEquipment |
| | Pluggable equipment does not work with the board configuration. | |
| Locked-disabled,mismatchOfEquipment | Delete unsupported service rate or modify provisioning so that the pluggable equipment is no longer a mismatch. | Unlocked-enabled |
| Locked-disabled,notInstalled | Insert valid pluggable equipment. | Unlocked-enabled |
| Locked-disabled,mismatchOfEquipment & maintenance | Delete unsupported service rate or modify provisioning so that the pluggable equipment is no longer a mismatch. | Locked-enabled,maintenance |
| Locked-disabled,maintenance & notInstalled | Insert valid pluggable equipment. | Locked-enabled,maintenance |
| Locked-disabled,unassigned | Provision valid pluggable equipment. | Unlocked-enabled |
| Locked-disabled,unassigned & notInstalled | Insert valid pluggable equipment. | Unlocked-enabled |
| | Insert pluggable equipment with the incorrect rate. | Unlocked-disabled,mismatchOfEquipment |
| | Pluggable equipment does not work with the board configuration. | |
| Locked-enabled,maintenance | Reset the pluggable equipment. | Locked-enabled,maintenance |
| | Provision an unsupported service rate. | Locked-disabled,mismatchOfEquipment & maintenance |
| | Pluggable equipment does not work with the board configuration. | |

■    **B.3.3   Pluggable Equipment Service State Transitions**

# Network Element Defaults

This appendix describes the factory-configured (default) network element (NE) settings for the Cisco ONS 15600 SDH. It includes descriptions of card default settings and node default settings. For procedures for importing, exporting and editing the settings, refer to the "Maintain the Node" chapter of the *Cisco ONS 15600 SDH Procedure Guide*. Cards supported by this platform that are not listed in this appendix are not supported by user-configurable NE defaults settings.

To change card settings individually (that is, without directly changing the NE defaults), refer to the "Change Card Settings" chapter of the *Cisco ONS 15600 SDH Procedure Guide*. To change node settings, refer to the "Change Node Settings" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

This appendix includes the following sections:

## C.1  Network Element Defaults Description

The NE defaults are preinstalled on each Cisco ONS 15600 SDH TSC card. Cisco also ships a file named 15600SDH-defaults.txt on the Cisco Transport Controller (CTC) software CD in case you want to import the defaults onto existing TSC cards. The NE defaults include card-level, CTC, and node-level defaults.

Changes to card provisioning that are made manually using the procedures in the "Change Card Settings" chapter in the *Cisco ONS 15600 SDH Procedure Guide* override default settings. If you use the CTC Defaults editor (on the node view Provisioning > Defaults tab) or import a new defaults file, any changes to card or port settings that result only affect cards that are installed or preprovisioned after the defaults have changed.

Changes that are made manually to most node-level default settings override the current settings, whether default or provisioned. If you change node-level default settings, either by using the Defaults editor or by importing a new defaults file, the new defaults reprovision the node immediately for all settings except those relating to protection (1+1 bidirectional switching, 1+1 reversion time, 1+1 revertive switching, multiplex section-shared protection ring [MS-SPRing] ring reversion time, MS-SPRing ring revertive switching, MS-SPRing span reversion time, and MS-SPRing span revertive switching). Settings relating to protection apply to subsequent provisioning.

✎
**Note**  Changing some node-level provisioning through NE defaults can cause CTC disconnection or a reboot of the node in order for the provisioning to take effect. Before you change a default, check in 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.

# C.2  Card Default Settings

The tables in this section list the default settings for each SDH card. Cisco provides several types of user-configurable defaults for Cisco ONS 15600 SDH optical, electrical, storage access networking, and Ethernet (or data) cards. Types of card defaults can be broadly grouped by function, as outlined in the following subsections. For information about individual card settings, refer to the "Change Card Settings" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

✎
**Note**  When the card level defaults are changed, the new provisioning done after the defaults have changed is affected. Existing provisioning remains unaffected.

The following types of defaults are defined for SDH cards.

# C.2.1  Configuration Defaults

Card-level and port-level configuration defaults correspond to settings found in the CTC card-level Provisioning tabs.

Configuration defaults that correspond to settings that are reachable from the CTC card-level Provisioning tabs include the following types of options (arranged by CTC subtab):

- Line—(STM-N and STM64-4-DWDM cards) Line-level configuration settings.
- VC4—(STM-N and STM64-4-DWDM cards) VC4 configuration settings.
- VC3—(STM-N cards) VC3 configuration settings.
- Pluggable Port Modules—(ASAP cards only) PPM (SFP) slot and port rate configuration settings.
- Optical—(ASAP cards only) STM-N rate port-level line configuration, VC3, VC4, Optics threshold, and SDH threshold settings.
- Ethernet—(ASAP cards only) Ethernet port-level line configuration settings.

✎
**Note**  Ethernet line configuration defaults apply to both Ethernet port and packet-over-SDH (POS) port settings where the same setting exists for both.

✎
**Note**  For further information about supported features of each individual card, see Chapter 2, "Card Reference."

# C.2.2  Threshold Defaults

Threshold default settings define the default cumulative values (thresholds) beyond which a threshold crossing alert (TCA) will be raised, making it possible to monitor the network and detect errors early.

Card threshold default settings are provided as follows:

- PM thresholds—(STM-N, STM64-4-DWDM, and ASAP cards) Can be expressed in counts or seconds; includes line and SDH thresholds.
- Physical Layer thresholds—(STM-N, STM64-4-DWDM, and ASAP cards) Expressed in percentages; includes optics thresholds.

Threshold defaults are defined for near end and/or far end, at 15-minute and one-day intervals. Thresholds are further broken down by type, such as Multiplex Section, Regeneration Section, VC3, or VC4 for performance monitoring (PM) thresholds, and TCA (warning) or Alarm for physical thresholds. PM threshold types define the layer to which the threshold applies. Physical threshold types define the level of response expected when the threshold is crossed.

**Note**      For full descriptions of the thresholds you can set for each card, see Chapter 12, "Performance Monitoring."

**Note**      For additional information regarding PM parameter threshold defaults as defined by Telcordia specifications, refer to Telcordia GR-820-CORE and GR-253-CORE.

# C.2.3  Defaults by Card

In the tables that follow, card defaults are defined by the default name, its factory-configured value, and the domain of allowable values that you can assign to it.

**Note**      Some default values, such as certain thresholds, are interdependent. Before changing a value, review the domain for that default and any other related defaults for potential dependencies.

## C.2.3.1  STM64-4 Card Default Settings

Table C-1 lists the OC192/STM64 SR/SH 4 Port 1310 and OC192/STM64 LR/LH 4 Port 1550 card default settings.

*Table C-1          STM64-4 Card Default Settings*

| Default Name | Default Value | Default Domain |
|---|---|---|
| STM64_4.config.line.AINSSoakTime | 08:00 (hours:mins) | 00:00, 00:15, 00:30 .. 48:00 |
| STM64_4.config.line.AlsMode | Disabled | Disabled, Auto Restart, Manual Restart, Manual Restart for Test |
| STM64_4.config.line.AlsRecoveryPulseDuration | 2.0 (seconds) | 2.0, 2.1, 2.2 .. 100.0 when AlsMode Disabled, Auto Restart, Manual Restart; 80.0, 80.1, 80.2 .. 100.0 when AlsMode Manual Restart for Test |

*Table C-1*        *STM64-4 Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| STM64_4.config.line.AlsRecoveryPulseInterval | 100 (seconds) | 60 - 300 |
| STM64_4.config.line.SDBER | 1E-7 | 1E-5, 1E-6, 1E-7, 1E-8, 1E-9 |
| STM64_4.config.line.SFBER | 1E-4 | 1E-3, 1E-4, 1E-5 |
| STM64_4.config.line.SendDoNotUse | FALSE | TRUE, FALSE |
| STM64_4.config.line.State | unlocked, automaticInService | unlocked, locked, disabled, locked, maintenance, unlocked, automaticInService |
| STM64_4.config.line.SyncMsgIn | TRUE | FALSE, TRUE |
| STM64_4.config.vc4.IPPMEnabled | FALSE | TRUE, FALSE |
| STM64_4.physicalthresholds.alarm.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| STM64_4.physicalthresholds.alarm.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| STM64_4.physicalthresholds.alarm.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| STM64_4.physicalthresholds.alarm.OPR-LOW | 50 (%) | -1, 0, 1 .. OPR-HIGH |
| STM64_4.physicalthresholds.alarm.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| STM64_4.physicalthresholds.alarm.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| STM64_4.physicalthresholds.warning.15min.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| STM64_4.physicalthresholds.warning.15min.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| STM64_4.physicalthresholds.warning.15min.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| STM64_4.physicalthresholds.warning.15min.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| STM64_4.physicalthresholds.warning.15min.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| STM64_4.physicalthresholds.warning.15min.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| STM64_4.physicalthresholds.warning.1day.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| STM64_4.physicalthresholds.warning.1day.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| STM64_4.physicalthresholds.warning.1day.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| STM64_4.physicalthresholds.warning.1day.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| STM64_4.physicalthresholds.warning.1day.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| STM64_4.physicalthresholds.warning.1day.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| STM64_4.pmthresholds.ms.farend.15min.BBE | 85040 (count) | 0 - 8850600 |
| STM64_4.pmthresholds.ms.farend.15min.EB | 85040 (B2 count) | 0 - 8850600 |
| STM64_4.pmthresholds.ms.farend.15min.ES | 87 (seconds) | 0 - 900 |

**Table C-1**      **STM64-4 Card Default Settings (continued)**

| Default Name | Default Value | Default Domain |
|---|---|---|
| STM64_4.pmthresholds.ms.farend.15min.FC | 10 (count) | 0 - 72 |
| STM64_4.pmthresholds.ms.farend.15min.SES | 1 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.ms.farend.15min.UAS | 3 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.ms.farend.1day.BBE | 850400 (count) | 0 - 849657600 |
| STM64_4.pmthresholds.ms.farend.1day.EB | 850400 (B2 count) | 0 - 849657600 |
| STM64_4.pmthresholds.ms.farend.1day.ES | 864 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.ms.farend.1day.FC | 40 (count) | 0 - 6912 |
| STM64_4.pmthresholds.ms.farend.1day.SES | 4 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.ms.farend.1day.UAS | 10 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.ms.nearend.15min.BBE | 85040 (count) | 0 - 8850600 |
| STM64_4.pmthresholds.ms.nearend.15min.EB | 85040 (B2 count) | 0 - 8850600 |
| STM64_4.pmthresholds.ms.nearend.15min.ES | 87 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.ms.nearend.15min.FC | 10 (count) | 0 - 72 |
| STM64_4.pmthresholds.ms.nearend.15min.PSC | 1 (count) | 0 - 600 |
| STM64_4.pmthresholds.ms.nearend.15min.PSC-W | 1 (count) | 0 - 600 |
| STM64_4.pmthresholds.ms.nearend.15min.PSD | 300 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.ms.nearend.15min.PSD-W | 300 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.ms.nearend.15min.SES | 1 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.ms.nearend.15min.UAS | 3 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.ms.nearend.1day.BBE | 850400 (count) | 0 - 849657600 |
| STM64_4.pmthresholds.ms.nearend.1day.EB | 850400 (B2 count) | 0 - 849657600 |
| STM64_4.pmthresholds.ms.nearend.1day.ES | 864 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.ms.nearend.1day.FC | 40 (count) | 0 - 6912 |
| STM64_4.pmthresholds.ms.nearend.1day.PSC | 5 (count) | 0 - 57600 |
| STM64_4.pmthresholds.ms.nearend.1day.PSC-W | 5 (count) | 0 - 57600 |
| STM64_4.pmthresholds.ms.nearend.1day.PSD | 600 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.ms.nearend.1day.PSD-W | 600 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.ms.nearend.1day.SES | 4 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.ms.nearend.1day.UAS | 10 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.path.farend.15min.BBE | 25 (count) | 0 - 207273600 |
| STM64_4.pmthresholds.path.farend.15min.EB | 15 (B3 count) | 0 - 691200000 |
| STM64_4.pmthresholds.path.farend.15min.ES | 12 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.path.farend.15min.FC | 10 (count) | 0 - 72 |
| STM64_4.pmthresholds.path.farend.15min.SES | 3 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.path.farend.15min.UAS | 10 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.path.farend.1day.BBE | 250 (count) | 0 - 207273600 |

*Table C-1       STM64-4 Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| STM64_4.pmthresholds.path.farend.1day.EB | 125 (B3 count) | 0 - 691200000 |
| STM64_4.pmthresholds.path.farend.1day.ES | 100 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.path.farend.1day.FC | 40 (count) | 0 - 6912 |
| STM64_4.pmthresholds.path.farend.1day.SES | 7 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.path.farend.1day.UAS | 10 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.path.nearend.15min.BBE | 25 (count) | 0 - 2159100 |
| STM64_4.pmthresholds.path.nearend.15min.EB | 15 (B3 count) | 0 - 7200000 |
| STM64_4.pmthresholds.path.nearend.15min.ES | 12 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.path.nearend.15min.FC | 10 (count) | 0 - 72 |
| STM64_4.pmthresholds.path.nearend.15min.NPJC-PDET | 60 (count) | 0 - 7200000 |
| STM64_4.pmthresholds.path.nearend.15min.NPJC-PGEN | 60 (count) | 0 - 7200000 |
| STM64_4.pmthresholds.path.nearend.15min.PPJC-PDET | 60 (count) | 0 - 7200000 |
| STM64_4.pmthresholds.path.nearend.15min.PPJC-PGEN | 60 (count) | 0 - 7200000 |
| STM64_4.pmthresholds.path.nearend.15min.SES | 3 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.path.nearend.15min.UAS | 10 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.path.nearend.1day.BBE | 250 (count) | 0 - 207273600 |
| STM64_4.pmthresholds.path.nearend.1day.EB | 125 (B3 count) | 0 - 691200000 |
| STM64_4.pmthresholds.path.nearend.1day.ES | 100 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.path.nearend.1day.FC | 40 (count) | 0 - 6912 |
| STM64_4.pmthresholds.path.nearend.1day.NPJC-PDET | 5760 (count) | 0 - 691200000 |
| STM64_4.pmthresholds.path.nearend.1day.NPJC-PGEN | 5760 (count) | 0 - 691200000 |
| STM64_4.pmthresholds.path.nearend.1day.PPJC-PDET | 5760 (count) | 0 - 691200000 |
| STM64_4.pmthresholds.path.nearend.1day.PPJC-PGEN | 5760 (count) | 0 - 691200000 |
| STM64_4.pmthresholds.path.nearend.1day.SES | 7 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.path.nearend.1day.UAS | 10 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.rs.nearend.15min.BBE | 10000 (count) | 0 - 7967700 |
| STM64_4.pmthresholds.rs.nearend.15min.EB | 10000 (B1 count) | 0 - 7967700 |
| STM64_4.pmthresholds.rs.nearend.15min.ES | 500 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.rs.nearend.15min.OFS | 500 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.rs.nearend.15min.SES | 500 (seconds) | 0 - 900 |
| STM64_4.pmthresholds.rs.nearend.1day.BBE | 100000 (count) | 0 - 764899200 |
| STM64_4.pmthresholds.rs.nearend.1day.EB | 100000 (B1 count) | 0 - 764899200 |
| STM64_4.pmthresholds.rs.nearend.1day.ES | 5000 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.rs.nearend.1day.OFS | 5000 (seconds) | 0 - 86400 |
| STM64_4.pmthresholds.rs.nearend.1day.SES | 5000 (seconds) | 0 - 86400 |

## C.2.3.2 STM64-4-DWDM Card Default Settings

Table C-2 lists the STM64-4-DWDM (OC192/STM64 4 Port ITU C-Band) card default settings.

*Table C-2        STM64-4-DWDM Card Default Settings*

| Default Name | Default Value | Default Domain |
|---|---|---|
| STM64_4_DWDM.config.line.AINSSoakTime | 08:00 (hours:mins) | 00:00, 00:15, 00:30 .. 48:00 |
| STM64_4_DWDM.config.line.AlsMode | Disabled | Disabled, Auto Restart, Manual Restart, Manual Restart for Test |
| STM64_4_DWDM.config.line.AlsRecoveryPulseDuration | 100.0 (seconds) | 2.0, 2.1, 2.2 .. 100.0 when AlsMode Disabled, Auto Restart, Manual Restart; 80.0, 80.1, 80.2 .. 100.0 when AlsMode Manual Restart for Test |
| STM64_4_DWDM.config.line.AlsRecoveryPulseInterval | 100 (seconds) | 60 - 300 |
| STM64_4_DWDM.config.line.SDBER | 1E-7 | 1E-5, 1E-6, 1E-7, 1E-8, 1E-9 |
| STM64_4_DWDM.config.line.SFBER | 1E-4 | 1E-3, 1E-4, 1E-5 |
| STM64_4_DWDM.config.line.SendDoNotUse | FALSE | TRUE, FALSE |
| STM64_4_DWDM.config.line.State | unlocked, automaticInService | unlocked, locked, disabled, locked, maintenance, unlocked, automaticInService |
| STM64_4_DWDM.config.line.SyncMsgIn | TRUE | FALSE, TRUE |
| STM64_4_DWDM.config.vc4.IPPMEnabled | FALSE | TRUE, FALSE |
| STM64_4_DWDM.physicalthresholds.alarm.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| STM64_4_DWDM.physicalthresholds.alarm.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| STM64_4_DWDM.physicalthresholds.alarm.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| STM64_4_DWDM.physicalthresholds.alarm.OPR-LOW | 50 (%) | -1, 0, 1 .. OPR-HIGH |
| STM64_4_DWDM.physicalthresholds.alarm.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| STM64_4_DWDM.physicalthresholds.alarm.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| STM64_4_DWDM.physicalthresholds.warning.15min.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| STM64_4_DWDM.physicalthresholds.warning.15min.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| STM64_4_DWDM.physicalthresholds.warning.15min.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| STM64_4_DWDM.physicalthresholds.warning.15min.OPR-LOW | 50 (%) | -1, 0, 1 .. OPR-HIGH |
| STM64_4_DWDM.physicalthresholds.warning.15min.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| STM64_4_DWDM.physicalthresholds.warning.15min.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |

*Table C-2        STM64-4-DWDM Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| STM64_4_DWDM.physicalthresholds.warning.1day.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| STM64_4_DWDM.physicalthresholds.warning.1day.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| STM64_4_DWDM.physicalthresholds.warning.1day.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| STM64_4_DWDM.physicalthresholds.warning.1day.OPR-LOW | 50 (%) | -1, 0, 1 .. OPR-HIGH |
| STM64_4_DWDM.physicalthresholds.warning.1day.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| STM64_4_DWDM.physicalthresholds.warning.1day.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| STM64_4_DWDM.pmthresholds.ms.farend.15min.BBE | 85040 (count) | 0 - 2212200 |
| STM64_4_DWDM.pmthresholds.ms.farend.15min.EB | 85040 (B2 count) | 0 - 2212200 |
| STM64_4_DWDM.pmthresholds.ms.farend.15min.ES | 87 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.ms.farend.15min.FC | 10 (count) | 0 - 72 |
| STM64_4_DWDM.pmthresholds.ms.farend.15min.SES | 1 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.ms.farend.15min.UAS | 3 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.ms.farend.1day.BBE | 850400 (count) | 0 - 212371200 |
| STM64_4_DWDM.pmthresholds.ms.farend.1day.EB | 850400 (B2 count) | 0 - 212371200 |
| STM64_4_DWDM.pmthresholds.ms.farend.1day.ES | 864 (seconds) | 0 - 86400 |
| STM64_4_DWDM.pmthresholds.ms.farend.1day.FC | 40 (count) | 0 - 6912 |
| STM64_4_DWDM.pmthresholds.ms.farend.1day.SES | 4 (seconds) | 0 - 86400 |
| STM64_4_DWDM.pmthresholds.ms.farend.1day.UAS | 10 (seconds) | 0 - 86400 |
| STM64_4_DWDM.pmthresholds.ms.nearend.15min.BBE | 85040 (count) | 5 - 2212200 |
| STM64_4_DWDM.pmthresholds.ms.nearend.15min.EB | 85040 (B2 count) | 0 - 2212200 |
| STM64_4_DWDM.pmthresholds.ms.nearend.15min.ES | 87 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.ms.nearend.15min.FC | 10 (count) | 0 - 72 |
| STM64_4_DWDM.pmthresholds.ms.nearend.15min.PSC | 1 (count) | 0 - 600 |
| STM64_4_DWDM.pmthresholds.ms.nearend.15min.PSC-W | 1 (count) | 0 - 600 |
| STM64_4_DWDM.pmthresholds.ms.nearend.15min.PSD | 300 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.ms.nearend.15min.PSD-W | 300 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.ms.nearend.15min.SES | 1 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.ms.nearend.15min.UAS | 3 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.ms.nearend.1day.BBE | 850400 (count) | 0 - 212371200 |
| STM64_4_DWDM.pmthresholds.ms.nearend.1day.EB | 850400 (B2 count) | 0 - 212371200 |
| STM64_4_DWDM.pmthresholds.ms.nearend.1day.ES | 864 (seconds) | 0 - 86400 |
| STM64_4_DWDM.pmthresholds.ms.nearend.1day.FC | 40 (count) | 0 - 6912 |
| STM64_4_DWDM.pmthresholds.ms.nearend.1day.PSC | 5 (count) | 0 - 57600 |
| STM64_4_DWDM.pmthresholds.ms.nearend.1day.PSC-W | 5 (count) | 0 - 57600 |

*Table C-2        STM64-4-DWDM Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| STM64_4_DWDM.pmthresholds.ms.nearend.1day.PSD | 600 (seconds) | 0 - 86400 |
| STM64_4_DWDM.pmthresholds.ms.nearend.1day.PSD-W | 600 (seconds) | 0 - 86400 |
| STM64_4_DWDM.pmthresholds.ms.nearend.1day.SES | 4 (seconds) | 0 - 86400 |
| STM64_4_DWDM.pmthresholds.ms.nearend.1day.UAS | 10 (seconds) | 0 - 86400 |
| STM64_4_DWDM.pmthresholds.path.farend.15min.BBE | 25 (count) | 0 - 2212200 |
| STM64_4_DWDM.pmthresholds.path.farend.15min.EB | 15 (B3 count) | 0 - 7200000 |
| STM64_4_DWDM.pmthresholds.path.farend.15min.ES | 12 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.path.farend.15min.FC | 10 (count) | 0 - 72 |
| STM64_4_DWDM.pmthresholds.path.farend.15min.SES | 3 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.path.farend.15min.UAS | 10 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.path.farend.1day.BBE | 250 (count) | 0 - 2212200 |
| STM64_4_DWDM.pmthresholds.path.farend.1day.EB | 125 (B3 count) | 0 - 691200000 |
| STM64_4_DWDM.pmthresholds.path.farend.1day.ES | 100 (seconds) | 0 - 86400 |
| STM64_4_DWDM.pmthresholds.path.farend.1day.FC | 40 (count) | 0 - 6912 |
| STM64_4_DWDM.pmthresholds.path.farend.1day.SES | 7 (seconds) | 0 - 86400 |
| STM64_4_DWDM.pmthresholds.path.farend.1day.UAS | 10 (seconds) | 0 - 86400 |
| STM64_4_DWDM.pmthresholds.path.nearend.15min.BBE | 25 (count) | 0 - 2159100 |
| STM64_4_DWDM.pmthresholds.path.nearend.15min.EB | 15 (B3 count) | 0 - 7200000 |
| STM64_4_DWDM.pmthresholds.path.nearend.15min.ES | 12 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.path.nearend.15min.FC | 10 (count) | 0 - 72 |
| STM64_4_DWDM.pmthresholds.path.nearend.15min.NPJC-PDET | 60 (count) | 0 - 7200000 |
| STM64_4_DWDM.pmthresholds.path.nearend.15min.NPJC-PGEN | 60 (count) | 0 - 7200000 |
| STM64_4_DWDM.pmthresholds.path.nearend.15min.PPJC-PDET | 60 (count) | 0 - 7200000 |
| STM64_4_DWDM.pmthresholds.path.nearend.15min.PPJC-PGEN | 60 (count) | 0 - 7200000 |
| STM64_4_DWDM.pmthresholds.path.nearend.15min.SES | 3 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.path.nearend.15min.UAS | 10 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.path.nearend.1day.BBE | 250 (count) | 0 - 207273600 |
| STM64_4_DWDM.pmthresholds.path.nearend.1day.EB | 125 (B3 count) | 0 - 691200000 |
| STM64_4_DWDM.pmthresholds.path.nearend.1day.ES | 100 (seconds) | 0 - 86400 |
| STM64_4_DWDM.pmthresholds.path.nearend.1day.FC | 40 (count) | 0 - 6912 |
| STM64_4_DWDM.pmthresholds.path.nearend.1day.NPJC-PDET | 5760 (count) | 0 - 691200000 |
| STM64_4_DWDM.pmthresholds.path.nearend.1day.NPJC-PGEN | 5760 (count) | 0 - 691200000 |
| STM64_4_DWDM.pmthresholds.path.nearend.1day.PPJC-PDET | 5760 (count) | 0 - 691200000 |
| STM64_4_DWDM.pmthresholds.path.nearend.1day.PPJC-PGEN | 5760 (count) | 0 - 691200000 |
| STM64_4_DWDM.pmthresholds.path.nearend.1day.SES | 7 (seconds) | 0 - 86400 |
| STM64_4_DWDM.pmthresholds.path.nearend.1day.UAS | 10 (seconds) | 0 - 86400 |

*Table C-2 STM64-4-DWDM Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| STM64_4_DWDM.pmthresholds.rs.nearend.15min.BBE | 10000 (count) | 0 - 2151900 |
| STM64_4_DWDM.pmthresholds.rs.nearend.15min.EB | 10000 (B1 count) | 0 - 2151900 |
| STM64_4_DWDM.pmthresholds.rs.nearend.15min.ES | 500 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.rs.nearend.15min.OFS | 500 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.rs.nearend.15min.SES | 500 (seconds) | 0 - 900 |
| STM64_4_DWDM.pmthresholds.rs.nearend.1day.BBE | 100000 (count) | 0 - 206582400 |
| STM64_4_DWDM.pmthresholds.rs.nearend.1day.EB | 100000 (B1 count) | 0 - 206582400 |
| STM64_4_DWDM.pmthresholds.rs.nearend.1day.ES | 5000 (seconds) | 0 - 86400 |
| STM64_4_DWDM.pmthresholds.rs.nearend.1day.OFS | 5000 (seconds) | 0 - 86400 |
| STM64_4_DWDM.pmthresholds.rs.nearend.1day.SES | 5000 (seconds) | 0 - 86400 |

## C.2.3.3 STM16-16 Card Default Settings

Table C-3 lists the OC48/STM16 SR/SH 16 Port 1310 and OC48/STM16 LR/LH 16 Port 1550 card default settings.

*Table C-3 STM16-16 Card Default Settings*

| Default Name | Default Value | Default Domain |
|---|---|---|
| STM16_16.config.line.AINSSoakTime | 08:00 (hours:mins) | 00:00, 00:15, 00:30 .. 48:00 |
| STM16_16.config.line.AlsMode | Disabled | Disabled, Auto Restart, Manual Restart, Manual Restart for Test |
| STM16_16.config.line.AlsRecoveryPulseDuration | 2.0 (seconds) | 2.0, 2.1, 2.2 .. 100.0 when AlsMode Disabled, Auto Restart, Manual Restart; 80.0, 80.1, 80.2 .. 100.0 when AlsMode Manual Restart for Test |
| STM16_16.config.line.AlsRecoveryPulseInterval | 100 (seconds) | 60 - 300 |
| STM16_16.config.line.SDBER | 1E-7 | 1E-5, 1E-6, 1E-7, 1E-8, 1E-9 |
| STM16_16.config.line.SFBER | 1E-4 | 1E-3, 1E-4, 1E-5 |
| STM16_16.config.line.SendDoNotUse | FALSE | TRUE, FALSE |
| STM16_16.config.line.State | unlocked, automaticInService | unlocked, locked, disabled, locked, maintenance, unlocked, automaticInService |
| STM16_16.config.line.SyncMsgIn | TRUE | FALSE, TRUE |
| STM16_16.config.vc4.IPPMEnabled | FALSE | TRUE, FALSE |
| STM16_16.physicalthresholds.alarm.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| STM16_16.physicalthresholds.alarm.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| STM16_16.physicalthresholds.alarm.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |

*Table C-3* **STM16-16 Card Default Settings (continued)**

| Default Name | Default Value | Default Domain |
|---|---|---|
| STM16_16.physicalthresholds.alarm.OPR-LOW | 50 (%) | -1, 0, 1 .. OPR-HIGH |
| STM16_16.physicalthresholds.alarm.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| STM16_16.physicalthresholds.alarm.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| STM16_16.physicalthresholds.warning.15min.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| STM16_16.physicalthresholds.warning.15min.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| STM16_16.physicalthresholds.warning.15min.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| STM16_16.physicalthresholds.warning.15min.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| STM16_16.physicalthresholds.warning.15min.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| STM16_16.physicalthresholds.warning.15min.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| STM16_16.physicalthresholds.warning.1day.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| STM16_16.physicalthresholds.warning.1day.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| STM16_16.physicalthresholds.warning.1day.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| STM16_16.physicalthresholds.warning.1day.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| STM16_16.physicalthresholds.warning.1day.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| STM16_16.physicalthresholds.warning.1day.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| STM16_16.pmthresholds.ms.farend.15min.BBE | 21260 (count) | 0 - 2212200 |
| STM16_16.pmthresholds.ms.farend.15min.EB | 21260 (B2 count) | 0 - 2212200 |
| STM16_16.pmthresholds.ms.farend.15min.ES | 87 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.ms.farend.15min.FC | 10 (count) | 0 - 72 |
| STM16_16.pmthresholds.ms.farend.15min.SES | 1 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.ms.farend.15min.UAS | 3 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.ms.farend.1day.BBE | 212600 (count) | 0 - 212371200 |
| STM16_16.pmthresholds.ms.farend.1day.EB | 212600 (B2 count) | 0 - 212371200 |
| STM16_16.pmthresholds.ms.farend.1day.ES | 864 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.ms.farend.1day.FC | 40 (count) | 0 - 6912 |
| STM16_16.pmthresholds.ms.farend.1day.SES | 4 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.ms.farend.1day.UAS | 10 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.ms.nearend.15min.BBE | 21260 (count) | 5 - 2212200 |
| STM16_16.pmthresholds.ms.nearend.15min.EB | 21260 (B2 count) | 0 - 2212200 |
| STM16_16.pmthresholds.ms.nearend.15min.ES | 87 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.ms.nearend.15min.FC | 10 (count) | 0 - 72 |

**Cisco ONS 15600 SDH Reference Manual, R8.0**

*Table C-3* **STM16-16 Card Default Settings (continued)**

| Default Name | Default Value | Default Domain |
|---|---|---|
| STM16_16.pmthresholds.ms.nearend.15min.PSC | 1 (count) | 0 - 600 |
| STM16_16.pmthresholds.ms.nearend.15min.PSC-W | 1 (count) | 0 - 600 |
| STM16_16.pmthresholds.ms.nearend.15min.PSD | 300 (seconds) | 0 - 600 |
| STM16_16.pmthresholds.ms.nearend.15min.PSD-W | 300 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.ms.nearend.15min.SES | 1 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.ms.nearend.15min.UAS | 3 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.ms.nearend.1day.BBE | 212600 (count) | 0 - 212371200 |
| STM16_16.pmthresholds.ms.nearend.1day.EB | 212600 (B2 count) | 0 - 212371200 |
| STM16_16.pmthresholds.ms.nearend.1day.ES | 864 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.ms.nearend.1day.FC | 40 (count) | 0 - 6912 |
| STM16_16.pmthresholds.ms.nearend.1day.PSC | 5 (count) | 0 - 57600 |
| STM16_16.pmthresholds.ms.nearend.1day.PSC-W | 5 (count) | 0 - 57600 |
| STM16_16.pmthresholds.ms.nearend.1day.PSD | 600 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.ms.nearend.1day.PSD-W | 600 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.ms.nearend.1day.SES | 4 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.ms.nearend.1day.UAS | 10 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.path.farend.15min.BBE | 25 (count) | 0 - 2212200 |
| STM16_16.pmthresholds.path.farend.15min.EB | 15 (B3 count) | 0 - 7200000 |
| STM16_16.pmthresholds.path.farend.15min.ES | 12 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.path.farend.15min.FC | 10 (count) | 0 - 72 |
| STM16_16.pmthresholds.path.farend.15min.SES | 3 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.path.farend.15min.UAS | 10 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.path.farend.1day.BBE | 250 (count) | 0 - 2212200 |
| STM16_16.pmthresholds.path.farend.1day.EB | 125 (B3 count) | 0 - 691200000 |
| STM16_16.pmthresholds.path.farend.1day.ES | 100 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.path.farend.1day.FC | 40 (count) | 0 - 6912 |
| STM16_16.pmthresholds.path.farend.1day.SES | 7 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.path.farend.1day.UAS | 10 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.path.nearend.15min.BBE | 25 (count) | 0 - 2159100 |
| STM16_16.pmthresholds.path.nearend.15min.EB | 15 (B3 count) | 0 - 7200000 |
| STM16_16.pmthresholds.path.nearend.15min.ES | 12 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.path.nearend.15min.FC | 10 (count) | 0 - 72 |
| STM16_16.pmthresholds.path.nearend.15min.NPJC-PDET | 60 (count) | 0 - 7200000 |
| STM16_16.pmthresholds.path.nearend.15min.NPJC-PGEN | 60 (count) | 0 - 7200000 |
| STM16_16.pmthresholds.path.nearend.15min.PPJC-PDET | 60 (count) | 0 - 7200000 |
| STM16_16.pmthresholds.path.nearend.15min.PPJC-PGEN | 60 (count) | 0 - 7200000 |

*Table C-3        STM16-16 Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| STM16_16.pmthresholds.path.nearend.15min.SES | 3 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.path.nearend.15min.UAS | 10 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.path.nearend.1day.BBE | 250 (count) | 0 - 207273600 |
| STM16_16.pmthresholds.path.nearend.1day.EB | 125 (B3 count) | 0 - 691200000 |
| STM16_16.pmthresholds.path.nearend.1day.ES | 100 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.path.nearend.1day.FC | 40 (count) | 0 - 6912 |
| STM16_16.pmthresholds.path.nearend.1day.NPJC-PDET | 5760 (count) | 0 - 691200000 |
| STM16_16.pmthresholds.path.nearend.1day.NPJC-PGEN | 5760 (count) | 0 - 691200000 |
| STM16_16.pmthresholds.path.nearend.1day.PPJC-PDET | 5760 (count) | 0 - 691200000 |
| STM16_16.pmthresholds.path.nearend.1day.PPJC-PGEN | 5760 (count) | 0 - 691200000 |
| STM16_16.pmthresholds.path.nearend.1day.SES | 7 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.path.nearend.1day.UAS | 10 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.rs.nearend.15min.BBE | 10000 (count) | 0 - 2151900 |
| STM16_16.pmthresholds.rs.nearend.15min.EB | 88 (B1 count) | 0 - 2151900 |
| STM16_16.pmthresholds.rs.nearend.15min.ES | 500 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.rs.nearend.15min.OFS | 500 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.rs.nearend.15min.SES | 500 (seconds) | 0 - 900 |
| STM16_16.pmthresholds.rs.nearend.1day.BBE | 100000 (count) | 0 - 206582400 |
| STM16_16.pmthresholds.rs.nearend.1day.EB | 100000 (B1 count) | 0 - 206582400 |
| STM16_16.pmthresholds.rs.nearend.1day.ES | 5000 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.rs.nearend.1day.OFS | 5000 (seconds) | 0 - 86400 |
| STM16_16.pmthresholds.rs.nearend.1day.SES | 5000 (seconds) | 0 - 86400 |

## C.2.3.4  ASAP Card Default Settings

Table C-4 lists the ASAP card default settings.

*Table C-4        ASAP Card Default Settings*

| Default Name | Default Value | Default Domain |
|---|---|---|
| ASAP_4.ETHER-PORT.config.AINSSoakTime | 08:00 (hours:mins) | 00:00, 00:15, 00:30 .. 48:00 |
| ASAP_4.ETHER-PORT.config.State | locked, disabled | unlocked, locked, disabled, locked, maintenance, unlocked, automaticInService |
| ASAP_4.STM1-PORT.config.line.AINSSoakTime | 08:00 (hours:mins) | 00:00, 00:15, 00:30 .. 48:00 |
| ASAP_4.STM1-PORT.config.line.AlsMode | Disabled | Disabled, Auto Restart, Manual Restart, Manual Restart for Test |

*Table C-4  ASAP Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| ASAP_4.STM1-PORT.config.line.AlsRecoveryPulseDuration | 2.0 (seconds) | 2.0, 2.1, 2.2 .. 100.0 when AlsMode Disabled, Auto Restart, Manual Restart; 80.0, 80.1, 80.2 .. 100.0 when AlsMode Manual Restart for Test |
| ASAP_4.STM1-PORT.config.line.AlsRecoveryPulseInterval | 100 (seconds) | 60 - 300 |
| ASAP_4.STM1-PORT.config.line.SDBER | 1E-7 | 1E-5, 1E-6, 1E-7, 1E-8, 1E-9 |
| ASAP_4.STM1-PORT.config.line.SFBER | 1E-4 | 1E-3, 1E-4, 1E-5 |
| ASAP_4.STM1-PORT.config.line.SendDoNotUse | FALSE | TRUE, FALSE |
| ASAP_4.STM1-PORT.config.line.State | unlocked, automaticInService | unlocked, locked, disabled, locked, maintenance, unlocked, automaticInService |
| ASAP_4.STM1-PORT.config.line.SyncMsgIn | TRUE | FALSE, TRUE |
| ASAP_4.STM1-PORT.config.vc4.IPPMEnabled | FALSE | TRUE, FALSE |
| ASAP_4.STM1-PORT.physicalthresholds.alarm.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| ASAP_4.STM1-PORT.physicalthresholds.alarm.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| ASAP_4.STM1-PORT.physicalthresholds.alarm.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| ASAP_4.STM1-PORT.physicalthresholds.alarm.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| ASAP_4.STM1-PORT.physicalthresholds.alarm.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| ASAP_4.STM1-PORT.physicalthresholds.alarm.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| ASAP_4.STM1-PORT.physicalthresholds.warning.15min.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| ASAP_4.STM1-PORT.physicalthresholds.warning.15min.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| ASAP_4.STM1-PORT.physicalthresholds.warning.15min.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| ASAP_4.STM1-PORT.physicalthresholds.warning.15min.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| ASAP_4.STM1-PORT.physicalthresholds.warning.15min.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| ASAP_4.STM1-PORT.physicalthresholds.warning.15min.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| ASAP_4.STM1-PORT.physicalthresholds.warning.1day.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| ASAP_4.STM1-PORT.physicalthresholds.warning.1day.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| ASAP_4.STM1-PORT.physicalthresholds.warning.1day.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| ASAP_4.STM1-PORT.physicalthresholds.warning.1day.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| ASAP_4.STM1-PORT.physicalthresholds.warning.1day.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |

*Table C-4*      *ASAP Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| ASAP_4.STM1-PORT.physicalthresholds.warning.1day.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| ASAP_4.STM1-PORT.pmthresholds.ms.farend.15min.BBE | 1312 (count) | 0 - 2212200 |
| ASAP_4.STM1-PORT.pmthresholds.ms.farend.15min.EB | 1312 (B2 count) | 0 - 2212200 |
| ASAP_4.STM1-PORT.pmthresholds.ms.farend.15min.ES | 87 (seconds) | 0 - 900 |
| ASAP_4.STM1-PORT.pmthresholds.ms.farend.15min.FC | 10 (count) | 0 - 72 |
| ASAP_4.STM1-PORT.pmthresholds.ms.farend.15min.SES | 1 (seconds) | 0 - 900 |
| ASAP_4.STM1-PORT.pmthresholds.ms.farend.15min.UAS | 3 (seconds) | 0 - 900 |
| ASAP_4.STM1-PORT.pmthresholds.ms.farend.1day.BBE | 13120 (count) | 0 - 212371200 |
| ASAP_4.STM1-PORT.pmthresholds.ms.farend.1day.EB | 13120 (B2 count) | 0 - 212371200 |
| ASAP_4.STM1-PORT.pmthresholds.ms.farend.1day.ES | 864 (seconds) | 0 - 86400 |
| ASAP_4.STM1-PORT.pmthresholds.ms.farend.1day.FC | 40 (count) | 0 - 6912 |
| ASAP_4.STM1-PORT.pmthresholds.ms.farend.1day.SES | 4 (seconds) | 0 - 86400 |
| ASAP_4.STM1-PORT.pmthresholds.ms.farend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.15min.BBE | 1312 (count) | 0 - 2212200 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.15min.EB | 1312 (B2 count) | 0 - 2212200 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.15min.ES | 87 (seconds) | 0 - 900 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.15min.FC | 10 (count) | 0 - 72 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.15min.PSC | 1 (count) | 0 - 600 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.15min.PSD | 300 (seconds) | 0 - 600 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.15min.SES | 1 (seconds) | 0 - 900 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.15min.UAS | 3 (seconds) | 0 - 900 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.1day.BBE | 13120 (count) | 0 - 212371200 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.1day.EB | 13120 (B2 count) | 0 - 212371200 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.1day.ES | 864 (seconds) | 0 - 86400 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.1day.FC | 40 (count) | 0 - 6912 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.1day.PSC | 5 (count) | 0 - 57600 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.1day.PSD | 600 (seconds) | 0 - 86400 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.1day.SES | 4 (seconds) | 0 - 86400 |
| ASAP_4.STM1-PORT.pmthresholds.ms.nearend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM1-PORT.pmthresholds.path.farend.15min.BBE | 25 (count) | 0 - 2212200 |
| ASAP_4.STM1-PORT.pmthresholds.path.farend.15min.EB | 15 (B3 count) | 0 - 2160000 |
| ASAP_4.STM1-PORT.pmthresholds.path.farend.15min.ES | 12 (seconds) | 0 - 900 |
| ASAP_4.STM1-PORT.pmthresholds.path.farend.15min.FC | 10 (count) | 0 - 72 |

**Cisco ONS 15600 SDH Reference Manual, R8.0**

*Table C-4     ASAP Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| ASAP_4.STM1-PORT.pmthresholds.path.farend.15min.SES | 3 (seconds) | 0 - 900 |
| ASAP_4.STM1-PORT.pmthresholds.path.farend.15min.UAS | 10 (seconds) | 0 - 900 |
| ASAP_4.STM1-PORT.pmthresholds.path.farend.1day.BBE | 250 (count) | 0 - 212371200 |
| ASAP_4.STM1-PORT.pmthresholds.path.farend.1day.EB | 125 (B3 count) | 0 - 207360000 |
| ASAP_4.STM1-PORT.pmthresholds.path.farend.1day.ES | 100 (seconds) | 0 - 86400 |
| ASAP_4.STM1-PORT.pmthresholds.path.farend.1day.FC | 40 (count) | 0 - 6912 |
| ASAP_4.STM1-PORT.pmthresholds.path.farend.1day.SES | 7 (seconds) | 0 - 86400 |
| ASAP_4.STM1-PORT.pmthresholds.path.farend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.15min.BBE | 25 (count) | 0 - 2212200 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.15min.EB | 15 (B3 count) | 0 - 2160000 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.15min.ES | 12 (seconds) | 0 - 900 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.15min.FC | 10 (count) | 0 - 72 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.15min.NPJC-PDET | 60 (count) | 0 - 7200000 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.15min.NPJC-PGEN | 60 (count) | 0 - 7200000 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.15min.PPJC-PDET | 60 (count) | 0 - 7200000 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.15min.PPJC-PGEN | 60 (count) | 0 - 7200000 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.15min.SES | 3 (seconds) | 0 - 900 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.15min.UAS | 10 (seconds) | 0 - 900 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.1day.BBE | 250 (count) | 0 - 212371200 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.1day.EB | 125 (B3 count) | 0 - 207360000 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.1day.ES | 100 (seconds) | 0 - 86400 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.1day.FC | 40 (count) | 0 - 6912 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.1day.NPJC-PDET | 5760 (count) | 0 - 691200000 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.1day.NPJC-PGEN | 5760 (count) | 0 - 691200000 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.1day.PPJC-PDET | 5760 (count) | 0 - 691200000 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.1day.PPJC-PGEN | 5760 (count) | 0 - 691200000 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.1day.SES | 7 (seconds) | 0 - 86400 |
| ASAP_4.STM1-PORT.pmthresholds.path.nearend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM1-PORT.pmthresholds.rs.nearend.15min.BBE | 10000 (count) | 0 - 2212200 |
| ASAP_4.STM1-PORT.pmthresholds.rs.nearend.15min.EB | 10000 (B1 count) | 0 - 2151900 |
| ASAP_4.STM1-PORT.pmthresholds.rs.nearend.15min.ES | 500 (seconds) | 0 - 900 |
| ASAP_4.STM1-PORT.pmthresholds.rs.nearend.15min.OFS | 500 (seconds) | 0 - 900 |
| ASAP_4.STM1-PORT.pmthresholds.rs.nearend.15min.SES | 500 (seconds) | 0 - 900 |

*Table C-4     ASAP Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| ASAP_4.STM1-PORT.pmthresholds.rs.nearend.1day.BBE | 100000 (count) | 0 - 212371200 |
| ASAP_4.STM1-PORT.pmthresholds.rs.nearend.1day.EB | 100000 (B1 count) | 0 - 206582400 |
| ASAP_4.STM1-PORT.pmthresholds.rs.nearend.1day.ES | 5000 (seconds) | 0 - 86400 |
| ASAP_4.STM1-PORT.pmthresholds.rs.nearend.1day.OFS | 5000 (seconds) | 0 - 86400 |
| ASAP_4.STM1-PORT.pmthresholds.rs.nearend.1day.SES | 5000 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.config.line.AINSSoakTime | 08:00 (hours:mins) | 00:00, 00:15, 00:30 .. 48:00 |
| ASAP_4.STM16-PORT.config.line.AlsMode | Disabled | Disabled, Auto Restart, Manual Restart, Manual Restart for Test |
| ASAP_4.STM16-PORT.config.line.AlsRecoveryPulseDuration | 2.0 (seconds) | 2.0, 2.1, 2.2 .. 100.0 when AlsMode Disabled, Auto Restart, Manual Restart; 80.0, 80.1, 80.2 .. 100.0 when AlsMode Manual Restart for Test |
| ASAP_4.STM16-PORT.config.line.AlsRecoveryPulseInterval | 100 (seconds) | 60 - 300 |
| ASAP_4.STM16-PORT.config.line.SDBER | 1E-7 | 1E-5, 1E-6, 1E-7, 1E-8, 1E-9 |
| ASAP_4.STM16-PORT.config.line.SFBER | 1E-4 | 1E-3, 1E-4, 1E-5 |
| ASAP_4.STM16-PORT.config.line.SendDoNotUse | FALSE | TRUE, FALSE |
| ASAP_4.STM16-PORT.config.line.State | unlocked, automaticInService | unlocked, locked, disabled, locked, maintenance, unlocked, automaticInService |
| ASAP_4.STM16-PORT.config.line.SyncMsgIn | TRUE | FALSE, TRUE |
| ASAP_4.STM16-PORT.config.vc4.IPPMEnabled | FALSE | TRUE, FALSE |
| ASAP_4.STM16-PORT.physicalthresholds.alarm.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| ASAP_4.STM16-PORT.physicalthresholds.alarm.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| ASAP_4.STM16-PORT.physicalthresholds.alarm.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| ASAP_4.STM16-PORT.physicalthresholds.alarm.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| ASAP_4.STM16-PORT.physicalthresholds.alarm.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| ASAP_4.STM16-PORT.physicalthresholds.alarm.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| ASAP_4.STM16-PORT.physicalthresholds.warning.15min.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| ASAP_4.STM16-PORT.physicalthresholds.warning.15min.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |

*Table C-4    ASAP Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| ASAP_4.STM16-PORT.physicalthresholds.warning.15min.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| ASAP_4.STM16-PORT.physicalthresholds.warning.15min.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| ASAP_4.STM16-PORT.physicalthresholds.warning.15min.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| ASAP_4.STM16-PORT.physicalthresholds.warning.15min.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| ASAP_4.STM16-PORT.physicalthresholds.warning.1day.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| ASAP_4.STM16-PORT.physicalthresholds.warning.1day.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| ASAP_4.STM16-PORT.physicalthresholds.warning.1day.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| ASAP_4.STM16-PORT.physicalthresholds.warning.1day.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| ASAP_4.STM16-PORT.physicalthresholds.warning.1day.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| ASAP_4.STM16-PORT.physicalthresholds.warning.1day.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| ASAP_4.STM16-PORT.pmthresholds.ms.farend.15min.BBE | 21260 (count) | 0 - 2212200 |
| ASAP_4.STM16-PORT.pmthresholds.ms.farend.15min.EB | 21260 (B2 count) | 0 - 2212200 |
| ASAP_4.STM16-PORT.pmthresholds.ms.farend.15min.ES | 87 (seconds) | 0 - 900 |
| ASAP_4.STM16-PORT.pmthresholds.ms.farend.15min.FC | 10 (count) | 0 - 72 |
| ASAP_4.STM16-PORT.pmthresholds.ms.farend.15min.SES | 1 (seconds) | 0 - 900 |
| ASAP_4.STM16-PORT.pmthresholds.ms.farend.15min.UAS | 3 (seconds) | 0 - 900 |
| ASAP_4.STM16-PORT.pmthresholds.ms.farend.1day.BBE | 212600 (count) | 0 - 212371200 |
| ASAP_4.STM16-PORT.pmthresholds.ms.farend.1day.EB | 212600 (B2 count) | 0 - 212371200 |
| ASAP_4.STM16-PORT.pmthresholds.ms.farend.1day.ES | 864 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.ms.farend.1day.FC | 40 (count) | 0 - 6912 |
| ASAP_4.STM16-PORT.pmthresholds.ms.farend.1day.SES | 4 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.ms.farend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.15min.BBE | 21260 (count) | 0 - 2212200 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.15min.EB | 21260 (B2 count) | 0 - 2212200 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.15min.ES | 87 (seconds) | 0 - 900 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.15min.FC | 10 (count) | 0 - 72 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.15min.PSC | 1 (count) | 0 - 600 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.15min.PSC-W | 1 (count) | 0 - 600 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.15min.PSD | 300 (seconds) | 0 - 600 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.15min.PSD-W | 300 (seconds) | 0 - 900 |

*Table C-4*　　　*ASAP Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.15min.SES | 1 (seconds) | 0 - 900 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.15min.UAS | 3 (seconds) | 0 - 900 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.1day.BBE | 212600 (count) | 0 - 212371200 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.1day.EB | 212600 (B2 count) | 0 - 212371200 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.1day.ES | 864 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.1day.FC | 40 (count) | 0 - 6912 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.1day.PSC | 5 (count) | 0 - 57600 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.1day.PSC-W | 5 (count) | 0 - 57600 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.1day.PSD | 600 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.1day.PSD-W | 600 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.1day.SES | 4 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.ms.nearend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.path.farend.15min.BBE | 25 (count) | 0 - 2212200 |
| ASAP_4.STM16-PORT.pmthresholds.path.farend.15min.EB | 15 (B3 count) | 0 - 2160000 |
| ASAP_4.STM16-PORT.pmthresholds.path.farend.15min.ES | 12 (seconds) | 0 - 900 |
| ASAP_4.STM16-PORT.pmthresholds.path.farend.15min.FC | 10 (count) | 0 - 72 |
| ASAP_4.STM16-PORT.pmthresholds.path.farend.15min.SES | 3 (seconds) | 0 - 900 |
| ASAP_4.STM16-PORT.pmthresholds.path.farend.15min.UAS | 10 (seconds) | 0 - 900 |
| ASAP_4.STM16-PORT.pmthresholds.path.farend.1day.BBE | 250 (count) | 0 - 212371200 |
| ASAP_4.STM16-PORT.pmthresholds.path.farend.1day.EB | 125 (B3 count) | 0 - 207360000 |
| ASAP_4.STM16-PORT.pmthresholds.path.farend.1day.ES | 100 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.path.farend.1day.FC | 40 (count) | 0 - 6912 |
| ASAP_4.STM16-PORT.pmthresholds.path.farend.1day.SES | 7 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.path.farend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.15min.BBE | 25 (count) | 0 - 2212200 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.15min.EB | 15 (B3 count) | 0 - 2160000 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.15min.ES | 12 (seconds) | 0 - 900 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.15min.FC | 10 (count) | 0 - 72 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.15min.NPJC-PDET | 60 (count) | 0 - 7200000 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.15min.NPJC-PGEN | 60 (count) | 0 - 7200000 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.15min.PPJC-PDET | 60 (count) | 0 - 7200000 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.15min.PPJC-PGEN | 60 (count) | 0 - 7200000 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.15min.SES | 3 (seconds) | 0 - 900 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.15min.UAS | 10 (seconds) | 0 - 900 |

*Table C-4*    *ASAP Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.1day.BBE | 250 (count) | 0 - 2212200 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.1day.EB | 125 (B3 count) | 0 - 207360000 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.1day.ES | 100 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.1day.FC | 40 (count) | 0 - 6912 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.1day.NPJC-PDET | 5760 (count) | 0 - 691200000 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.1day.NPJC-PGEN | 5760 (count) | 0 - 691200000 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.1day.PPJC-PDET | 5760 (count) | 0 - 691200000 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.1day.PPJC-PGEN | 5760 (count) | 0 - 691200000 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.1day.SES | 7 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.path.nearend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.rs.nearend.15min.BBE | 10000 (count) | 0 - 2212200 |
| ASAP_4.STM16-PORT.pmthresholds.rs.nearend.15min.EB | 10000 (B1 count) | 0 - 2151900 |
| ASAP_4.STM16-PORT.pmthresholds.rs.nearend.15min.ES | 500 (seconds) | 0 - 900 |
| ASAP_4.STM16-PORT.pmthresholds.rs.nearend.15min.OFS | 500 (seconds) | 0 - 900 |
| ASAP_4.STM16-PORT.pmthresholds.rs.nearend.15min.SES | 500 (seconds) | 0 - 900 |
| ASAP_4.STM16-PORT.pmthresholds.rs.nearend.1day.BBE | 100000 (count) | 0 - 212371200 |
| ASAP_4.STM16-PORT.pmthresholds.rs.nearend.1day.EB | 100000 (B1 count) | 0 - 206582400 |
| ASAP_4.STM16-PORT.pmthresholds.rs.nearend.1day.ES | 5000 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.rs.nearend.1day.OFS | 5000 (seconds) | 0 - 86400 |
| ASAP_4.STM16-PORT.pmthresholds.rs.nearend.1day.SES | 5000 (seconds) | 0 - 86400 |
| ASAP_4.STM4-PORT.config.line.AINSSoakTime | 08:00 (hours:mins) | 00:00, 00:15, 00:30 .. 48:00 |
| ASAP_4.STM4-PORT.config.line.AlsMode | Disabled | Disabled, Auto Restart, Manual Restart, Manual Restart for Test |
| ASAP_4.STM4-PORT.config.line.AlsRecoveryPulseDuration | 2.0 (seconds) | 2.0, 2.1, 2.2 .. 100.0 when AlsMode Disabled, Auto Restart, Manual Restart; 80.0, 80.1, 80.2 .. 100.0 when AlsMode Manual Restart for Test |
| ASAP_4.STM4-PORT.config.line.AlsRecoveryPulseInterval | 100 (seconds) | 60 - 300 |
| ASAP_4.STM4-PORT.config.line.SDBER | 1E-7 | 1E-5, 1E-6, 1E-7, 1E-8, 1E-9 |
| ASAP_4.STM4-PORT.config.line.SFBER | 1E-4 | 1E-3, 1E-4, 1E-5 |
| ASAP_4.STM4-PORT.config.line.SendDoNotUse | FALSE | TRUE, FALSE |

*Table C-4* **ASAP Card Default Settings (continued)**

| Default Name | Default Value | Default Domain |
|---|---|---|
| ASAP_4.STM4-PORT.config.line.State | unlocked, automaticInService | unlocked, locked, disabled, locked, maintenance, unlocked, automaticInService |
| ASAP_4.STM4-PORT.config.line.SyncMsgIn | TRUE | FALSE, TRUE |
| ASAP_4.STM4-PORT.config.vc4.IPPMEnabled | FALSE | TRUE, FALSE |
| ASAP_4.STM4-PORT.physicalthresholds.alarm.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| ASAP_4.STM4-PORT.physicalthresholds.alarm.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| ASAP_4.STM4-PORT.physicalthresholds.alarm.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| ASAP_4.STM4-PORT.physicalthresholds.alarm.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| ASAP_4.STM4-PORT.physicalthresholds.alarm.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| ASAP_4.STM4-PORT.physicalthresholds.alarm.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| ASAP_4.STM4-PORT.physicalthresholds.warning.15min.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| ASAP_4.STM4-PORT.physicalthresholds.warning.15min.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| ASAP_4.STM4-PORT.physicalthresholds.warning.15min.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| ASAP_4.STM4-PORT.physicalthresholds.warning.15min.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| ASAP_4.STM4-PORT.physicalthresholds.warning.15min.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| ASAP_4.STM4-PORT.physicalthresholds.warning.15min.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| ASAP_4.STM4-PORT.physicalthresholds.warning.1day.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| ASAP_4.STM4-PORT.physicalthresholds.warning.1day.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| ASAP_4.STM4-PORT.physicalthresholds.warning.1day.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| ASAP_4.STM4-PORT.physicalthresholds.warning.1day.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| ASAP_4.STM4-PORT.physicalthresholds.warning.1day.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| ASAP_4.STM4-PORT.physicalthresholds.warning.1day.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| ASAP_4.STM4-PORT.pmthresholds.ms.farend.15min.BBE | 5315 (count) | 0 - 2212200 |
| ASAP_4.STM4-PORT.pmthresholds.ms.farend.15min.EB | 5315 (B2 count) | 0 - 2212200 |
| ASAP_4.STM4-PORT.pmthresholds.ms.farend.15min.ES | 87 (seconds) | 0 - 900 |
| ASAP_4.STM4-PORT.pmthresholds.ms.farend.15min.FC | 10 (count) | 0 - 72 |
| ASAP_4.STM4-PORT.pmthresholds.ms.farend.15min.SES | 1 (seconds) | 0 - 900 |
| ASAP_4.STM4-PORT.pmthresholds.ms.farend.15min.UAS | 3 (seconds) | 0 - 900 |

**Cisco ONS 15600 SDH Reference Manual, R8.0**

*Table C-4 ASAP Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| ASAP_4.STM4-PORT.pmthresholds.ms.farend.1day.BBE | 53150 (count) | 0 - 212371200 |
| ASAP_4.STM4-PORT.pmthresholds.ms.farend.1day.EB | 53150 (B2 count) | 0 - 212371200 |
| ASAP_4.STM4-PORT.pmthresholds.ms.farend.1day.ES | 864 (seconds) | 0 - 86400 |
| ASAP_4.STM4-PORT.pmthresholds.ms.farend.1day.FC | 40 (count) | 0 - 6912 |
| ASAP_4.STM4-PORT.pmthresholds.ms.farend.1day.SES | 4 (seconds) | 0 - 86400 |
| ASAP_4.STM4-PORT.pmthresholds.ms.farend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.15min.BBE | 5315 (count) | 0 - 2212200 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.15min.EB | 5315 (B2 count) | 0 - 2212200 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.15min.ES | 87 (seconds) | 0 - 900 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.15min.FC | 10 (count) | 0 - 72 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.15min.PSC | 1 (count) | 0 - 600 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.15min.PSD | 300 (seconds) | 0 - 600 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.15min.SES | 1 (seconds) | 0 - 900 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.15min.UAS | 3 (seconds) | 0 - 900 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.1day.BBE | 53150 (count) | 0 - 212371200 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.1day.EB | 53150 (B2 count) | 0 - 212371200 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.1day.ES | 864 (seconds) | 0 - 86400 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.1day.FC | 40 (count) | 0 - 6912 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.1day.PSC | 5 (count) | 0 - 57600 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.1day.PSD | 600 (seconds) | 0 - 86400 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.1day.SES | 4 (seconds) | 0 - 86400 |
| ASAP_4.STM4-PORT.pmthresholds.ms.nearend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM4-PORT.pmthresholds.path.farend.15min.BBE | 25 (count) | 0 - 2212200 |
| ASAP_4.STM4-PORT.pmthresholds.path.farend.15min.EB | 15 (B3 count) | 0 - 2160000 |
| ASAP_4.STM4-PORT.pmthresholds.path.farend.15min.ES | 12 (seconds) | 0 - 900 |
| ASAP_4.STM4-PORT.pmthresholds.path.farend.15min.FC | 10 (count) | 0 - 72 |
| ASAP_4.STM4-PORT.pmthresholds.path.farend.15min.SES | 3 (seconds) | 0 - 900 |
| ASAP_4.STM4-PORT.pmthresholds.path.farend.15min.UAS | 10 (seconds) | 0 - 900 |
| ASAP_4.STM4-PORT.pmthresholds.path.farend.1day.BBE | 250 (count) | 0 - 212371200 |
| ASAP_4.STM4-PORT.pmthresholds.path.farend.1day.EB | 125 (B3 count) | 0 - 207360000 |
| ASAP_4.STM4-PORT.pmthresholds.path.farend.1day.ES | 100 (seconds) | 0 - 86400 |
| ASAP_4.STM4-PORT.pmthresholds.path.farend.1day.FC | 40 (count) | 0 - 6912 |
| ASAP_4.STM4-PORT.pmthresholds.path.farend.1day.SES | 7 (seconds) | 0 - 86400 |

*Table C-4      ASAP Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| ASAP_4.STM4-PORT.pmthresholds.path.farend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.15min.BBE | 25 (count) | 0 - 2212200 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.15min.EB | 15 (B3 count) | 0 - 2160000 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.15min.ES | 12 (seconds) | 0 - 900 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.15min.FC | 10 (count) | 0 - 72 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.15min.NPJC-PDET | 60 (count) | 0 - 7200000 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.15min.NPJC-PGEN | 60 (count) | 0 - 7200000 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.15min.PPJC-PDET | 60 (count) | 0 - 7200000 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.15min.PPJC-PGEN | 60 (count) | 0 - 7200000 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.15min.SES | 3 (seconds) | 0 - 900 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.15min.UAS | 10 (seconds) | 0 - 900 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.1day.BBE | 250 (count) | 0 - 212371200 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.1day.EB | 125 (B3 count) | 0 - 207360000 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.1day.ES | 100 (seconds) | 0 - 86400 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.1day.FC | 40 (count) | 0 - 6912 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.1day.NPJC-PDET | 5760 (count) | 0 - 691200000 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.1day.NPJC-PGEN | 5760 (count) | 0 - 691200000 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.1day.PPJC-PDET | 5760 (count) | 0 - 691200000 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.1day.PPJC-PGEN | 5760 (count) | 0 - 691200000 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.1day.SES | 7 (seconds) | 0 - 86400 |
| ASAP_4.STM4-PORT.pmthresholds.path.nearend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM4-PORT.pmthresholds.rs.nearend.15min.BBE | 10000 (count) | 0 - 2212200 |
| ASAP_4.STM4-PORT.pmthresholds.rs.nearend.15min.EB | 10000 (B1 count) | 0 - 2151900 |
| ASAP_4.STM4-PORT.pmthresholds.rs.nearend.15min.ES | 500 (seconds) | 0 - 900 |
| ASAP_4.STM4-PORT.pmthresholds.rs.nearend.15min.OFS | 500 (seconds) | 0 - 900 |
| ASAP_4.STM4-PORT.pmthresholds.rs.nearend.15min.SES | 500 (seconds) | 0 - 900 |
| ASAP_4.STM4-PORT.pmthresholds.rs.nearend.1day.BBE | 100000 (count) | 0 - 212371200 |
| ASAP_4.STM4-PORT.pmthresholds.rs.nearend.1day.EB | 100000 (B1 count) | 0 - 206582400 |
| ASAP_4.STM4-PORT.pmthresholds.rs.nearend.1day.ES | 5000 (seconds) | 0 - 86400 |
| ASAP_4.STM4-PORT.pmthresholds.rs.nearend.1day.OFS | 5000 (seconds) | 0 - 86400 |
| ASAP_4.STM4-PORT.pmthresholds.rs.nearend.1day.SES | 5000 (seconds) | 0 - 86400 |

*Table C-4*     ***ASAP Card Default Settings (continued)***

| Default Name | Default Value | Default Domain |
|---|---|---|
| ASAP_4.STM64-PORT.config.line.AINSSoakTime | 08:00 (hours:mins) | 00:00, 00:15, 00:30 .. 48:00 |
| ASAP_4.STM64-PORT.config.line.AlsMode | Disabled | Disabled, Auto Restart, Manual Restart, Manual Restart for Test |
| ASAP_4.STM64-PORT.config.line.AlsRecoveryPulseDuration | 2.0 (seconds) | 2.0, 2.1, 2.2 .. 100.0 when AlsMode Disabled, Auto Restart, Manual Restart; 80.0, 80.1, 80.2 .. 100.0 when AlsMode Manual Restart for Test |
| ASAP_4.STM64-PORT.config.line.AlsRecoveryPulseInterval | 100 (seconds) | 60 - 300 |
| ASAP_4.STM64-PORT.config.line.SDBER | 1E-7 | 1E-5, 1E-6, 1E-7, 1E-8, 1E-9 |
| ASAP_4.STM64-PORT.config.line.SFBER | 1E-4 | 1E-3, 1E-4, 1E-5 |
| ASAP_4.STM64-PORT.config.line.SendDoNotUse | FALSE | TRUE, FALSE |
| ASAP_4.STM64-PORT.config.line.State | unlocked, automaticInService | unlocked, locked, disabled, locked, maintenance, unlocked, automaticInService |
| ASAP_4.STM64-PORT.config.line.SyncMsgIn | TRUE | FALSE, TRUE |
| ASAP_4.STM64-PORT.config.vc4.IPPMEnabled | FALSE | TRUE, FALSE |
| ASAP_4.STM64-PORT.physicalthresholds.alarm.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| ASAP_4.STM64-PORT.physicalthresholds.alarm.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| ASAP_4.STM64-PORT.physicalthresholds.alarm.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| ASAP_4.STM64-PORT.physicalthresholds.alarm.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| ASAP_4.STM64-PORT.physicalthresholds.alarm.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| ASAP_4.STM64-PORT.physicalthresholds.alarm.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| ASAP_4.STM64-PORT.physicalthresholds.warning.15min.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| ASAP_4.STM64-PORT.physicalthresholds.warning.15min.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |
| ASAP_4.STM64-PORT.physicalthresholds.warning.15min.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| ASAP_4.STM64-PORT.physicalthresholds.warning.15min.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| ASAP_4.STM64-PORT.physicalthresholds.warning.15min.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| ASAP_4.STM64-PORT.physicalthresholds.warning.15min.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| ASAP_4.STM64-PORT.physicalthresholds.warning.1day.LBC-HIGH | 200 (%) | LBC-LOW, LBC-LOW + 1, LBC-LOW + 2 .. 255 |
| ASAP_4.STM64-PORT.physicalthresholds.warning.1day.LBC-LOW | 20 (%) | 0, 1, 2 .. LBC-HIGH |

*Table C-4      ASAP Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| ASAP_4.STM64-PORT.physicalthresholds.warning.1day.OPR-HIGH | 200 (%) | OPR-LOW, OPR-LOW + 1, OPR-LOW + 2 .. 255 |
| ASAP_4.STM64-PORT.physicalthresholds.warning.1day.OPR-LOW | 50 (%) | 0, 1, 2 .. OPR-HIGH |
| ASAP_4.STM64-PORT.physicalthresholds.warning.1day.OPT-HIGH | 120 (%) | OPT-LOW, OPT-LOW + 1, OPT-LOW + 2 .. 255 |
| ASAP_4.STM64-PORT.physicalthresholds.warning.1day.OPT-LOW | 80 (%) | 0, 1, 2 .. OPT-HIGH |
| ASAP_4.STM64-PORT.pmthresholds.ms.farend.15min.BBE | 85040 (count) | 0 - 2212200 |
| ASAP_4.STM64-PORT.pmthresholds.ms.farend.15min.EB | 85040 (B2 count) | 0 - 2212200 |
| ASAP_4.STM64-PORT.pmthresholds.ms.farend.15min.ES | 87 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.ms.farend.15min.FC | 10 (count) | 0 - 72 |
| ASAP_4.STM64-PORT.pmthresholds.ms.farend.15min.SES | 1 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.ms.farend.15min.UAS | 3 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.ms.farend.1day.BBE | 850400 (count) | 0 - 212371200 |
| ASAP_4.STM64-PORT.pmthresholds.ms.farend.1day.EB | 850400 (B2 count) | 0 - 212371200 |
| ASAP_4.STM64-PORT.pmthresholds.ms.farend.1day.ES | 864 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.ms.farend.1day.FC | 40 (count) | 0 - 6912 |
| ASAP_4.STM64-PORT.pmthresholds.ms.farend.1day.SES | 4 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.ms.farend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.15min.BBE | 85040 (count) | 0 - 2212200 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.15min.EB | 85040 (B2 count) | 0 - 2212200 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.15min.ES | 87 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.15min.FC | 10 (count) | 0 - 72 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.15min.PSC | 1 (count) | 0 - 600 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.15min.PSC-W | 1 (count) | 0 - 600 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.15min.PSD | 300 (seconds) | 0 - 600 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.15min.PSD-W | 300 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.15min.SES | 1 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.15min.UAS | 3 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.1day.BBE | 850400 (count) | 0 - 212371200 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.1day.EB | 850400 (B2 count) | 0 - 212371200 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.1day.ES | 864 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.1day.FC | 40 (count) | 0 - 6912 |

*Table C-4*    *ASAP Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.1day.PSC | 5 (count) | 0 - 57600 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.1day.PSC-W | 5 (count) | 0 - 57600 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.1day.PSD | 600 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.1day.PSD-W | 600 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.1day.SES | 4 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.ms.nearend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.path.farend.15min.BBE | 25 (count) | 0 - 2212200 |
| ASAP_4.STM64-PORT.pmthresholds.path.farend.15min.EB | 15 (B3 count) | 0 - 2160000 |
| ASAP_4.STM64-PORT.pmthresholds.path.farend.15min.ES | 12 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.path.farend.15min.FC | 10 (count) | 0 - 72 |
| ASAP_4.STM64-PORT.pmthresholds.path.farend.15min.SES | 3 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.path.farend.15min.UAS | 10 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.path.farend.1day.BBE | 250 (count) | 0 - 212371200 |
| ASAP_4.STM64-PORT.pmthresholds.path.farend.1day.EB | 125 (B3 count) | 0 - 207360000 |
| ASAP_4.STM64-PORT.pmthresholds.path.farend.1day.ES | 100 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.path.farend.1day.FC | 40 (count) | 0 - 6912 |
| ASAP_4.STM64-PORT.pmthresholds.path.farend.1day.SES | 7 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.path.farend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.15min.BBE | 25 (count) | 0 - 2212200 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.15min.EB | 15 (B3 count) | 0 - 2160000 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.15min.ES | 12 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.15min.FC | 10 (count) | 0 - 72 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.15min.NPJC-PDET | 60 (count) | 0 - 7200000 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.15min.NPJC-PGEN | 60 (count) | 0 - 7200000 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.15min.PPJC-PDET | 60 (count) | 0 - 7200000 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.15min.PPJC-PGEN | 60 (count) | 0 - 7200000 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.15min.SES | 3 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.15min.UAS | 10 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.1day.BBE | 250 (count) | 0 - 212371200 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.1day.EB | 125 (B3 count) | 0 - 207360000 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.1day.ES | 100 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.1day.FC | 40 (count) | 0 - 6912 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.1day.NPJC-PDET | 5760 (count) | 0 - 691200000 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.1day.NPJC-PGEN | 5760 (count) | 0 - 691200000 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.1day.PPJC-PDET | 5760 (count) | 0 - 691200000 |

*Table C-4       ASAP Card Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.1day.PPJC-PGEN | 5760 (count) | 0 - 691200000 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.1day.SES | 7 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.path.nearend.1day.UAS | 10 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.rs.nearend.15min.BBE | 10000 (count) | 0 - 2212200 |
| ASAP_4.STM64-PORT.pmthresholds.rs.nearend.15min.EB | 10000 (B1 count) | 0 - 2151900 |
| ASAP_4.STM64-PORT.pmthresholds.rs.nearend.15min.ES | 500 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.rs.nearend.15min.OFS | 500 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.rs.nearend.15min.SES | 500 (seconds) | 0 - 900 |
| ASAP_4.STM64-PORT.pmthresholds.rs.nearend.1day.BBE | 100000 (count) | 0 - 212371200 |
| ASAP_4.STM64-PORT.pmthresholds.rs.nearend.1day.EB | 100000 (B1 count) | 0 - 206582400 |
| ASAP_4.STM64-PORT.pmthresholds.rs.nearend.1day.ES | 5000 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.rs.nearend.1day.OFS | 5000 (seconds) | 0 - 86400 |
| ASAP_4.STM64-PORT.pmthresholds.rs.nearend.1day.SES | 5000 (seconds) | 0 - 86400 |

# C.3  Node Default Settings

Table C-5 on page C-29 lists the node-level default settings for the Cisco ONS 15600 SDH. Cisco provides the following user-configurable defaults for each Cisco ONS 15600 SDH node:

- Circuit settings—Set the administrative state and subnetwork connection protection (SNCP) circuit defaults.

- General settings—Set general node management defaults, including whether to use Daylight Savings Time (DST), the IP address of the Network Time Protocol/Simple Network Time Protocol (NTP/SNTP) server to be used, the time zone where the node is located, the signal degrade (SD) path bit error rate (BER) value, the defaults description, whether automatic autonomous Transcation Language One (TL1) reporting of PM data is enabled for cross-connect paths on the node, whether or not to allow ports to be disabled when they are providing services (when the default is set to FALSE users must remove or disable the services first, then put the ports out of service), and whether to report loopback conditions on ports in the Locked,maintenance state.

- Network settings—Set default gateway node type, and whether to raise an alarm when the backplane LAN cable is disconnected.

- OSI settings—Set the Open System Interconnection (OSI) main setup, generic routing encapsulation (GRE) tunnel default, the link access protocol on the D channel (LAP-D), the router subnet, and the TID address resolution protocol (TARP) settings.

- 1+1 protection settings—Set whether or not protected circuits have bidirectional switching, are revertive, and what the reversion time is.

- MS-SPRing protection settings—Set whether MS-SPRing-protected circuits are revertive, and what the reversion time is, at both the ring and span levels.

- Legal Disclaimer—Set the legal disclaimer that warns users at the login screen about the possible legal or contractual ramifications of accessing equipment, systems, or networks without authorization.

- Power Monitor—Set the power monitoring settings for the node.

- Security Grant Permissions—Set default user security levels for activating/reverting software, PM data clearing, database restoring, and retrieving audit logs.

- Security Access settings—Set default security settings for LAN access, shell access, serial craft access, element management system (EMS) access (including Internet Inter-Object Request Broker Protocol [IIOP] listener port number), TL1 access, and Simple Network Management Protocol (SNMP) access.

- Security RADIUS settings—Set default RADIUS server settings for the accounting port number and the authentication port number, and whether to enable the node as a final authenticator.

- Security Policy settings—Set the allowable failed logins before lockout, idle user timeout for each user level, optional lockout duration or manual unlock enabled, password reuse and change frequency policies, number of characters difference that is required between the old and new password, password aging by security level, enforced single concurrent session per user, and option to disable inactive user after a set inactivity period.

- Security Password settings—Set when passwords can be changed, how many characters they must differ by, whether or not password reuse is allowed, and whether a password change is required on first login to a new account; set password aging enforcement and user-level specific aging and warning periods; set how many consecutive identical characters are allowed in a password, maximum password length, minimum password length, minimum number and combination of nonalphabetical characters required, and whether or not to allow a password that is a reversal of the login ID associated with the password.

- BITS Timing settings—Set the coding, framing, state, Admin synchronization status messaging (SSM), AISThreshold, CableType, FacilityType, line build out, and Sa bit settings for building integrated timing supply 1 (BITS-1) and BITS2 timing.

- General Timing settings—Set the mode (External, Line, or Mixed), quality of reserved (RES) timing (the rule that defines the order of clock quality from lowest to highest), revertive, reversion time, and SSM message set for node timing.

**Note** Any node level defaults changed using the **Provisioning > Defaults** tab, changes existing node level provisioning. Although this is service affecting, it depends on the type of defaults changed, for example, general, and all timing and security attributes. The "Changing default values for some node level attributes overrides the current provisioning." message is displayed. The Side Effects column of the Defaults editor (right-click a column header and select **Show Column > Side Effects**) explains the effect of changing the default values. However, when the card level defaults are changed using the **Provisioning > Defaults** tab, existing card provisioning remains unaffected.

**Note** For more information about each individual node setting, refer to the "Change Node Settings" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

*Table C-5        Node Default Settings*

| Default Name | Default Value | Default Domain |
|---|---|---|
| NODE.circuits.State | unlocked, automaticInService | unlocked, locked, disabled, locked, maintenance, unlocked, automaticInService |
| NODE.circuits.sncp.HO_SDBER | 1E-6 | 1E-5, 1E-6, 1E-7, 1E-8, 1E-9 |
| NODE.circuits.sncp.HO_SFBER | 1E-4 | 1E-3, 1E-4, 1E-5 |
| NODE.circuits.sncp.ReversionTime | 5.0 (minutes) | 0.5, 1.0, 1.5 .. 12.0 |
| NODE.circuits.sncp.Revertive | FALSE | TRUE, FALSE |
| NODE.general.AllowServiceAffectingPortChangeToDisabled | TRUE | FALSE, TRUE |
| NODE.general.AutoPM | FALSE | FALSE, TRUE |
| NODE.general.DefaultsDescription | Factory Defaults | Free form field |
| NODE.general.NtpSntpServer | 0.0.0.0 | IP Address |
| NODE.general.ReportLoopbackConditionsOnOOS-MTPorts | FALSE | FALSE, TRUE |
| NODE.general.TimeZone | (GMT-06:00) Central Time (US & Canada) | (For applicable time zones, see Table C-6 on page C-36.) |
| NODE.general.UseDST | TRUE | TRUE, FALSE |
| NODE.network.general.AlarmMissingBackplaneLAN | FALSE | TRUE, FALSE |
| NODE.network.general.GatewaySettings | None | LeaveAsIs, None, ENE, GNE, ProxyOnlyNode |
| NODE.osi.greTunnel.OspfCost | 110 | 110, 111, 112 .. 65535 |
| NODE.osi.greTunnel.SubnetMask | 24 (bits) | 8, 9, 10 .. 32 |
| NODE.osi.lapd.MTU | 512 | 512, 513, 514 .. 1500 |
| NODE.osi.lapd.Mode | AITS | AITS, UITS |
| NODE.osi.lapd.Role | Network | Network, User |
| NODE.osi.lapd.T200 | 200 (ms) | 200, 300, 400 .. 20000 |
| NODE.osi.lapd.T203 | 10000 (ms) | 4000, 4100, 4200 .. 120000 |
| NODE.osi.mainSetup.L1L2LSPBufferSize | 512 (bytes) | 512 - 1500 |
| NODE.osi.mainSetup.L1LSPBufferSize | 512 (bytes) | 512 - 1500 |
| NODE.osi.mainSetup.NodeRoutingMode | Intermediate System Level 1/Level 2 | Intermediate System Level 1, Intermediate System Level 1/Level 2 |
| NODE.osi.subnet.DISPriority | 63 | 1, 2, 3 .. 127 |

*Table C-5* **Node Default Settings (continued)**

| Default Name | Default Value | Default Domain |
|---|---|---|
| NODE.osi.subnet.ESH | 10 (sec) | 10, 20, 30 .. 1000 |
| NODE.osi.subnet.IIH | 3 (sec) | 1, 2, 3 .. 600 |
| NODE.osi.subnet.ISH | 10 (sec) | 10, 20, 30 .. 1000 |
| NODE.osi.subnet.LANISISCost | 20 | 1, 2, 3 .. 63 |
| NODE.osi.subnet.LDCCISISCost | 40 | 1, 2, 3 .. 63 |
| NODE.osi.subnet.SDCCISISCost | 60 | 1, 2, 3 .. 63 |
| NODE.osi.tarp.L1DataCache | TRUE | FALSE, TRUE |
| NODE.osi.tarp.L2DataCache | FALSE | FALSE, TRUE |
| NODE.osi.tarp.LANStormSuppression | TRUE | FALSE, TRUE |
| NODE.osi.tarp.LDB | TRUE | FALSE, TRUE |
| NODE.osi.tarp.LDBEntry | 5 (min) | 1 - 10 |
| NODE.osi.tarp.LDBFlush | 5 (min) | 0 - 1440 |
| NODE.osi.tarp.PDUsL1Propagation | TRUE | FALSE, TRUE |
| NODE.osi.tarp.PDUsL2Propagation | TRUE | FALSE, TRUE |
| NODE.osi.tarp.PDUsOrigination | TRUE | FALSE, TRUE |
| NODE.osi.tarp.T1Timer | 15 (sec) | 0 - 3600 |
| NODE.osi.tarp.T2Timer | 25 (sec) | 0 - 3600 |
| NODE.osi.tarp.T3Timer | 40 (sec) | 0 - 3600 |
| NODE.osi.tarp.T4Timer | 20 (sec) | 0 - 3600 |
| NODE.osi.tarp.Type4PDUDelay | 0 (sec) | 0 - 255 |
| NODE.powerMonitor.EHIBATVG | -72.0 (Vdc) | -40.5, -41.0, -41.5 .. -72.0 |
| NODE.powerMonitor.ELWBATVG | -40.5 (Vdc) | -40.5, -41.0, -41.5 .. -72.0 |
| NODE.protection.1+1.BidirectionalSwitching | FALSE | TRUE, FALSE |
| NODE.protection.1+1.ReversionTime | 5.0 (minutes) | 0.5, 1.0, 1.5 .. 12.0 |
| NODE.protection.1+1.Revertive | FALSE | TRUE, FALSE |
| NODE.protection.msspr.RingReversionTime | 5.0 (minutes) | 0.5, 1.0, 1.5 .. 12.0 |
| NODE.protection.msspr.RingRevertive | TRUE | TRUE, FALSE |
| NODE.security.emsAccess.AccessState | NonSecure | NonSecure, Secure |
| NODE.security.emsAccess.IIOPListenerPort (May reboot node) | 57790 (port #) | 0 - 65535 |
| NODE.security.grantPermission.ActivateRevertSoftware | Superuser | Provisioning, Superuser |
| NODE.security.grantPermission.PMClearingPrivilege | Provisioning | Provisioning, Superuser |
| NODE.security.grantPermission.RestoreDB | Superuser | Provisioning, Superuser |

***Table C-5 Node Default Settings (continued)***

| Default Name | Default Value | Default Domain |
|---|---|---|
| NODE.security.grantPermission.RetrieveAuditLog | Superuser | Provisioning, Superuser |
| NODE.security.idleUserTimeout.Maintenance | 01:00 (hours:mins) | 00:00, 00:01, 00:02 .. 16:39 |
| NODE.security.idleUserTimeout.Provisioning | 00:30 (hours:mins) | 00:00, 00:01, 00:02 .. 16:39 |
| NODE.security.idleUserTimeout.Retrieve | 00:00 (hours:mins) | 00:00, 00:01, 00:02 .. 16:39 |
| NODE.security.idleUserTimeout.Superuser | 00:15 (hours:mins) | 00:00, 00:01, 00:02 .. 16:39 |
| NODE.security.lanAccess.LANAccess (May disconnect CTC from node) | Front & Backplane | No LAN Access, Front Only, Backplane Only, Front & Backplane |
| NODE.security.lanAccess.RestoreTimeout | 5 (minutes) | 0 - 60 |
| NODE.security.legalDisclaimer.LoginWarningMessage | &lt;html&gt;&lt;center&gt;&lt;b&gt;WARNING&lt;/b&gt;&lt;/center&gt;This system is restricted to authorized users for business purposes. Unauthorized&lt;p&gt;access is a violation of the law. This service may be monitored for administrative&lt;p&gt;and security reasons. By proceeding, you consent to this monitoring. | Free form field |
| NODE.security.other.DisableInactiveUser | FALSE | FALSE, TRUE |
| NODE.security.other.InactiveDuration | 45 (days) | 1, 2, 3 .. 99 when nothing TRUE; 45 when nothing FALSE |
| NODE.security.other.SingleSessionPerUser | FALSE | TRUE, FALSE |

*Table C-5      Node Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| NODE.security.passwordAging.EnforcePasswordAging | FALSE | TRUE, FALSE |
| NODE.security.passwordAging.maintenance.AgingPeriod | 45 (days) | 20 - 90 |
| NODE.security.passwordAging.maintenance.WarningPeriod | 5 (days) | 2 - 20 |
| NODE.security.passwordAging.provisioning.AgingPeriod | 45 (days) | 20 - 90 |
| NODE.security.passwordAging.provisioning.WarningPeriod | 5 (days) | 2 - 20 |
| NODE.security.passwordAging.retrieve.AgingPeriod | 45 (days) | 20 - 90 |
| NODE.security.passwordAging.retrieve.WarningPeriod | 5 (days) | 2 - 20 |
| NODE.security.passwordAging.superuser.AgingPeriod | 45 (days) | 20 - 90 |
| NODE.security.passwordAging.superuser.WarningPeriod | 5 (days) | 2 - 20 |
| NODE.security.passwordChange.CannotChangeNewPassword | FALSE | TRUE, FALSE |
| NODE.security.passwordChange.CannotChangeNewPasswordForNDays | 20 (days) | 20 - 95 |
| NODE.security.passwordChange.NewPasswordMustDifferFromOldByNCharacters | 1 (characters) | 1 - 20 |
| NODE.security.passwordChange.PreventReusingLastNPasswords | 1 (times) | 1 - 10 |
| NODE.security.passwordChange.RequirePasswordChangeOnFirstLoginToNewAccount | FALSE | TRUE, FALSE |
| NODE.security.passwordComplexity.IdenticalConsecutiveCharactersAllowed | 3 or more | 0-2, 3 or more |
| NODE.security.passwordComplexity.MaximumLength | 20 | 20, 80 |
| NODE.security.passwordComplexity.MinimumLength | 6 | 6, 8, 10, 12 |
| NODE.security.passwordComplexity.MinimumRequiredCharacters | 1 num, 1 letter & 1 TL1 special | 1 num, 1 letter & 1 TL1 special, 1 num, 1 letter & 1 special, 2 each of any 2 of num, upper, lower & TL1 special, 2 each of any 2 of num, upper, lower & special |
| NODE.security.passwordComplexity.ReverseUserIdAllowed | TRUE | TRUE, FALSE |
| NODE.security.radiusServer.AccountingPort | 1813 (port) | 0 - 32767 |
| NODE.security.radiusServer.AuthenticationPort | 1812 (port) | 0 - 32767 |
| NODE.security.radiusServer.EnableNodeAsFinalAuthenticator | TRUE | FALSE, TRUE |
| NODE.security.serialCraftAccess.EnableCraftPortA | TRUE | TRUE, FALSE |
| NODE.security.serialCraftAccess.EnableCraftPortB | TRUE | TRUE, FALSE |
| NODE.security.shellAccess.AccessState | NonSecure | Disabled, NonSecure, Secure |
| NODE.security.shellAccess.EnableShellPassword | FALSE | TRUE, FALSE |
| NODE.security.shellAccess.TelnetPort | 23 | 23 - 9999 |
| NODE.security.snmpAccess.AccessState | NonSecure | Disabled, NonSecure |
| NODE.security.tl1Access.AccessState | NonSecure | Disabled, NonSecure, Secure |

*Table C-5 Node Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| NODE.security.userLockout.FailedLoginsAllowedBeforeLockout | 5 (times) | 0 - 10 |
| NODE.security.userLockout.LockoutDuration | 00:30 (mins:secs) | 00:00, 00:05, 00:10 .. 10:00 |
| NODE.security.userLockout.ManualUnlockBySuperuser | FALSE | TRUE, FALSE |
| NODE.timing.bits-1.AISThreshold | G812L | G811, STU, G812T, G812L, SETS, DUS |
| NODE.timing.bits-1.AdminSSMIn | STU | G811, STU, G812T, G812L, SETS, DUS |
| NODE.timing.bits-1.CableType | 120 ohm | 75 ohm, 120 ohm when nothing E1; 100 ohm when nothing DS1; 75 ohm, 120 ohm when nothing 2MHz; 120 ohm when nothing 64kHz+8kHz |
| NODE.timing.bits-1.Coding | HDB3 | B8ZS, AMI when FacilityType DS1; HDB3, AMI when FacilityType E1; N/A when FacilityType 2MHz; AMI when FacilityType 64kHz+8kHz |
| NODE.timing.bits-1.CodingOut | HDB3 | B8ZS, AMI when FacilityTypeOut DS1; HDB3, AMI when FacilityTypeOut E1; N/A when FacilityTypeOut 2MHz; AMI when FacilityTypeOut 64kHz+8kHz |
| NODE.timing.bits-1.FacilityType | E1 | DS1, E1, 64kHz+8kHz, 2MHz |
| NODE.timing.bits-1.FacilityTypeOut | E1 | DS1, E1, 64kHz+8kHz, 2MHz |
| NODE.timing.bits-1.Framing | FAS+CAS+CRC | ESF, D4 when FacilityType DS1; FAS+CRC, FAS+CAS, FAS+CAS+CRC, FAS, Unframed when FacilityType E1; N/A when FacilityType 2MHz; N/A when FacilityType 64kHz+8kHz |

**Cisco ONS 15600 SDH Reference Manual, R8.0**

*Table C-5        Node Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| NODE.timing.bits-1.FramingOut | FAS+CAS+ CRC | ESF, D4 when FacilityTypeOut DS1; FAS+CRC, FAS+CAS, FAS+CAS+CRC, FAS, Unframed when FacilityTypeOut E1; N/A when FacilityTypeOut 2MHz; N/A when FacilityTypeOut 64kHz+8kHz |
| NODE.timing.bits-1.LBO | 0-133 | 0-133, 134-266, 267-399, 400-533, 534-655 |
| NODE.timing.bits-1.Sa bit | 4 | 4, 5, 6, 7, 8 when FacilityType E1; N/A when FacilityType DS1; N/A when FacilityType 2MHz; N/A when FacilityType 64kHz+8kHz |
| NODE.timing.bits-1.State | unlocked | unlocked, locked, disabled |
| NODE.timing.bits-1.StateOut | unlocked | locked, disabled when FacilityTypeOut DS1; unlocked, locked, disabled when FacilityTypeOut E1; unlocked, locked, disabled when FacilityTypeOut 2MHz; unlocked, locked, disabled when FacilityTypeOut 64kHz+8kHz |
| NODE.timing.bits-2.AISThreshold | G812L | G811, STU, G812T, G812L, SETS, DUS |
| NODE.timing.bits-2.AdminSSMIn | STU | G811, STU, G812T, G812L, SETS, DUS |
| NODE.timing.bits-2.CableType | 120 ohm | 75 ohm, 120 ohm when nothing E1; 100 ohm when nothing DS1; 75 ohm, 120 ohm when nothing 2MHz; 120 ohm when nothing 64kHz+8kHz |

*Table C-5  Node Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| NODE.timing.bits-2.Coding | HDB3 | B8ZS, AMI when FacilityType DS1; HDB3, AMI when FacilityType E1; N/A when FacilityType 2MHz; AMI when FacilityType 64kHz+8kHz |
| NODE.timing.bits-2.CodingOut | HDB3 | B8ZS, AMI when FacilityTypeOut DS1; HDB3, AMI when FacilityTypeOut E1; N/A when FacilityTypeOut 2MHz; AMI when FacilityTypeOut 64kHz+8kHz |
| NODE.timing.bits-2.FacilityType | E1 | DS1, E1, 64kHz+8kHz, 2MHz |
| NODE.timing.bits-2.FacilityTypeOut | E1 | DS1, E1, 64kHz+8kHz, 2MHz |
| NODE.timing.bits-2.Framing | FAS+CAS+CRC | ESF, D4 when FacilityType DS1; FAS+CRC, FAS+CAS, FAS+CAS+CRC, FAS, Unframed when FacilityType E1; N/A when FacilityType 2MHz; N/A when FacilityType 64kHz+8kHz |
| NODE.timing.bits-2.FramingOut | FAS+CAS+CRC | ESF, D4 when FacilityTypeOut DS1; FAS+CRC, FAS+CAS, FAS+CAS+CRC, FAS, Unframed when FacilityTypeOut E1; N/A when FacilityTypeOut 2MHz; N/A when FacilityTypeOut 64kHz+8kHz |
| NODE.timing.bits-2.LBO | 0-133 | 0-133, 134-266, 267-399, 400-533, 534-655 |

*Table C-5        Node Default Settings (continued)*

| Default Name | Default Value | Default Domain |
|---|---|---|
| NODE.timing.bits-2.Sa bit | 4 | 4, 5, 6, 7, 8 when FacilityType E1; N/A when FacilityType DS1; N/A when FacilityType 2MHz; N/A when FacilityType 64kHz+8kHz |
| NODE.timing.bits-2.State | unlocked | unlocked, locked, disabled |
| NODE.timing.bits-2.StateOut | unlocked | locked, disabled when FacilityTypeOut DS1; unlocked, locked, disabled when FacilityTypeOut E1; unlocked, locked, disabled when FacilityTypeOut 2MHz; unlocked, locked, disabled when FacilityTypeOut 64kHz+8kHz |
| NODE.timing.general.Mode | External | External, Line, Mixed |
| NODE.timing.general.ReversionTime | 5.0 (minutes) | 0.0, 0.5, 1.0 .. 12.0 |
| NODE.timing.general.Revertive | FALSE | TRUE, FALSE |
| NODE.timing.general.SSMMessageSet | Generation 2 | Generation 1, Generation 2 |

# C.3.1  Time Zones

Table C-6 lists the time zones that apply for node time zone defaults. Time zones in the table are ordered by their relative relationships to Greenwich Mean Time (GMT), and the default values are displayed in the correct format for valid default input.

*Table C-6        Time Zones*

| Time Zone (GMT +/– Hours) | Default Value |
|---|---|
| GMT-11:00 | (GMT-11:00) Midway Islands, Samoa |
| GMT-10:00 | (GMT-10:00) Hawaiian Islands, Tahiti |
| GMT-09:00 | (GMT-09:00) Anchorage - Alaska |
| GMT-08:00 | (GMT-08:00) Pacific Time (US & Canada), Tijuana |
| GMT-07:00 | (GMT-07:00) Mountain Time (US & Canada) |
| GMT-07:00 | (GMT-07:00) Phoenix - Arizona |
| GMT-06:00 | (GMT-06:00) Central Time (US & Canada) |

*Table C-6        Time Zones (continued)*

| Time Zone (GMT +/– Hours) | Default Value |
|---|---|
| GMT-06:00 | (GMT-06:00) Mexico City |
| GMT-06:00 | (GMT-06:00) Costa Rica, Managua, San Salvador |
| GMT-06:00 | (GMT-06:00) Saskatchewan |
| GMT-05:00 | (GMT-05:00) Bogota, Lima, Quito |
| GMT-05:00 | (GMT-05:00) Eastern Time (US & Canada) |
| GMT-05:00 | (GMT-05:00) Havana |
| GMT-05:00 | (GMT-05:00) Indiana (US) |
| GMT-04:00 | (GMT-04:00) Asuncion |
| GMT-04:00 | (GMT-04:00) Caracas, La Paz, San Juan |
| GMT-04:00 | (GMT-04:00) Atlantic Time (Canada), Halifax, Saint John, Charlottetown |
| GMT-04:00 | (GMT-04:00) Santiago |
| GMT-04:00 | (GMT-04:00) Thule (Qaanaaq) |
| GMT-03:30 | (GMT-03:30) St. John's - Newfoundland |
| GMT-03:00 | (GMT-03:00) Brasilia, Rio de Janeiro, Sao Paulo |
| GMT-03:00 | (GMT-03:00) Buenos Aires, Georgetown |
| GMT-03:00 | (GMT-03:00) Godthab (Nuuk) - Greenland |
| GMT-02:00 | (GMT-02:00) Mid-Atlantic |
| GMT-01:00 | (GMT-01:00) Azores, Scoresbysund |
| GMT-01:00 | (GMT-01:00) Praia - Cape Verde |
| GMT 00:00 | (GMT 00:00) Casablanca, Reykjavik, Monrovia |
| GMT | (GMT) Greenwich Mean Time |
| GMT 00:00 | (GMT 00:00) Dublin, Edinburgh, London, Lisbon |
| GMT+01:00 | (GMT+01:00) Amsterdam, Berlin, Rome, Stockholm, Paris |
| GMT+01:00 | (GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague |
| GMT+01:00 | (GMT+01:00) Brussels, Copenhagen, Madrid, Vienna |
| GMT+01:00 | (GMT+01:00) Sarajevo, Skopje, Sofija, Vilnius, Warsaw, Zagreb |
| GMT+01:00 | (GMT+01:00) West Central Africa, Algiers, Lagos, Luanda |
| GMT+01:00 | (GMT+01:00) Windhoek (Namibia) |
| GMT+02:00 | (GMT+02:00) Al Jizah, Alexandria, Cairo |
| GMT+02:00 | (GMT+02:00) Amman |
| GMT+02:00 | (GMT+02:00) Athens, Bucharest, Istanbul |
| GMT+02:00 | (GMT+02:00) Beirut |
| GMT+02:00 | (GMT+02:00) Cape Town, Harare, Johannesburg, Pretoria |
| GMT+02:00 | (GMT+02:00) Jerusalem |
| GMT+02:00 | (GMT+02:00) Kaliningrad, Minsk |
| GMT+03:00 | (GMT+03:00) Aden, Antananarivo, Khartoum, Nairobi |

*Table C-6 Time Zones (continued)*

| Time Zone (GMT +/– Hours) | Default Value |
|---|---|
| GMT+03:00 | (GMT+03:00) Baghdad |
| GMT+03:00 | (GMT+03:00) Kuwait, Riyadh |
| GMT+03:00 | (GMT+03:00) Moscow, St. Petersburg, Novgorod |
| GMT+03:30 | (GMT+03:30) Tehran |
| GMT+04:00 | (GMT+04:00) Abu Dhabi, Mauritius, Muscat |
| GMT+04:00 | (GMT+04:00) Aqtau, T'bilisi |
| GMT+04:00 | (GMT+04:00) Baku |
| GMT+04:00 | (GMT+04:00) Yerevan, Samara |
| GMT+04:30 | (GMT+04:30) Kabul |
| GMT+05:00 | (GMT+05:00) Chelyabinsk, Prem, Yekaterinburg, Ufa |
| GMT+05:00 | (GMT+05:00) Islamabad, Karachi, Tashkent |
| GMT+05:30 | (GMT+05:30) Calcutta, Mumbai, New Delhi, Chennai |
| GMT+05:45 | (GMT+05:45) Kathmandu |
| GMT+06:00 | (GMT+06:00) Almaty |
| GMT+06:00 | (GMT+06:00) Colombo, Dhaka, Astana |
| GMT+06:00 | (GMT+06:00) Novosibirsk, Omsk |
| GMT+06:30 | (GMT+06:30) Cocos, Rangoon |
| GMT+07:00 | (GMT+07:00) Bangkok, Hanoi, Jakarta |
| GMT+07:00 | (GMT+07:00) Krasnoyarsk, Norilsk, Novokuznetsk |
| GMT+08:00 | (GMT+08:00) Irkutsk, Ulaan Bataar |
| GMT+08:00 | (GMT+08:00) Beijing, Shanghai, Hong Kong, Urumqi |
| GMT+08:00 | (GMT+08:00) Perth |
| GMT+08:00 | (GMT+08:00) Singapore, Manila, Taipei, Kuala Lumpur |
| GMT+09:00 | (GMT+09:00) Chita, Yakutsk |
| GMT+09:00 | (GMT+09:00) Osaka, Sapporo, Tokyo |
| GMT+09:00 | (GMT+09:00) Palau, Pyongyang, Seoul |
| GMT+09:30 | (GMT+09:30) Adelaide, Broken Hill |
| GMT+09:30 | (GMT+09:30) Darwin |
| GMT+10:00 | (GMT+10:00) Brisbane, Port Moresby, Guam |
| GMT+10:00 | (GMT+10:00) Canberra, Melbourne, Sydney |
| GMT+10:00 | (GMT+10:00) Hobart |
| GMT+10:00 | (GMT+10:00) Khabarovsk, Vladivostok |
| GMT+10:30 | (GMT+10:30) Lord Howe Island |
| GMT+11:00 | (GMT+11:00) Honiara, Magadan, Soloman Islands |
| GMT+11:00 | (GMT+11:00) Noumea - New Caledonia |
| GMT+11:30 | (GMT+11:30) Kingston - Norfolk Island |

*Table C-6      Time Zones (continued)*

| Time Zone (GMT +/– Hours) | Default Value |
|---|---|
| GMT+12:00 | (GMT+12:00) Andyra, Kamchatka |
| GMT+12:00 | (GMT+12:00) Auckland, Wellington |
| GMT+12:00 | (GMT+12:00) Marshall Islands, Eniwetok |
| GMT+12:00 | (GMT+12:00) Suva - Fiji |
| GMT+12:45 | (GMT+12:45) Chatham Island |
| GMT+13:00 | (GMT+13:00) Nuku'alofa - Tonga |
| GMT+13:00 | (GMT+13:00) Rawaki, Phoenix Islands |
| GMT+14:00 | (GMT+14:00) Line Islands, Kiritimati - Kiribati |

# C.4  CTC Default Settings

Table C-7 lists the CTC-level default settings for the Cisco ONS 15600 SDH. Cisco provides the following user-configurable defaults for CTC:

- Automatic Routing—Set circuit creation with the Route Automatically check box selected by default.

- Network Circuit Automatic Routing Overridable—Set by default whether or not a user creating circuits can change (override) the Automatic Circuit Routing setting (also provisionable as a default). When this default is set to TRUE it enables users to change whether or not Route Automatically is selected in the check box. When this default is set to FALSE it ensures that users cannot change the Route Automatically setting while creating circuits in CTC.

**Note**     When the Route Automatically check box is not selectable (and is not checked) during circuit creation, the Using Required Nodes/Spans and Review Route Before Creation check boxes are also unavailable.

- Create TL1-like—Set whether to create only TL1-like circuits; that is, instruct the node to create only cross-connects, allowing the resulting circuits to be in an upgradable state.

- Local domain creation and viewing—Set whether domains that users create and view persist globally (all CTC sessions), or only locally (within the current CTC session).

- Network Map—Set the default network map (which country's map is displayed in CTC network view).

*Table C-7      CTC Default Settings*

| Default Name | Default Value | Default Domain |
|---|---|---|
| CTC.circuits.CreateLikeTL1 | FALSE | TRUE, FALSE |
| CTC.circuits.RouteAutomatically | TRUE | TRUE, FALSE |
| CTC.circuits.RouteAutomaticallyDefaultOverridable | TRUE | TRUE, FALSE |
| CTC.network.LocalDomainCreationAndViewing | FALSE | TRUE, FALSE |
| CTC.network.Map | United States | -none-, Germany, Japan, Netherlands, South Korea, United Kingdom, United States |

**Cisco ONS 15600 SDH Reference Manual, R8.0**