Cisco ONS 15327 Reference Manual

Product and Documentation Release 6.0
October 2008

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7816925=
Text Part Number: 78-16925-01

Cisco ONS 15327 Reference Manual, Release 6.0

FIGURES

About this Manual

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

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.

Revision History

Date	Notes
03/23/2007	Revision History Table added for the first time
08/23/2007	Updated About this Manual chapter
09/08/2008	Added a note in Card Default Settings and Node Default Settings section of Appendix C, Network Element Defaults.

This section provides the following information:

Document Objectives

The *Cisco ONS 15327 Reference Manual* provides hardware and software reference information for Cisco ONS 15327 nodes and networks. Use this manual in conjunction with the appropriate publications listed in the Related Documentation section.

Audience

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

Document Organization

Table 1 Cisco ONS 15327 Reference Manual Chapters

Title	Summary
Chapter 1, "Shelf Assembly Hardware"	Includes descriptions of the rack, backplane, backplane pins, ferrites, power and ground, fan-tray assembly, air filter, card slots, cables, cable connectors, and cable routing.
Chapter 2, "Card Reference"	Includes descriptions of the XTC-14 and XTC-28-3 cards; MIC A and MIC B cards; OC-3, OC-12, and OC-48 optical cards; and the G1000-2 and E10/100-4 cards.
Chapter 3, "Card Protection"	Includes electrical and optical card protection methods.
Chapter 4, "Cisco Transport Controller Operation"	Includes information about Cisco Transport Controller (CTC) installation, the CTC window, computer requirements, software versions, and database reset and revert.
Chapter 5, "Security"	Includes user set up and information, security policies and parameters, and audit trail information.
Chapter 6, "Timing"	Includes node and network timing information.
Chapter 7, "Circuits and Tunnels"	Includes synchronous transport signal (STS) and Virtual Tributary (VT), bidirectional and unidirectional, revertive and nonrevertive, electrical and optical, multiple and path trace circuit information, as well as data communications channel (DCC) tunnels.
Chapter 8, "SONET Topologies and Upgrades"	Includes the SONET configurations used by the ONS 15327; including bidirectional line switched rings (BLSRs), path protection configurations, linear add/drop multiplexers (ADMs), subtending rings, and optical bus configurations, as well as information about upgrading optical speeds within any configuration.
Chapter 9, "Management Network Connectivity"	Includes IP addressing scenarios and information about open GNE, provisionable patchcords, firewalls, and the routing table.

Table 1 Cisco ONS 15327 Reference Manual Chapters (continued)

Title	Summary
Chapter 10, "Alarm Monitoring and Management"	Includes CTC alarm management information.
Appendix A, "Hardware Specifications"	Includes shelf assembly and card specifications.
Appendix B, "Administrative and Service States"	Describes the state model for Cisco ONS 15327 cards, ports, and cross-connects.
Appendix C, "Network Element Defaults"	Lists card-level and network-level factory default (NE default) settings.

Related Documentation

Use the *Cisco ONS 15327 Reference Manual* in conjunction with the following referenced publications:

- *Cisco ONS 15327 Procedure Guide*
  Provides installation, turn-up, test, and maintenance procedures.
- *Cisco ONS 15327 Troubleshooting Guide*
  Provides alarm descriptions and troubleshooting procedures, general troubleshooting procedures, error messages, performance monitoring parameters, and SNMP information.
- *Cisco ONS SONET TL1 Command Guide*
  Provides a full TL1 command and autonomous message set including parameters, access identifiers (AIDs), conditions, and modifiers for the Cisco ONS 15454, ONS 15327, ONS 1560, and ONS 15310-CL systems.
- *Cisco ONS SONET TL1 Reference Guide*
  Provides general information, procedures, and errors for TL1 in the Cisco ONS 15454, ONS 15327, ONS 15600, and ONS 15310-CL systems.
- *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*
  Provides software features and operations for all Ethernet cards and configuration information for Cisco IOS on ML-Series cards.
- *Release Notes for the Cisco ONS 15327 Release 6.0*
  Provides caveats, closed issues, and new features and functionality information.

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.

Convention	Application
{ 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

Figyelem

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

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 Guidelines 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, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

Shelf Assembly Hardware

This chapter provides a description of Cisco ONS 15327 shelf and backplane hardware. Card and cable descriptions as well as instructions for installing equipment are provided in the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

Note The Cisco ONS 15327 assembly is intended for use with telecommunications equipment only.

Note The ONS 15327 is designed to comply with Telcordia GR-1089-CORE Type 2 and Type 4. Install and operate the ONS 15327 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

You can mount the ONS 15327 in a 19- or 23-inch (482.6- or 584.2-mm) rack. Including the fan-tray assembly, the shelf assembly weighs approximately 15 pounds (6.8 kg) without cards installed and 27 pounds (12.2 kg) fully loaded. An ONS 15327 is installed in a rack using reversible mounting brackets on each side of the shelf. The ONS 15327 is powered using –48 VDC power. Positive and negative power terminals are accessible on the front panel.

You can access the ONS 15327 cards, cables, connectors, power feeds, and fan-tray assembly through the front of the shelf assembly only. The CRIT, MAJ, MIN, and REM alarm LEDs visible on the Cross-Connect, Timing, and Control (XTC) card faceplate indicate whether a Critical, Major, Minor, or Remote alarm is present anywhere on the ONS 15327 assembly. These LEDs help you to determine quickly if any alarms are present on the assembly.

When installed in an equipment rack, the ONS 15327 assembly is typically connected to a fuse and alarm panel that provides centralized alarm connection points and distributed power for the ONS 15327. Fuse and alarm panels are third-party equipment and are not described in this documentation. If you are unsure about the requirements or specifications for a fuse and alarm panel, consult the documentation for that product.

Note In this chapter, the terms "ONS 15327" and "shelf assembly" are used interchangeably. In the installation context, these terms have the same meaning. Otherwise, shelf assembly refers to the physical steel enclosure that holds cards and connects power, and ONS 15327 refers to the entire system, both hardware and software.

Install the ONS 15327 in compliance with your local and national electrical codes:

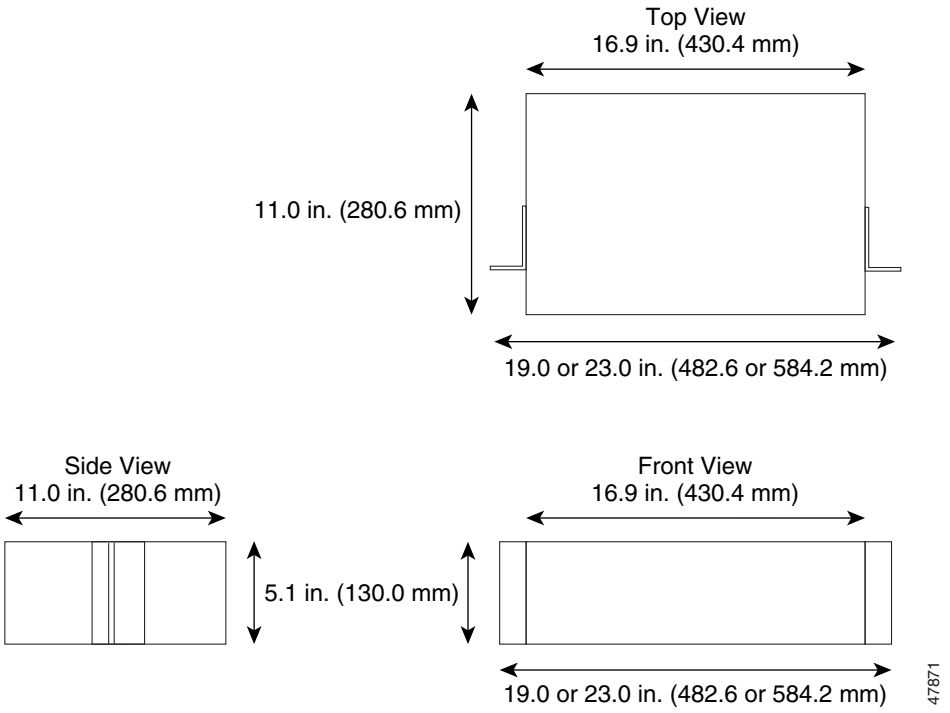
- United States: National Fire Protection Association (NFPA) 70; United States National Electrical Code
- Canada: Canadian Electrical Code, Part I, CSA C22.1
- Other countries: If local and national electrical codes, are not available, refer to IEC 364, Part 1 through Part 7.

1.2 Rack Installation

The ONS 15327 is mounted in a 19- or 23-inch (482.6- or 584.2-mm) equipment rack. The shelf assembly projects two inches from the front of the rack. It mounts in both EIA-standard and Telcordia-standard racks. The shelf assembly is a total of 17 inches (431.8 mm) wide with no mounting ears attached. With the mounting ears attached, the shelf assembly is 19 inches (482.6 mm) wide.

The ONS 15327 measures 5.1 inches high, 19 or 23 inches wide (depending on which way the mounting ears are attached), and 11 inches deep (129.5 x 482.6 or 584.2 x 279.4 mm). Figure 1-1 shows the dimensions of the ONS 15327 shelf assembly.

Figure 1-1 ONS 15327 Shelf Assembly Dimensions



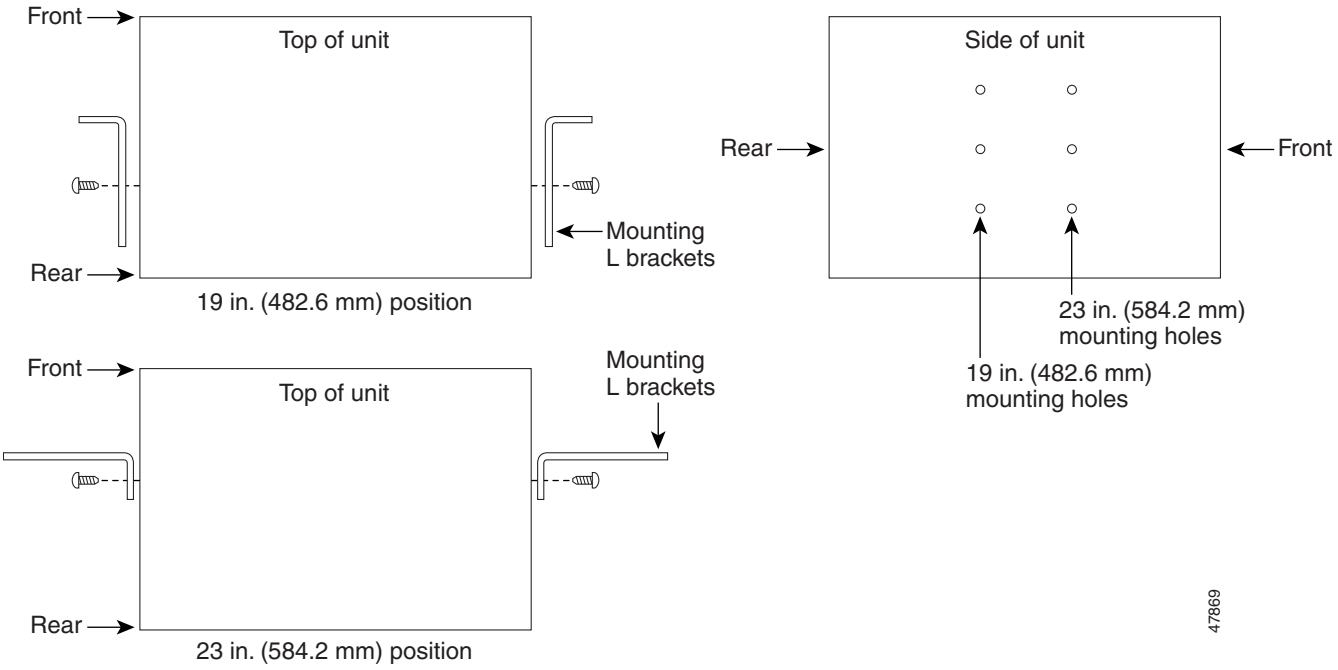
1.2.1 Reversible Mounting Bracket

Caution Use only the fastening hardware provided with the ONS 15327 to prevent loosening, deterioration, and electromechanical corrosion of the hardware and joined material.

Caution When mounting the ONS 15327 in a frame with a nonconductive coating (such as paint, lacquer, or enamel), use either the thread-forming screws provided with the ONS 15327 shipping kit or remove the coating from the threads to ensure electrical continuity.

The shelf assembly comes with mounting brackets that can be reversed for use with a 19- or 23-inch (482.6- or 584.2-mm) rack (Figure 1-2).

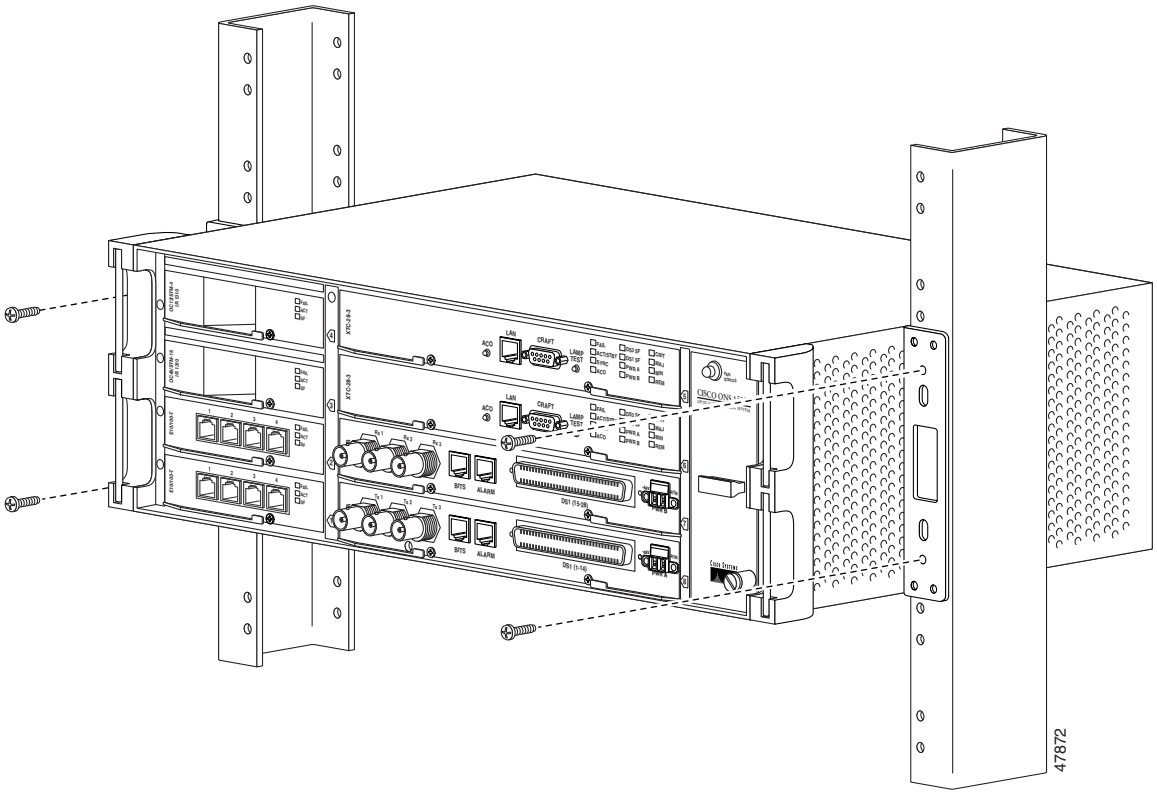
Figure 1-2 Reversing the Mounting Brackets (23 in. [482.6 mm] Position to 19 in. [584.2 mm] Position)



1.2.2 Mounting a Single Node

Mounting the ONS 15327 in a rack requires a minimum of 5.2 inches (132 mm) of vertical rack space (plus 1 inch [25.4 mm] for air flow). To ensure that the mounting is secure, use two to four #12-24 mounting screws for each side of the shelf assembly. Figure 1-3 shows the rack mounting position for the ONS 15327.

Figure 1-3 Mounting an ONS 15327 in a Rack



1.2.3 Mounting Multiple Nodes

Most standard seven-foot (2.1 m) racks can hold twelve ONS 15327s and a fuse and alarm panel.

1.3 Power and Ground Description

This section describes how to connect the ONS 15327 shelf assembly to the power supply. For detailed procedures, refer to the *Cisco ONS 15327 Procedure Guide*. Terminate the chassis ground to either the office ground or rack ground before you install the power. Use the grounding lug to attach the ground cable to the shelf assembly according to local site practice.

Ground one cable to ground the shelf assembly. Terminate the other end of the rack ground cable to ground according to local site practice.

If the system loses power or both XTC cards are reset, you must reset the ONS 15327 clock unless the node has been previously provisioned to use Simple Network Time Protocol (SNTP) to update the clock over the LAN.

Caution Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Use the following wiring conventions:

- Red wire for battery (–48 VDC) connections
- Black wire for battery return (0 VDC) connections

Note Use an external disconnect for service purposes and install it according to local site practice.

The ONS 15327 has redundant –48 VDC power terminals on the mechanical interface cards (MICs). The terminals are labeled PWR A and PWR B and are located on the far right-hand side of the MICs if you are facing the shelf assembly. Both MIC A and MIC B must be installed to create redundant power connections.

To install redundant power feeds, use four power cables and one ground cable. For a single power feed, only two power cables and one ground cable are required. Use #12 AWG cable and, to ensure circuit overcurrent protection, use a conductor with low impedance.

Caution The conductor must have the capability to safely conduct any fault current that might be imposed. Do not use aluminum conductors.

The MIC power connector is shipped with the fastening screws inserted but not tightened. The screws may have tightened due to vibration during shipping. Make sure the screws are loose before attempting to remove the connector.

Figure 1-4 shows the MIC power connector being removed.

Figure 1-4 Removing the MIC Power Connector

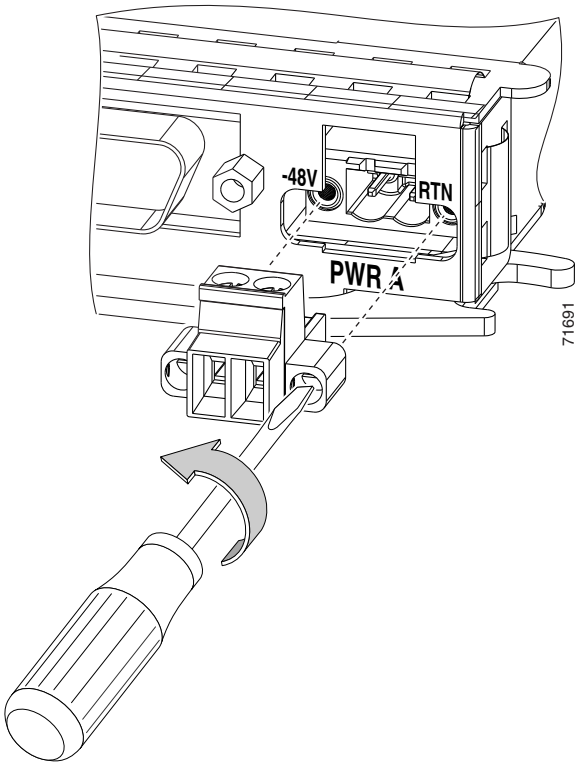


Figure 1-5 shows a power cable being inserted into the MIC power connector.

Figure 1-5 Inserting a Power Cable into the MIC Power Connector

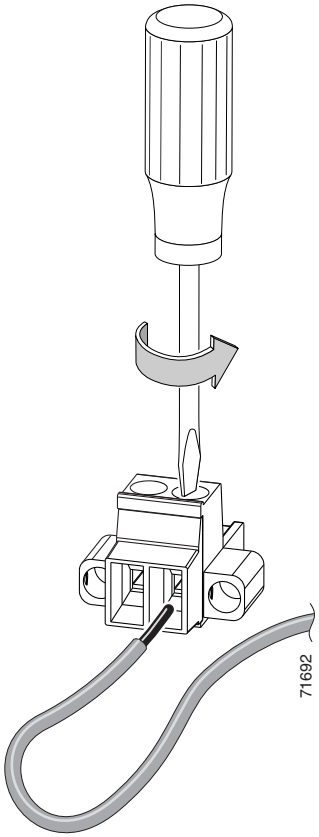


Figure 1-6 shows the MIC power connector being installed.

Figure 1-6 Installing the MIC Power Connector

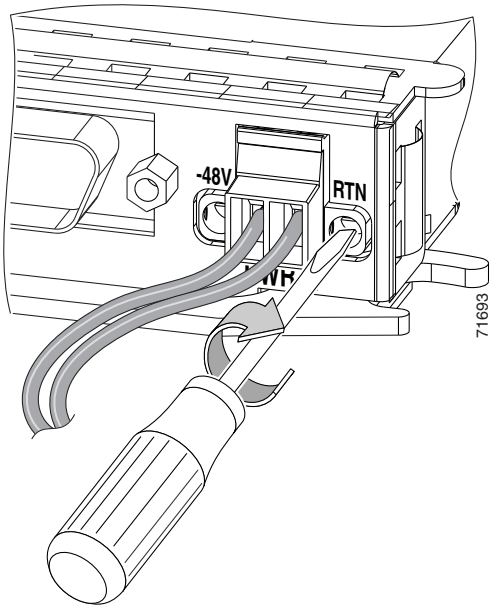
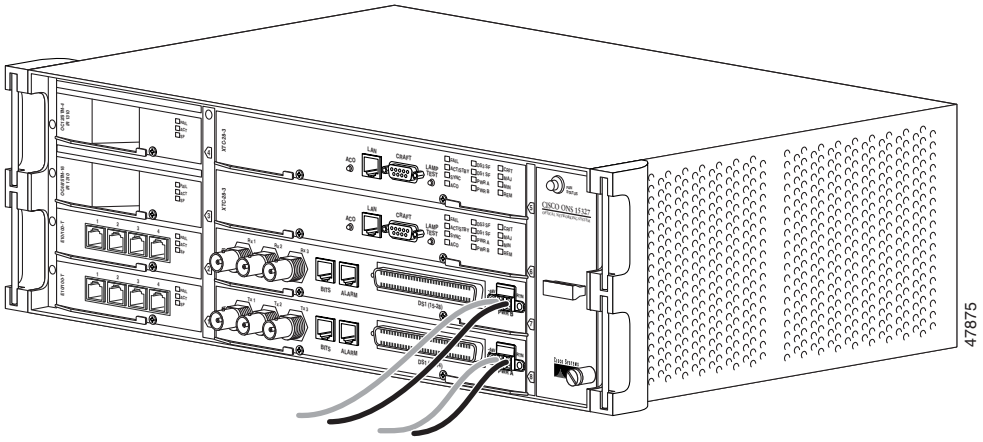


Figure 1-7 shows redundant power feeds connected to an ONS 15327.

Figure 1-7 Redundant Power Feeds Connected to an ONS 15327



1.4 Ferrites

Place third-party ferrites on power cables to dampen electromagnetic interference (EMI) from the ONS 15327. Ferrites must be added to meet the requirements of Telcordia GR 1089. Refer to the ferrite manufacturer documentation for proper use and installation of the ferrites.

1.5 Cable Description and Installation

This section describes fiber-optic, DS-3 (coaxial), DS-1 (Champ), and twisted-pair cables.

1.5.1 Cabling Types

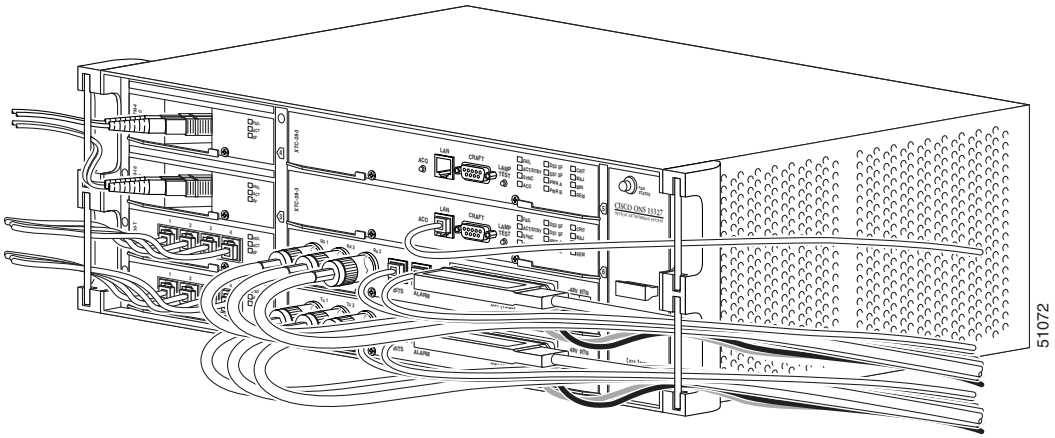
ONS 15327 cables use cable guides at each side of the front of the shelf assembly to economize shelf space and manage cables. The following types of cables are used with the ONS 15327:

- Optical cables—Connect to the SC connectors on the OC-12 and OC-48 card faceplates and the LC connectors on the OC-3 card faceplates. See the "1.5.4 Fiber Cable Installation" section on page 1-12 for more information. Make sure the fiber cables do not bend excessively; maintaining a proper bend radius prevents damage to the optical cable.
- Coaxial cables—Connect to the MICs on the ONS 15327 using BNC cable connectors. Coaxial cables carry DS-3 traffic to and from the ONS 15327. The ONS 15327 supports up to three transmit and three receive coaxial connectors on each shelf assembly.
- AMP Champ cables—Connect to MICs on the ONS 15327 using AMP Champ cable connectors. Each Champ connector on the MIC supports one AMP Champ cable connection for a total of two connectors per node. Each Champ connector supports a maximum of 14 DS-1s. See the "1.5.6 DS-1 Cable Installation" section on page 1-13 for more information about the AMP Champ cables and connectors.
- Twisted-pair cables for timing—Connect to the building integrated timing supply (BITS) ports on the MICs. The twisted-pair cables for timing use RJ-45 connectors. Connecting to the BITS ports requires a BITS clock cable and twisted-pair #22 or #24 shielded AWG wire.
- CAT-5 Twisted-Pair cables—Connect to the ports on the E-Series Ethernet card, the alarm ports on the MICs, and the LAN port on the XTC cards. The twisted-pair cables use RJ-45 connectors. The Ethernet ports and the LAN ports use a standard straight-through cable.

1.5.2 Cable Guides

The ONS 15327 has cable guides located on each side of the front of the shelf assembly (Figure 1-8). These cable guides ensure that the proper bend radius is maintained in the fibers and that all other cables are properly routed. To remove cable guides, remove the screws that anchor them to the side of the shelf assembly.

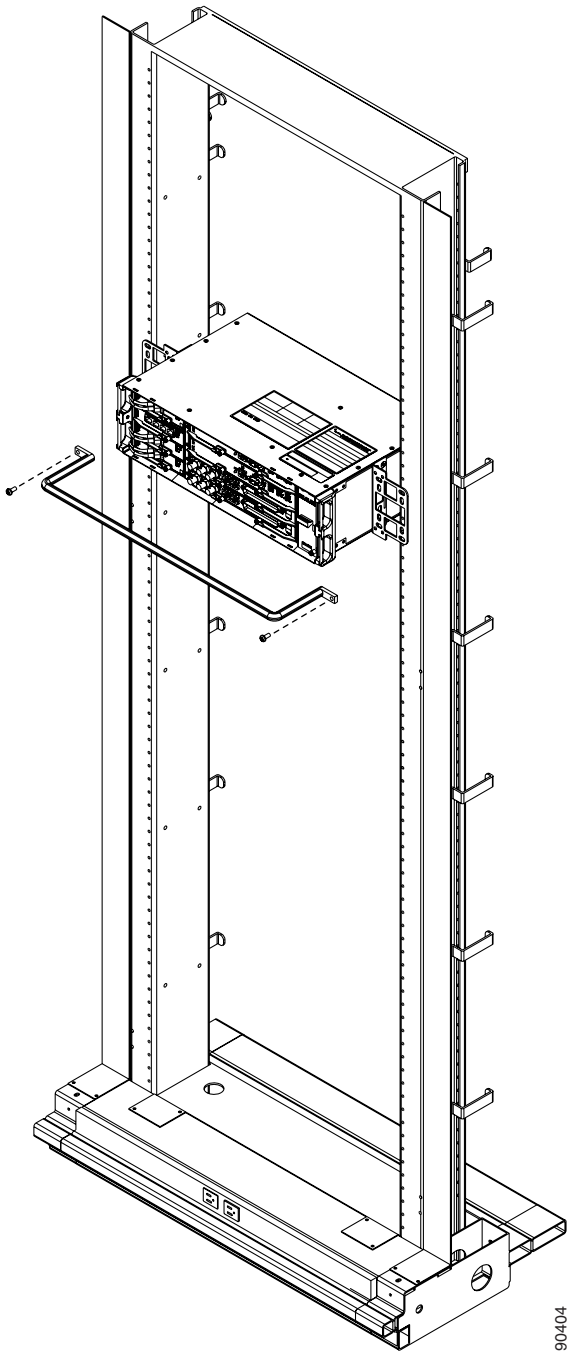
Figure 1-8 Managing Front Panel Cables with Locking Cable Guides



To relieve strain, you can also use the optional tie-down bar to secure the cables using tie-wraps or other site-specific methods.

Figure 1-9 shows the tie-down bar, the ONS 15327, and the rack.

Figure 1-9 Tie-Down Bar



1.5.3 Cabling Sequence and Location

To maintain access to all of the connectors during cable installation, cables must be attached to the MICs in the following order, starting with MIC A (the bottom MIC) and repeating for MIC B:

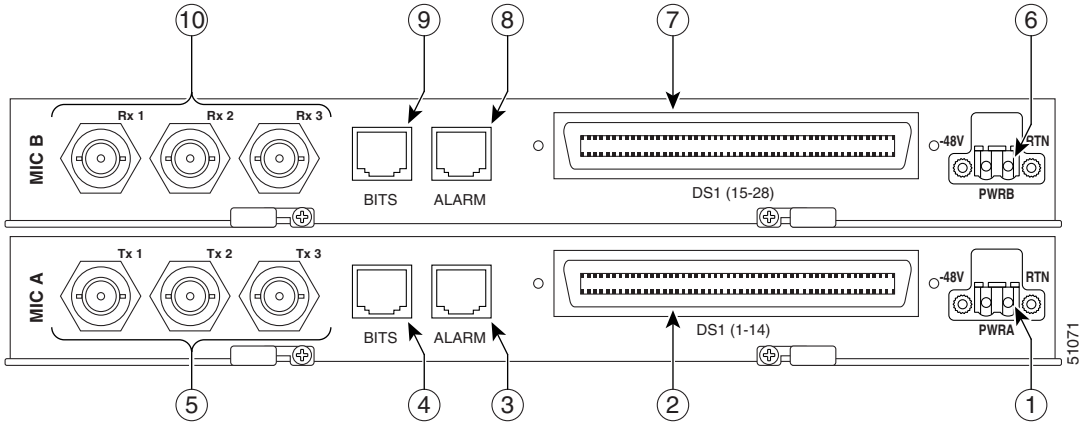
1. Attach power cables

2. Attach DS-1 (Champ) cables
3. Attach Alarm (RJ-45) cables
4. Attach BITS (RJ-45) cables
5. Attach DS-3 (BNC) cables

After attaching all of the cables to the MICs, route the cables out through the bottom right cable guide and snap it closed. Tie wrap the cables according to local site practice. Leave enough slack to remove the fan-tray assembly and fan filter.

You do not need to connect cables for the XTC cards and traffic cards in any particular order. Route XTC cables through the top-right cable guide. Route electrical and fiber-optic cables out through the corresponding cable guides on the left side of the shelf assembly. Figure 1-10 shows the order in which you should install cables on the ONS 15327.

Figure 1-10 Cable Installation Sequence

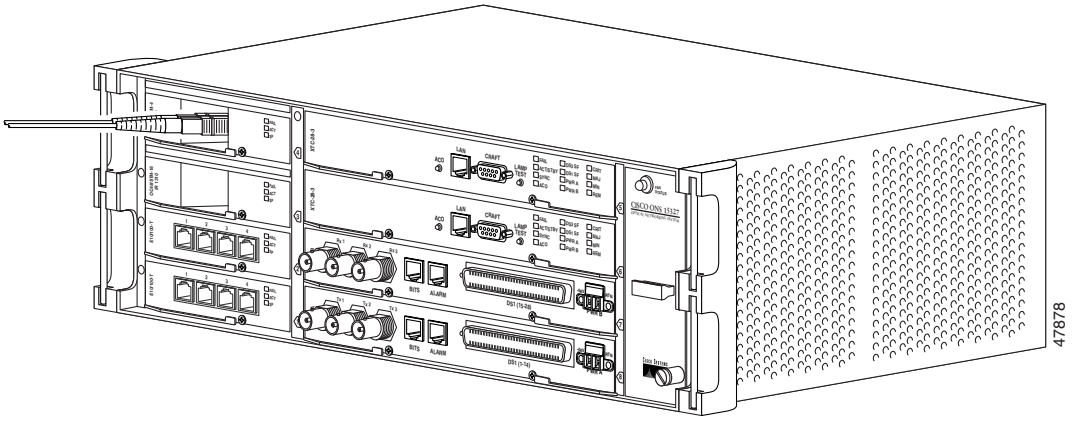


1.5.4 Fiber Cable Installation

ONS 15327 OC-12 and OC-48 cards have SC connectors and the OC-3 and G1000-2 cards have LC connectors. To install fiber-optic cables in the ONS 15327, a fiber cable with the corresponding connector type must be connected to the transmit and receive ports on the ONS 15327 cards (Figure 1-11). On ONS 15327 OC-12 and OC-48 card ports, the left side connector is the transmit port and the right-side connector is the receive port. Cisco recommends that you label the transmit and receive ports and the working and protection fibers at each end of the fiber span to avoid confusion with cables that are similar in appearance.

Note Clean all fiber connectors thoroughly. Dust particles can degrade performance. Put caps on any fiber connectors that you do not use.

Figure 1-11 Installing a Fiber-Optic Cable



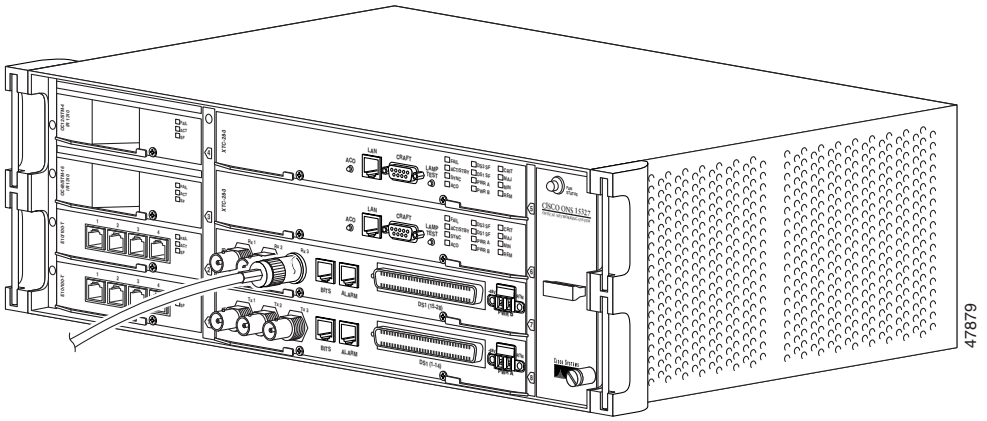
1.5.5 Coaxial Cable Installation

For DS-3 traffic, the ONS 15327 uses coaxial cables and connectors. Cisco recommends connecting an RG-59/U cable to a patch panel; RG-59/U cable is designed for long runs of up to 450 feet (137.16 meters). Use a compatible straight male BNC connector to connect the cable to the DS-3 ports on the MICs. The transmit (TX) ports on MIC A and the receive (RX) ports on MIC B use the same type of connector.

The electromagnetic compatibility (EMC) performance of the node depends on good-quality DS-3 coaxial cables, such as Shuner Type G 03233 D, or the equivalent.

Figure 1-12 shows a coaxial cable connected to the ONS 15327 MIC.

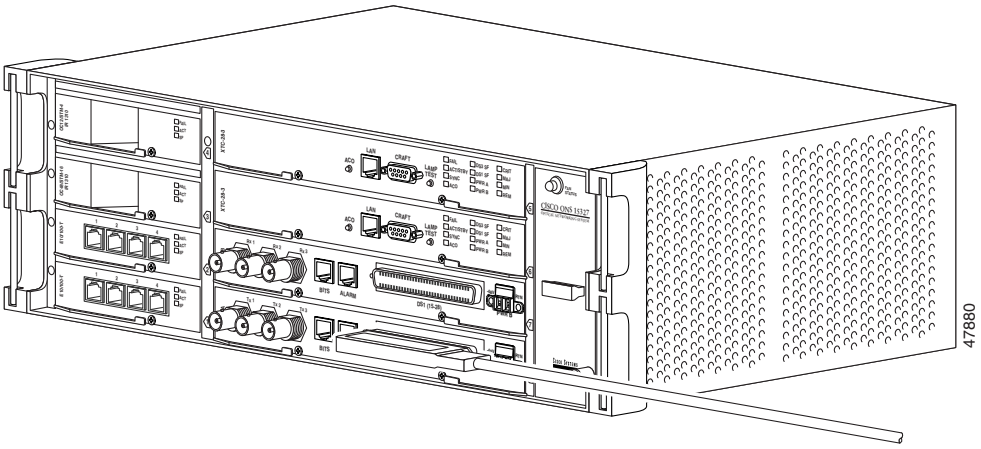
Figure 1-12 Installing a Coaxial Cable with BNC Connectors



1.5.6 DS-1 Cable Installation

The MIC uses AMP Champ connector cabling for DS-1 connections. Installing AMP Champ connector DS-1 cables requires 64-pin bundled cable connectors with a 64-pin male AMP Champ connector. Figure 1-13 shows DS-1 cable installation.

Figure 1-13 Installing a DS-1 Cable



1.5.6.1 Straight DS-1 Cable Connectors

Cisco-supplied AMP Champ DS-1 cables include a straight (180-degree) connector for use with the 19-inch (482.6-mm) Cisco tie-down bar (P/N 15327-TIE-BAR-19=) or 23-inch (584.2-mm) Cisco tie-down bar (P/N 15327-TIE-BAR-23=). Cisco offers four DS-1 cables with a straight AMP Champ connector. Table 1-1 lists the cable product numbers and lengths.

Table 1-1 Cisco-Supplied DS-1 Cables With Straight AMP Champ Connector

Cisco Product Number	Length of Cable (ft)
15327-AMP-WW-30=	30
15327-AMP-WW-50=	50
15327-AMP-WW-100=	100
15327-AMP-WW-250=	250

In addition to the Cisco-supplied DS-1 cables, the MIC-A-1-T and MIC-B-1-T can use the CHAMP #552285-1 and 180 degree shell housing CHAMP #552082-1 for DS-1 cabling with a straight AMP Champ connector.

1.5.6.2 90-Degree DS-1 Cable Connectors

A 90-degree angled connector is recommended for lower front profile applications. Cisco does not supply 90-degree connectors. Table 1-2 lists compatible third-party DS-1 cables with 90-degree connectors.

Table 1-2 Third-Party DS-1 Cables With 90-degree DS-1 Connectors

MIC-28-3 Version	End of Sale	Third-party DS1 Connector
15327-MIC-28-3-A 15327-MIC-28-3-A= 15327-MIC-28-3-B 15327-MIC-28-3-B=	June 2002	"Bail loop" type DS1 connector requires CHAMP #552276-1 and a 90-degree shell housing #1-552496-1, or functional equivalents.
15327-MIC-A-T 15327-MIC-A-T= 15327-MIC-B-T 15327-MIC-B-T=	October 2003	"Screw down/lock" type connector requires CHAMP #552285-1 and 90-degree shell housing #1-552496-1, or functional equivalents.

15327-MIC-A-1-T
15327-MIC-A-1-T=
15327-MIC-B-1-T
15327-MIC-B-1-T=
	Current production	"Screw down/lock" type connector requires one of the following:
		• Amphenol #GCA70
		  • GCA70 03006 RSE (30-ft [9.1-m] cable)
		  • GCA70 03007 RSE (50-ft [15.2-m] cable)
		  • GCA70 03008 RSE (100-ft [30.5-m] cable)
		  • GCA70 03009 RSE (250-ft [76.2-m] cable)
		• Volex #VLX979
		  • VLX979-30 (30-ft [9.1-m] cable)
		  • VLX979-50 (0-ft [15.2-m] cable)
		  • VLX979-100 (100-ft [30.5-m] cable)
		  • VLX979-250 (250-ft [76.2-m] cable)
		• Functional equivalent

Contact information for 90-degree cables:

- Alpine Electronics (distributor for Amphenol)

  Phone number: 408 278 7171
- Volex Inc.

  Phone number: 510 360 5250

Note The 90-degree connectors/cables that were compatible with previous versions of the MICs can interfere with the power connector on the newest version of the MICs. Customers who are replacing an older version MIC with a spare new version MIC and use the same/existing cables as the old MIC can remove the 90-degree shell housing and replace it with 180 degree shell housing 552082-1 to avoid interference with the power connector.

1.5.7 Alarm Cable Installation

The alarm cables attach to the MICs using twisted-pair cables terminated with an RJ-45 connector that plugs into the ALARM port. The other end of the cable plugs into the alarm-collection equipment. Terminate this end of the cable according to local site practice.

The pins on the ALARM port correspond to the six external alarm inputs and the two external alarm outputs (controls) that you can define using Cisco Transport Controller (CTC). Alarms 2, 4, and 6 correspond to MIC A and alarms 1, 3, and 5 correspond to MIC B. Alarm output 1 corresponds to MIC B and alarm output 2 corresponds to MIC A. Table 1-3 lists the input alarm pinouts and the corresponding alarm function numbers assigned to each MIC port.

Table 1-3 Alarm Input (External Alarm) Pin Assignments

Alarm Input Number (MIC A)	Alarm Input Number (MIC B)	RJ-45 Pin Number	Function
2	1	5	Alarm 2+
		6	Alarm 2–
4	3	3	Alarm 1+
		4	Alarm 1–
6	5	1	Alarm 0+
		2	Alarm 0–

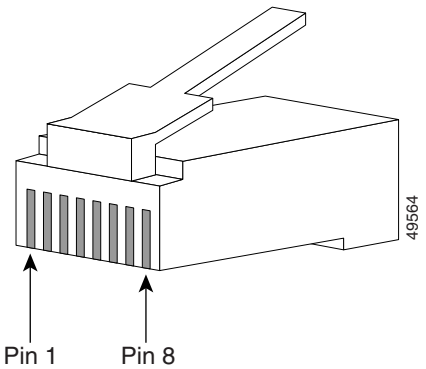
Table 1-4 lists the output alarm pinouts.

Table 1-4 Alarm Output (External Control) Pin Assignments

Alarm Output Number (MIC A)	Alarm Output Number (MIC B)	RJ-45 Pin Number	Function
2	1	7	Contact+
		8	Contact–

Figure 1-14 shows RJ-45 pin numbering.

Figure 1-14 Pins 1 and 8 on the RJ-45 Connector



1.5.8 BITS Cable Installation

The building integrated timing supply (BITS) cables attach to the MICs using BITS clock cable and twisted-pair #22 or #24 shielded AWG wire terminated with an RJ-45 connector that plugs into the BITS port. The other end of the cable plugs into the BITS clock. Terminate this end of the cable according to local site practice.

Each MIC has one BITS input and one BITS output. The BITS inputs and outputs have corresponding pins on the RJ-45 BITS ports. The BITS 1 inputs and outputs are on MIC A and the BITS 2 inputs and outputs are on MIC B. When connecting BITS cable to the ONS 15327, refer to Table 1-5 for the BITS cable pin assignments.

Table 1-5 BITS Cable Pin Assignments

MIC A	MIC B	RJ-45 Pin Number	Function
BITS 1 In	BITS 2 In	3	BITS Input+
		4	BITS Input–
BITS 1 Out	BITS 2 Out	7	BITS Output+
		8	BITS Output–

Figure 1-15 shows the BITS In pins on the RJ-45 connector.

Figure 1-15 BITS In Pins on the RJ-45 Connector

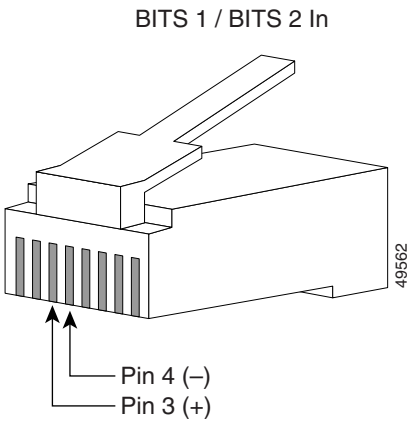
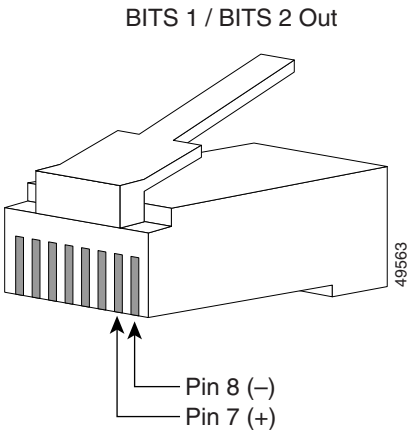


Figure 1-16 shows the BITS Out pins on the RJ-45 connector.

Figure 1-16 BITS Out Pins on the RJ-45 Connector



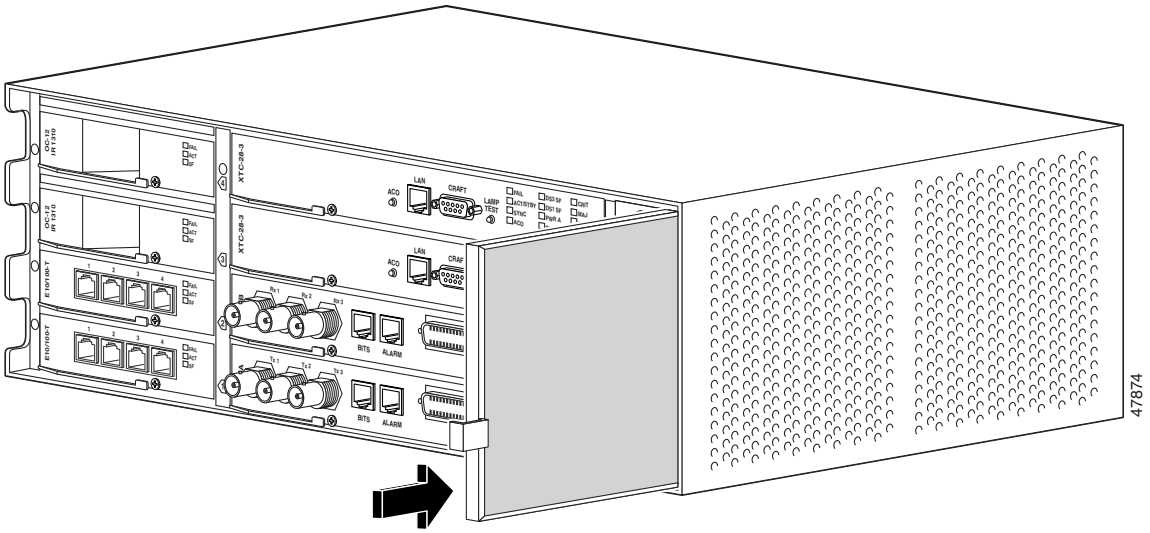
1.6 Fan-Tray Assembly

Facing the front of the ONS 15327, the fan-tray assembly is located on the far right side. The fan-tray assembly is a removable drawer that holds fans and fan-control circuitry for the ONS 15327. After you install the fan-tray assembly, you should not need to remove it unless a fan failure occurs.

The fan-tray assembly has an air filter on the right side of the fan-tray assembly that you can install and remove by hand. Remove and visually inspect this filter every 30 days. For inspection procedures, refer to the *Cisco ONS 15327 Procedure Guide*. Spare filters should be kept in stock. If you are replacing the air filter, you must first move aside the cables that cross in front of it. You must install the air filter with its metal bracing against the fan-tray assembly.

Figure 1-17 shows the location of the fan-tray air filter.

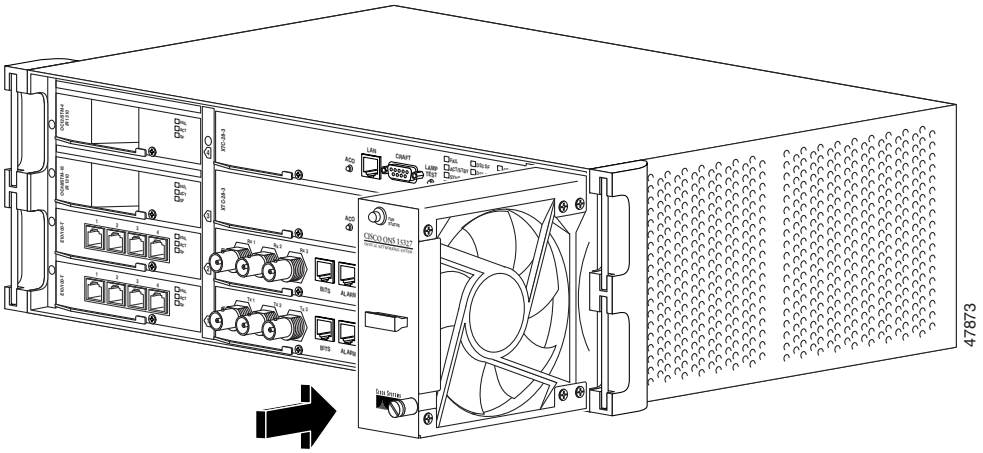
Figure 1-17 Fan-Tray Air Filter



Caution Do not force the fan-tray assembly into place while installing it. Forcing the fan-tray assembly into place can damage the connectors on the fan tray or the connectors on the back panel of the shelf assembly.

Figure 1-18 shows the location of the fan-tray assembly.

Figure 1-18 Fan-Tray Assembly



1.7 Alarm Cutoff

Visual and audible alarms are typically wired to trigger an alarm light at a central alarm collection point when the corresponding contacts are closed. The alarm cutoff (ACO) function turns off the alarm signal being transmitted to the alarm collection point.

To activate the ACO function, press the ACO button on the XTC card faceplate. The ACO button clears all audible alarm indications. After clearing the audible alarm indication, the alarm is still present on the Alarms tab in CTC and appropriate action is needed to clear the alarm. For information about connecting to alarm collection equipment, refer to the *Cisco ONS 15327 Procedure Guide*. To clear alarms, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

1.8 Timing Installation

The ONS 15327 supports two BITS clock interfaces. The physical connection is provided through an RJ-45 connector on each MIC. Two pins on each RJ-45 are used for BITS timing. BITS 1 In (MIC A) and BITS 2 In (MIC B) use Pins 3 and 4. BITS 1 Out (MIC A) and BITS 2 Out (MIC B) use Pins 7 and 8. The BITS 1 pins support output and input from the first external timing device. The BITS 2 pins perform the identical functions for the second external timing device. Table 1-6 lists the pin assignments for the BITS timing pin fields. For more information about connecting BITS timing to the ONS 15327, refer to the *Cisco ONS 15327 Procedure Guide*.

Table 1-6 External Timing Pin Assignments for BITS

External Device	Contact	RJ-45 Pin	Tip & Ring	Function
First external device (MIC A)	BITS 1 Out	7	Primary ring (–)	Output to external device
	BITS 1 Out	8	Primary tip (+)	Output to external device
	BITS 1 In	3	Secondary ring (–)	Input from external device
	BITS 1 In	4	Secondary tip (+)	Input from external device
Second external device (MIC B)	BITS 2 Out	7	Primary ring (–)	Output to external device
	BITS 2 Out	8	Primary tip (+)	Output to external device
	BITS 2 In	3	Secondary ring (–)	Input from external device
	BITS 2 In	4	Secondary tip (+)	Input from external device

Note Refer to Telcordia SR-NWT-002224 for rules about how to provision timing references.

1.9 Cards and Slots

Caution Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

ONS 15327 cards have electrical plugs at the back that plug into electrical connectors on the shelf assembly backplane. When the ejectors are fully closed, the card plugs into the assembly backplane. Figure 1-19 on page 1-21 shows the slot numbering.

Note DS-1 and DS-3 interfaces are not intended for direct connection to the network. These interfaces should be connected to the network via a channel service unit/data service unit (CSU/DSU) that has the proper certification.

1.9.1 Slot Requirements

The ONS 15327 shelf assembly has eight card slots: four traffic card slots (Slots 1 to 4), two XTC slots (Slots 5 and 6), and two MIC slots (Slots 7 and 8). The wider slots host the XTC cards and MICs. The narrower slots host Ethernet, OC-3, OC-12, and OC-48 (traffic) cards.

The XTC slots host both XTC-14 and XTC-28-3 cards. XTC cards are required for system operation. The MIC slots host MIC A and MIC B cards. The MIC slots are keyed to ensure that you install the MICs in the correct slot. Install MIC A in the bottom MIC slot (Slot 8) and MIC B in the top MIC slot (Slot 7). MICs are also required for system operation. Make DS-1 and DS-3 connections using the connectors on the MICs. Refer to Chapter 2, “Card Reference” for more information about ONS 15327 cards.

Table 1-7 lists the number of ports, line rates, connector options, and connector locations for ONS 15327 electrical, Ethernet, and optical interfaces.

Table 1-7 Port Line Rates, Connector Types, and Locations

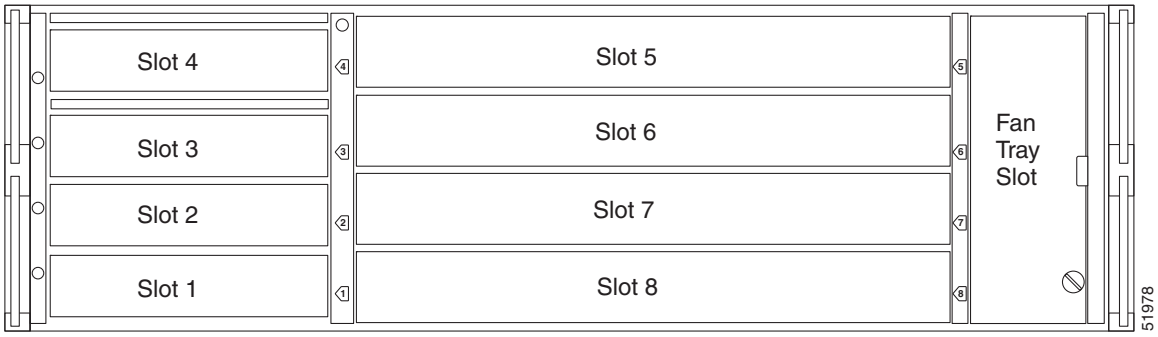
Interface	Ports	Line Rate per Port	Connector Types	Connector Location
DS-1	1–28	1.544 Mbps	CHAMP Connector	MIC faceplate
DS-3	3	44.736 Mbps	BNC	MIC faceplate
E10/100-4	4	10/100 Mbps	RJ-45	E10/100-4 card faceplate
G1000-2	2	1000 Mbps	LC (GBIC)	G1000-2 card faceplate
OC-3 IR 1310	4	155.52 Mbps (STS-3)	LC	OC-3 IR 1310 card faceplate
OC-12 IR 1310	1	622.08 Mbps (STS-12)	SC	OC-12 IR 1310 card faceplate
OC-12 LR 1550	1	622.08 Mbps (STS-12)	SC	OC-12 LR 1550 card faceplate
OC-48 IR 1310	1	2488.32 Mbps (STS-48)	SC	OC-48 IR 1310 card faceplate
OC-48 LR 1550	1	2488.32 Mbps (STS-48)	SC	OC-48 LR 1550 card faceplate

1.9.2 Card Installation

The procedure for installing ONS 15327 cards is slightly different for each card. Before installing any XTC or traffic cards, install at least one MIC and apply power to the shelf assembly. First install MIC A in Slot 8. After successfully connecting the power to MIC A, install MIC B followed by the XTC cards. Install any traffic cards after you have successfully installed and turned up the XTC cards and MICs.

Figure 1-19 shows the location and number of each card slot.

Figure 1-19 ONS 15327 Slot Numbering



Note Because all traffic cards boot from the working XTC card, at least one XTC card must be installed in order to boot any traffic cards.

Figure 1-20 shows XTC card installation.

Figure 1-20 Installing an XTC Card (XTC 28-3)

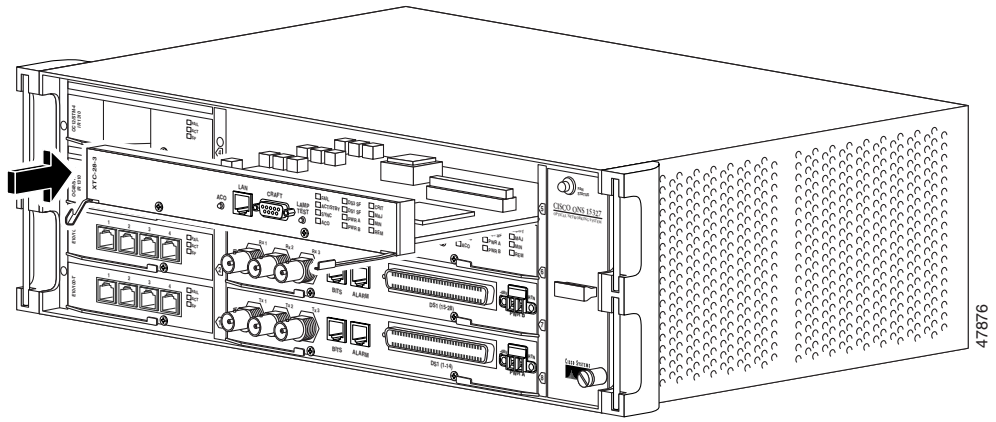
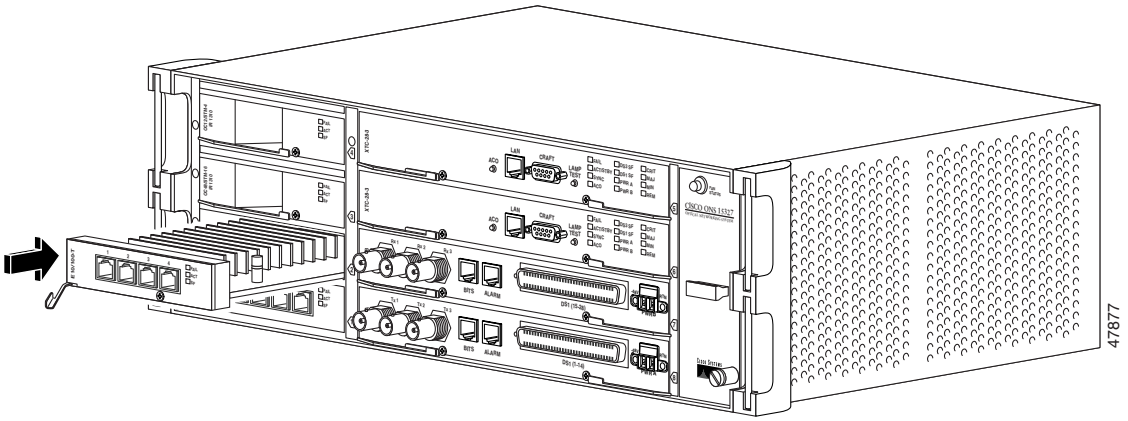


Figure 1-21 shows and Ethernet card used as an example for traffic card installation.

Figure 1-21 Installing an Ethernet Traffic Card



CHAPTER 2

Card Reference

This chapter describes the Cisco ONS 15327 cards. It includes descriptions, hardware specifications, and block diagrams for each card. For installation and turn-up procedures, refer to the *Cisco ONS 15327 Procedure Guide*.

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.

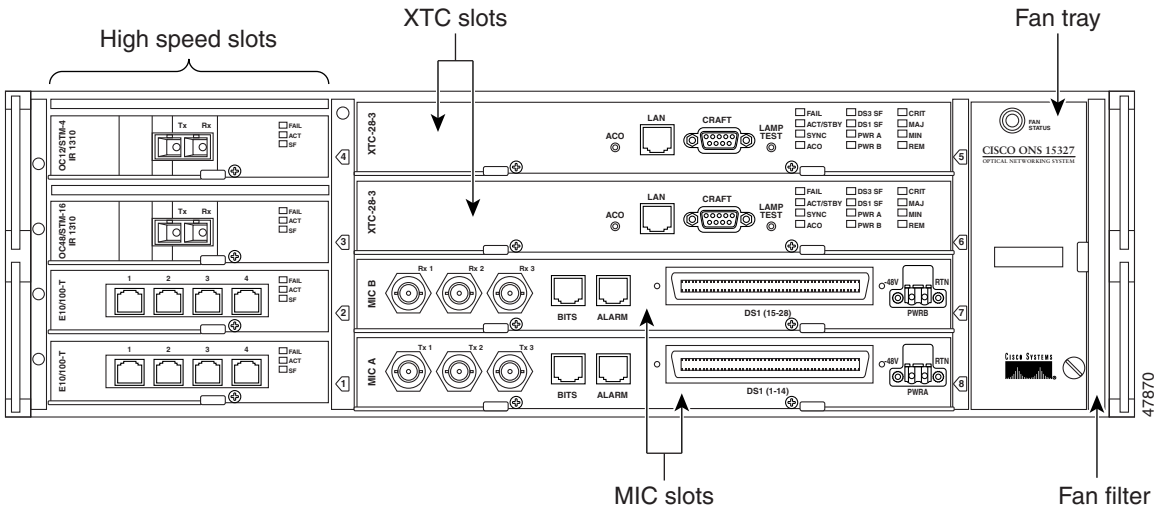
Chapter topics include:

Note The I-Temp symbol is located on the faceplate of an I-Temp-compliant card. A card without this symbol is C-Temp compliant.

2.1 Overview

The Cisco ONS 15327 uses common control cards, mechanical interface cards, optical cards, an Ethernet/Fast Ethernet card, and a Gigabit Ethernet card. This overview provides a summary of the cards. Figure 2-1 shows the ONS 15327 slot assignments.

Figure 2-1 ONS 15327 Slot Assignments



2.1.1 Card Compatibility

This section lists ONS 15327 cards and their compatible software versions. In the table below, "Yes" means the cards are compatible with the listed software version. Table cells with dashes mean cards are not compatible with the listed software versions.

Table 2-1 lists Cisco Transport Controller (CTC) software release compatibility for each card.

Table 2-1 Cards Software Release Compatibility

Card	R1.0	R3.3	R3.4	R4.0 R4.1	R4.6	R5.0	R5.0	R6.0
XTC-28-3	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
XTC-14	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MIC-28-3-A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MIC-28-3-B	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OC-3 IR 4 1310	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OC12 IR 1310	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OC-12 LR 1550	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OC48-I13-T	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OC-48 LR 1550	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
E10/100-4	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
G1000-2	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes

2.1.2 Common Control Cards

The two common control cards are the Cross-Connect, Timing, and Control (XTC-28-3 and XTC-14) cards. Both cards provide timing, control, and digital cross-connect functions. They also provide the EIA/TIA-232 DB9 TL1 connection and RJ-45 LAN connection. The XTC-28-3 provides electrical-tributary circuitry for 28 DS-1s and three DS-3s. The XTC-14 provides electrical-tributary circuitry for 14 DS-1s.

2.1.3 Mechanical Interface Cards

The mechanical interface cards (MICs) provide the physical connection points for the DS-1 and DS-3 interfaces on the XTC cards, the redundant power inputs, the alarm inputs and outputs, and the building integrated timing supply (BITS) inputs and outputs.

2.1.4 Optical Cards

The ONS 15327 optical cards include:

- OC3 IR 4 1310—Provides four intermediate-reach OC-3 interfaces
- OC12 IR 1310—Provides one intermediate- or short-reach OC-12 interface
- OC12 LR 1550—Provides one long-reach OC-12 interface
- OC48 IR 1310—Provides one intermediate-reach OC-48 interface
- OC48 LR 1550— Provides one long-reach OC-48 interface

2.1.5 E10/100-4 Ethernet Card

The Ethernet card provides four Layer 2 switched, autosensing, 10/100BaseT Ethernet interfaces. Each interface supports full-duplex operation for a maximum bandwidth of 200 Mbps per port.

2.1.6 Gigabit Ethernet Card

The Gigabit Ethernet card provides two 1000-Mbps Gigabit Ethernet interfaces. Each interface supports full-duplex operation for a maximum bandwidth of 2000 Mbps per port.

2.2 XTC Cards (XTC-28-3/XTC-14)

Note For hardware specifications, see the "A.3.1 XTC Card (XTC 28-3/XTC-14) Specifications" section on page A-4.

This section describes the features and functions of the XTC cards.

2.2.1 XTC Card Overview

The XTC cards perform system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection and resolution, SONET data communication channel (DCC) termination, system fault detection, and cross-connect maintenance and management for the ONS 15327. The XTC cards also provide the circuitry for the DS-1 and DS-3 interfaces and ensure that the system maintains Telcordia timing requirements.

An XTC card is required to operate the ONS 15327 and can be used in a redundant or nonredundant configuration. Figure 2-2 shows the XTC-28-3 faceplate.

Note You can connect to either the active or standby XTC using the LAN or CRAFT port, but you cannot connect to both cards simultaneously. Connecting to both the active and standby XTC at the same time results in a loss of connectivity.

Figure 2-2 XTC-28-3 Card Faceplate

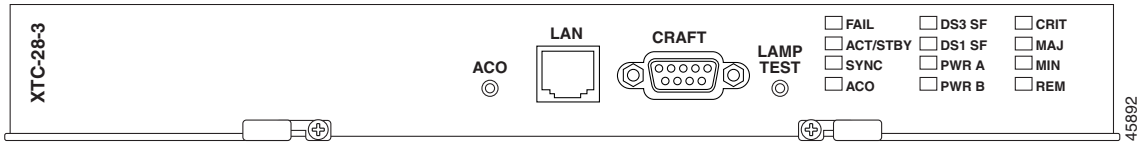
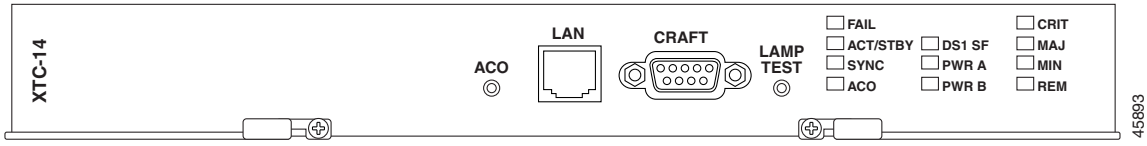


Figure 2-3 shows the XTC-14 faceplate.

Figure 2-3 XTC-14 Card Faceplate



2.2.2 XTC Front Panel

The XTC cards have an alarm cutoff (ACO) button, an RJ-45 LAN port, an EIA/TIA-232 TL1 (CRAFT) interface port, and a LAMP TEST button. The XTC-28-3 front panel has 12 LEDs, and the XTC-14 front panel has 11 LEDs. The following list describes each LED:

- The red FAIL LED indicates an XTC hardware problem. Replace the card if the FAIL LED persists.
- The ACT/STBY (Active/Standby) LED indicates whether the XTC is active and providing timing reference and shelf control (green), or is in standby to the active XTC (amber). When the active XTC is writing to its database or to the standby XTC database, the card LEDs blink. To avoid memory corruption, do not remove the XTC when the active or standby LED is blinking.
- The green SYNC LED turns on when the active XTC qualifies a timing reference from the optical facility or an external BITS input.
- The ACO LED indicates that the ACO function has been activated. To activate the ACO, press the ACO button on the front panel.
- The DS3 SF LED (XTC-28-3 only) indicates a signal fail with one or more of the DS-3 interfaces.

- The DS1 SF LED indicates a signal fail with one or more of the DS-1 interfaces.
- The green PWR A and PWR B LEDs illuminate when adequate power voltage is being received by the PWR A and PWR B connections on the MIC cards.
- The CRIT LED turns on when a critical alarm is present.
- The MAJ LED turns on when a major alarm is present.
- The MIN LED turns on when a minor alarm is present.
- The red REM LED turns on when a remote alarm is present in one or more of the remote terminals, or if an external alarm or condition is present.

2.2.3 Support for DS-1 and DS-3

The XTC cards contain the circuitry for connecting DS-1s. The XTC-28-3 also contains the circuitry for connecting DS-3s. The XTC-28-3 supports 28 DS-1s and 3 DS-3s. The XTC-14 supports 14 DS-1s. The DS-1 circuitry on the XTC cards maps each of the received DS-1 signals into VT 1.5s and concatenates these virtual tributaries (VTs) into one STS-1. Full VT1.5 grooming is supported.

The physical connection points are located on the MIC. See the "2.3.1 MIC Overview" section on page 2-8 for more information about physical connections.

2.2.4 XTC Timing and Control Functionality

The XTC cards combine the timing and control functions into one card. You can install the XTC cards in one or both of the common control slots (Slots 5 and 6). XTC cards must be installed in both of the common control slots for redundancy. In a nonredundant configuration, you must install the XTC in Slot 6.

The XTC cards support multichannel, high-level data link control (HDLC) processing for the DCC. Up to four DCCs can be routed over the serial communication interface (SCI) and terminated at the XTC card. The XTC cards process ten DCCs to enable remote system management interfaces.

Note ONS 15327 Release 3.3 and later support DCC tunneling of non-Cisco equipment.

The node database, IP address, and system software are stored in XTC card nonvolatile memory, which allows quick recovery in the event of a power or card failure.

The XTC cards perform all system-timing functions for each ONS 15327. The XTC cards select a recovered clock from optical line cards, a BITS, or an internal Stratum 3 reference as the system-timing reference. You can provision any of the clock inputs as a primary or secondary timing source. A slow-reference tracking loop allows the XTC cards to synchronize to the recovered clock, which provides holdover if the reference is lost.

In a redundant configuration, if the working XTC card fails, traffic switches to the protect XTC card. All XTC protection switches conform to protection switching standards when the bit error rate (BER) counts are not in excess of 1 E-3 and completion time is less than 50 ms.

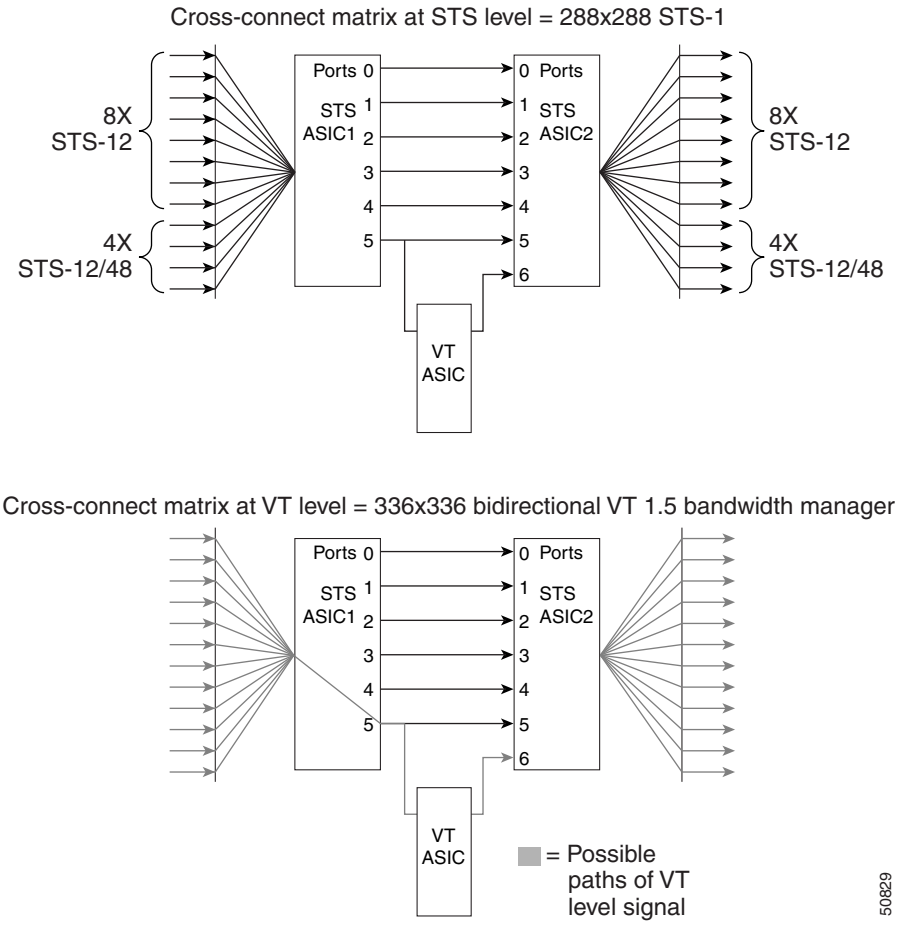
The XTC cards feature an RJ-45 10BaseT LAN port and an EIA/TIA-232 DB9 type craft interface for user interfaces. The craft port runs at 9600 bps.

2.2.5 XTC Cross-Connect Functionality

The XTC card is the central element for ONS 15327 switching. It establishes cross connections and performs time-division switching (TDS) at the STS-1 and VT 1.5 level between ONS 15327 traffic cards.

The switch matrix on the XTC card consists of 288 bidirectional ports. When creating bidirectional STS-1 cross-connects, each cross-connect uses two STS-1 ports. This results in 144 bidirectional STS-1 cross-connects. The switch matrix is nonblocking and broadcast supporting. This allows network operators to concentrate or groom low-speed traffic from line cards onto high-speed transport spans and to drop low-speed traffic from transport spans onto line cards. Figure 2-4 shows the cross-connect matrix for the XTC card.

Figure 2-4 Cross-Connect Matrix



The XTC card supports a total of 672 cross-connects with a payload granularity of VT 1.5. The VT functionality supports ring configurations with a mix of VT-capable Cisco transport network elements (NEs) and STS-only capable Cisco transport NEs.

The XTC card provides protection switching control for external and internal VT paths. The card also performs path- and STS-level monitoring and protection switching.

2.2.6 VT Mapping

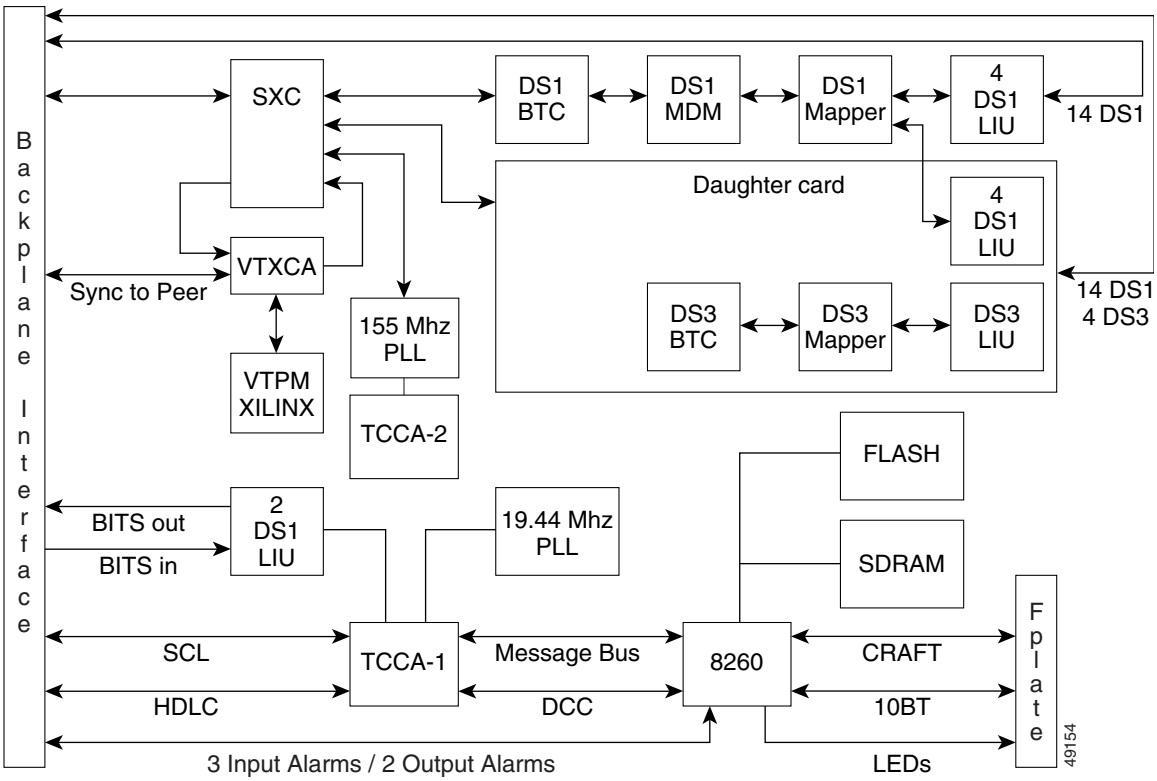
The ONS 15327 performs VT mapping according to Telcordia GR-253 standards. Table 2-2 shows the VT numbering scheme for the ONS 15327 as it relates to the Telcordia standard.

Table 2-2 VT Mapping

ONS 15327 VT Number	Telcordia Group/VT Number
VT1	Group1/VT1
VT2	Group2/VT1
VT3	Group3/VT1
VT4	Group4/VT1
VT5	Group5/VT1
VT6	Group6/VT1
VT7	Group7/VT1
VT8	Group1/VT2
VT9	Group2/VT2
VT10	Group3/VT2
VT11	Group4/VT2
VT12	Group5/VT2
VT13	Group6/VT2
VT14	Group7/VT2
VT15	Group1/VT3
VT16	Group2/VT3
VT17	Group3/VT3
VT18	Group4/VT3
VT19	Group5/VT3
VT20	Group6/VT3
VT21	Group7/VT3
VT22	Group1/VT4
VT23	Group2/VT4
VT24	Group3/VT4
VT25	Group4/VT4
VT26	Group5/VT4
VT27	Group6/VT4
VT28	Group7/VT4

Figure 2-5 shows the block diagram for the XTC card.

Figure 2-5 XTC Block Diagram



2.3 Mechanical Interface Cards

Note For hardware specifications, see the "A.3.2 MIC Specifications" section on page A-5.

This section describes the features and functions of the MICs.

2.3.1 MIC Overview

Two MICs (MIC A and MIC B) are required to operate the ONS 15327 when using XTC-28-3 cards or when redundant power inputs are needed. The MICs provide power connection points, physical interfaces for DS-1s and DS-3s, and external timing and alarm interfaces.

Figure 2-6 shows the MIC A faceplate. MIC A is keyed so that it can only be installed in Slot 8.

Figure 2-6 MIC A Faceplate

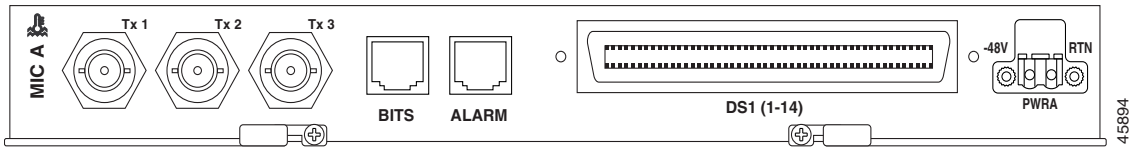
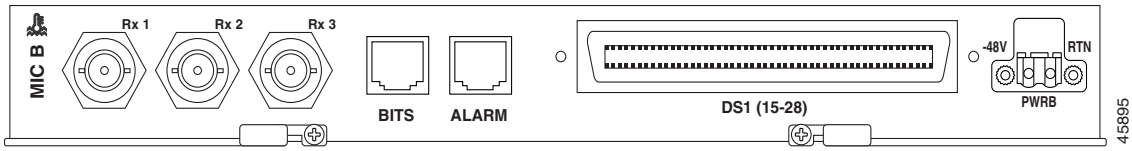


Figure 2-7 shows the MIC-28-3-B faceplate. MIC-B is keyed so that it can only be installed in Slot 7.

Figure 2-7 MIC B Faceplate



2.3.2 DS-1 Physical Interface

Each MIC uses a 64-pin Champ connector to provide 14 DS-1 interfaces. MIC-28-3-A provides connection to DS-1s 1 to 14, and MIC-28-3-B provides connection to DS-1s 15 to 28. The XTC cards house the electrical tributary circuitry for managing the individual DS-1s.

2.3.3 DS-3 Physical Interface

Because the transmit (out) and receive (in) interfaces are on different cards, you must install both MICs to use the DS-3 capabilities of the ONS 15327. The DS-3 interfaces use BNC connectors. MIC-28-3-A provides the three transmit (Tx) interfaces and MIC-28-3-B provides the three receive (Rx) interfaces. The XTC-28-3 card houses the electrical-tributary circuitry for managing DS-3s.

2.3.4 Power Connection

Each MIC has one –48 VDC power terminal that uses spring terminal block connectors and accepts #12 to #16 AWG wire (the National Electrical Code [NEC] requires #12 to #14 AWG wire). To establish redundant power, install both MICs and connect each one to a power source.

2.3.5 External Alarms and Controls

Each MIC has three Form C discrete external alarm inputs and one Form C discrete external control. Connection to the external alarms and controls uses an RJ-45 connector. Two wires of the RJ-45 connector are used for the external control, which defaults to the open position. Six wires of the RJ-45 connector are used for the external alarm input.

In CTC, you can provision the six external alarm inputs (three on each MIC) and the two external controls (one on each MIC). External alarm inputs are typically used for external sensors such as open doors, temperature sensors, flood sensors, and other environmental conditions. They can be set to Alarm on Closure or Alarm on Open. The alarm severity can be set to any of five available levels (Critical,

Major, Minor, Not Alarmed, Not Reported). In addition to severity, you can set alarm type and virtual wire for alarm contacts 1 to 4 and define when the alarm is raised. You can assign a 63-character alarm description for display in the alarm log of the CTC. The alarm condition remains raised until the external input quits driving the contact and you clear the alarm in the CTC. For instructions, refer to the *Cisco ONS 15327 Procedure Guide*.

External controls are typically used to drive visual or audible devices such as bells and lights, but they can control other devices such as generators, heaters, and fans. You can set them to close when the specified alarm condition is triggered; the default condition for output alarms is the open position. The alarm triggering conditions can be any ONS 15327 alarm condition including the user-defined input alarms, severity-based alarms (for example, trigger when any major alarm occurs), or remote alarms. CTC provisioning of this alarm-to-output-contact association is menu driven and includes alarms and individual alarms within categories. The output contact electrical interface is 50 V, 100 mA. To provision external controls, refer to the *Cisco ONS 15327 Procedure Guide*.

2.3.6 BITS Interface

Each MIC provides connection for one BITS clock input and one BITS clock output using an RJ-45 connector. Each MIC uses two wires of the RJ-45 connector.

2.4 OC3 IR 4 1310 Card

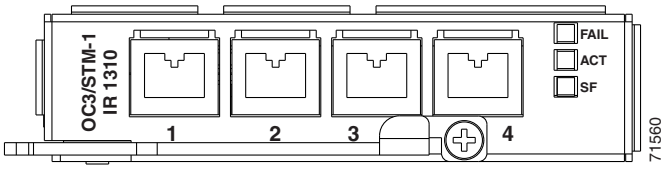
Note For hardware specifications, see the "A.3.3 OC3 IR 4 1310 Card Specifications" section on page A-5.

This section describes the features and functions of the OC3 IR 4 1310 card.

2.4.1 OC3 IR 4 1310 Card Description

The OC3 IR 4 1310 card provides four intermediate-reach, Telcordia-compliant, GR-253 SONET OC-3 interfaces per card. The interface operates at 155.52 Mbps over a single-mode fiber span and supports VT payloads and nonconcatenated or concatenated payloads for STS-1 or STS-3c. Figure 2-8 shows the OC3 IR 4 1310 faceplate.

Figure 2-8 OC3 IR 4 1310 Card Faceplate



You can install the OC3 IR 4 1310 card in any ONS 15327 high-speed card slot. The card can be provisioned as part of a path protection or a linear add-drop multiplexer (ADM) configuration.The card does not support bidirectional line-switched rings (BLSR). Each port features a 1310 nm laser and contains a transmit and receive connector on the card faceplate (the left-hand connector is the transmit [Tx] port and the right-hand connector is the receive [Rx] port). The card uses LC connectors.

The OC3 IR 4 1310 card supports 1+1 unidirectional or bidirectional protection switching. You can provision protection on a per-port basis. See the "3.1.2 Optical 1+1 Protection" section on page 3-2 for more information.

The OC3 IR 4 1310 detects loss of signal (LOS), loss of frame (LOF), loss of pointer (LOP), alarm indication signal-line (AIS-L), and line remote defect indication (RDI-L) conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* for a description of these conditions. The card also counts section and line bit interleaved parity (BIP) errors.

2.4.2 OC3 IR 4 1310 Card-Level Indicators

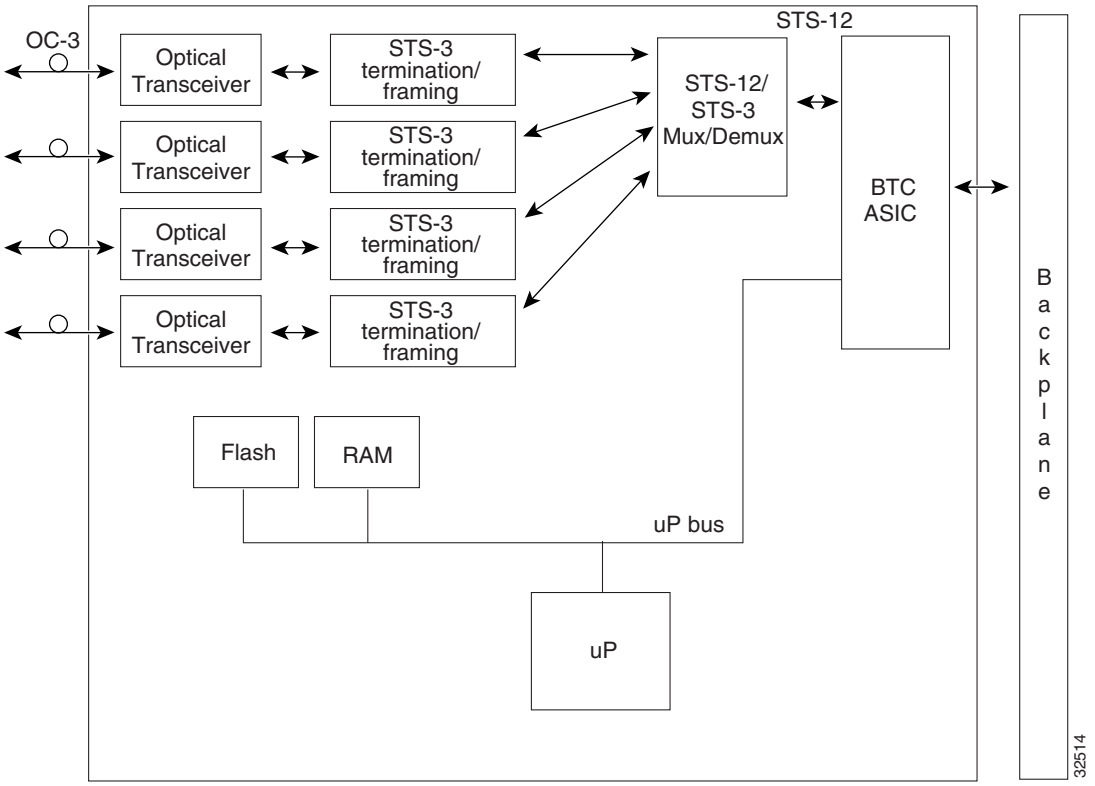
Table 2-3 describes the three card-level LED indicators on the OC3 IR 4 1310 card.

Table 2-3 OC3 IR 4 1310 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	Indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	Indicates that the OC3 IR 4 1310 card is carrying traffic or is traffic-ready.
Amber SF LED	Indicates a signal failure or condition such as loss of signal (LOS), loss of frame (LOF), line alarm indication signal (AIS-L), or high bit error rate (BER) on one or more of the card's ports. The amber signal fail (SF) LED also turns on when the transmit and receive fibers are incorrectly connected. The light turns off when the fibers are properly connected.

Figure 2-9 shows the OC3 IR 4 1310 card block diagram.

Figure 2-9 OC3 IR 4 1310 Card Block Diagram



2.5 OC12 IR 1310 Card

Note For hardware specifications, see the "A.3.4 OC12 IR 1310 Card Specifications" section on page A-6.

This section describes the features and functions of the OC12 IR 1310 card.

2.5.1 OC12 IR 1310 Card Description

The OC12 IR 1310 card provides one intermediate- or short-reach, SONET OC-12 interface per card, compliant with Telcordia GR-253. The interface operates at 622.08 Mbps over a single-mode fiber span and supports VT payloads and nonconcatenated or concatenated payloads for STS-1, STS-3c, STS-6c, or STS-12c. Figure 2-10 shows the OC12 IR 1310 faceplate.

Figure 2-10 OC12 IR 1310 Card Faceplate

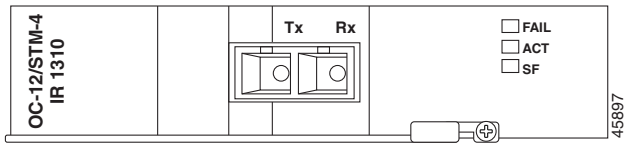
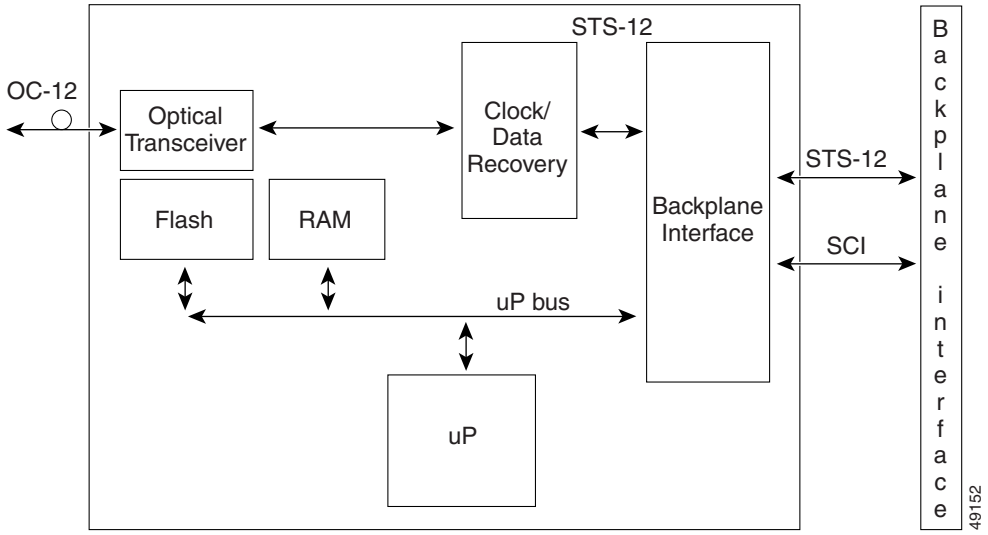


Figure 2-11 shows the OC12 IR 1310 card block diagram.

Figure 2-11 OC12 IR 1310 Card Block Diagram



You can install the OC12 IR 1310 card in any ONS 15327 high-speed slot and provision the card as a drop card or span (trunk) card in a two-fiber BLSR, path protection, or ADM (linear) configuration.

The OC12 IR 1310 port features a 1310-nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The OC12 IR 1310 card uses SC optical connections and supports 1+1 unidirectional and bidirectional protection.

The OC12 IR 1310 detects LOS, LOF, LOP, AIS-L, and RDI-L conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* for a description of these conditions. The card counts section and line BIT errors.

2.5.2 OC12 IR 1310 Card-Level Indicators

Table 2-4 describes the three card-level LED indicators on the OC12 IR 1310 card.

Table 2-4 OC12 IR 1310 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	Indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.

Table 2-4 OC12 IR 1310 Card-Level Indicators (continued)

Card-Level Indicators	Description
Green ACT LED	Indicates that the OC12 IR 1310 card is operational and is carrying traffic or is traffic-ready.
Amber SF LED	Indicates a signal failure or condition such as LOS, LOF, AIS-L or high BERs on the card's port. The amber SF LED also turns on when the transmit and receive fibers are incorrectly connected. The light turns off when the fibers are properly connected.

2.6 OC12 LR 1550 Card

Note For hardware specifications, see the "A.3.5 OC12 LR 1550 Card Specifications" section on page A-7.

This section describes the features and functions of the OC12 LR 1550 card.

2.6.1 OC12 LR 1550 Card Description

The OC12 LR 1550 card provides one long-reach, Telcordia-compliant, GR-253 SONET OC-12 interface per card. The interface operates at 622.08 Mbps over a single-mode fiber span and supports VT payloads and nonconcatenated or concatenated payloads for STS-1, STS-3c, STS-6c, or STS-12c. Figure 2-12 shows the OC12 LR 1550 faceplate.

Figure 2-12 OC12 LR 1550 Card Faceplate

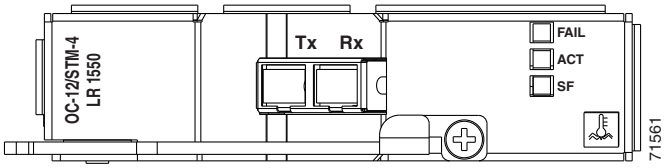
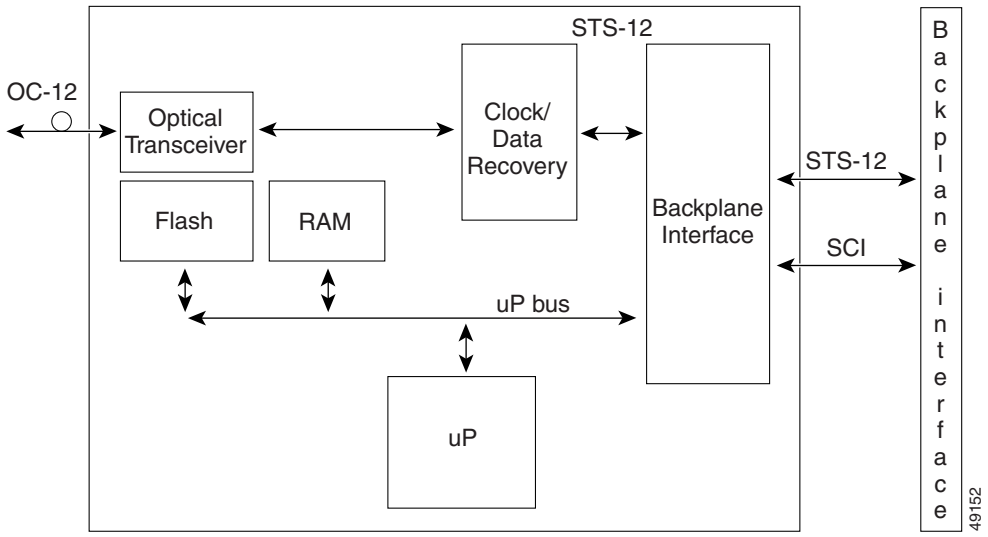


Figure 2-13 shows the OC12 LR 1550 card block diagram.

Figure 2-13 OC12 LR 1550 Card Block Diagram



You can install the OC12 LR 1550 card in any ONS 15327 high-speed card slot and provision the card as a drop card or span (trunk) card in a BLSR, path protection, or ADM (linear) configurations.

The OC-12 interface features a 1550-nm laser and contains a transmit (Tx) and receive (Rx) connector (labeled) on the card faceplate. The OC12 LR 1550 uses SC connectors. The OC12 LR 1550 card supports 1+1 unidirectional and bidirectional switching.

The OC12 LR 1550 detects LOS, LOF, and LOP, and AIS-L conditions (refer to the *Cisco ONS 15327 Troubleshooting Guide* for a complete description of alarm conditions). The OC12 LR 1550 counts path and line BIT errors.

The OC12 LR 1550 extracts the K1 and K2 bytes from the SONET overhead to perform an appropriate protection switch. The DCC bytes are forwarded to the DCC-terminating XTC.

2.6.2 OC12 LR 1550 Card-Level Indicators

Table 2-5 describes the three card-level LED indicators on the OC12 LR 1550 card.

Table 2-5 OC12 LR 1550 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	Indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	Indicates that the OC12 LR 1550 card is carrying traffic or is traffic-ready.
Amber SF LED	Indicates a signal failure or condition such as LOS, LOF or high BERs on the card's port. The amber SF LED also turns on when the transmit and receive fibers are incorrectly connected. The light turns off when the fibers are properly connected.

2.7 OC48-1-IR Card

Note For hardware specifications, see the "A.3.6 OC48-1-IR Card Specifications" section on page A-8.

This section describes the features and functions of the OC48-1-IR card.

2.7.1 OC48-1-IR Card Description

The OC48-1-IR card provides one intermediate-reach, Telcordia-compliant, GR-253 SONET OC-48 interface per card. Each interface operates at 2488.320 Mbps over a single-mode fiber span and supports VT payloads and nonconcatenated or concatenated payloads for STS-1, STS-3c, STS-6c, STS-12c, or STS-48c. Figure 2-14 shows the OC48-1-IR faceplate.

Figure 2-14 OC48-1-IR Card Faceplate

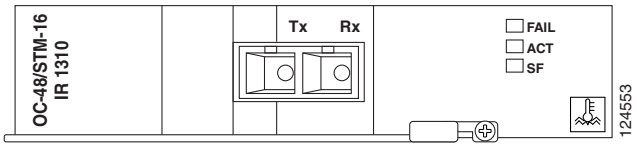
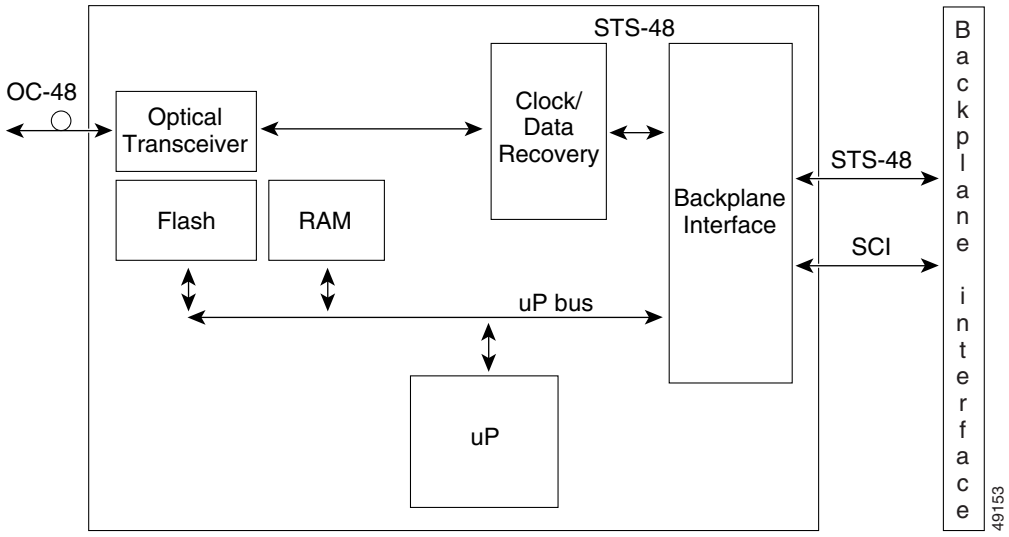


Figure 2-15 shows the OC48-1-IR block diagram.

Figure 2-15 OC48-1-IR Block Diagram



You can install the OC48-1-IR card in any ONS 15327 high-speed card slot and provision the card as a drop or span (trunk) card in a two-fiber BLSR, path protection, or in an ADM (linear) configuration.

The OC-48 port features a 1310-nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The OC48-1-IR uses SC connectors. The card supports 1+1 unidirectional and bidirectional protection switching.

The OC48-1-IR detects LOS, LOF, LOP, AIS-L, and RDI-L conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* for a description of these conditions. The card also counts section and line BIT errors.

2.7.2 OC48-1-IR Card-Level Indicators

Table 2-6 describes the three card-level LED indicators on the OC48-1-IR card.

Table 2-6 OC48-1-IR Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	Indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	Indicates that the OC48 1I13-T card is carrying traffic or is traffic-ready.
Amber SF LED	Indicates a signal failure or condition such as LOS, LOF, AIS-L or high BERs on the card's port. The amber SF LED also turns on when the transmit and receive fibers are incorrectly connected. The light turns off when the fibers are properly connected.

2.8 OC48 LR 1550 Card

Note For hardware specifications, see the "A.3.7 OC48 LR 1550 Card Specifications" section on page A-8.

This section describes the features and functions of the OC48 LR 1550 card.

2.8.1 OC48 LR 1550 Card Description

The OC48 LR 1550 card provides one intermediate-reach, Telcordia-compliant, GR-253 SONET OC-48 interface per card. Each interface operates at 2488.320 Mbps over a single-mode fiber span and supports VT payloads and nonconcatenated or concatenated payloads for STS-1, STS-3c, STS-6c, STS-12c, or STS-48c. Figure 2-16 shows the OC48 LR 1550 faceplate.

Figure 2-16 OC48 LR 1550 Card Faceplate

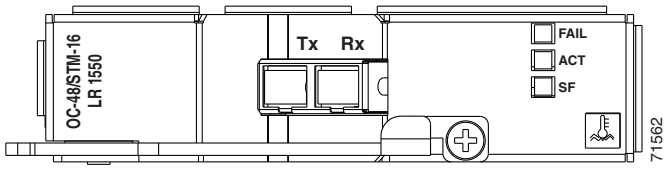
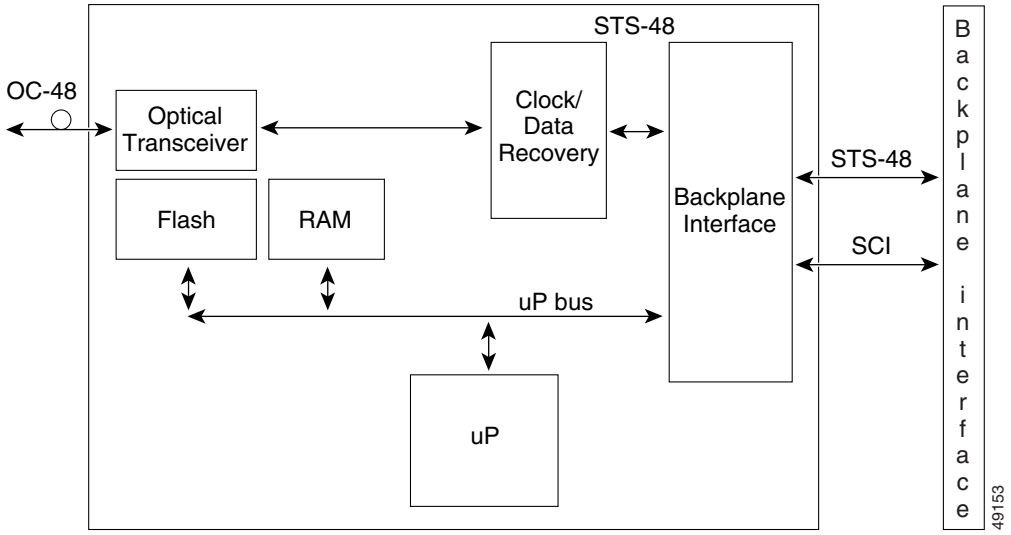


Figure 2-17 shows the OC48 LR 1550 block diagram.

Figure 2-17 OC48 LR 1550 Block Diagram



You can install the OC48 LR 1550 card in any ONS 15327 high-speed card slot and provision the card as a drop or span (trunk) card in a two-fiber BLSR, path protection, or ADM (linear) configuration.

The OC48 LR 1550 port features a 1550-nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The card uses SC connectors, and it supports 1+1 unidirectional and bidirectional protection switching.

The OC48 LR 1550 detects LOS, LOF, LOP, AIS-L, and RDI-L conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* for a description of these conditions. The card also counts section and line BIT errors.

2.8.2 OC48 LR 1550 Card-Level Indicators

Table 2-7 describes the three card-level LED indicators on the OC48 LR 1550 card.

Table 2-7 OC48 LR 1550 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	Indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	Indicates that the OC48 LR 1550 card is carrying traffic or is traffic-ready.
Amber SF LED	Indicates a signal failure or condition such as LOS, LOF, or high BERs on the card's port. The amber SF LED also turns on when the transmit and receive fibers are incorrectly connected. The light turns off when the fibers are properly connected.

2.9 E10/100-4 Card

Note For hardware specifications, see the "A.3.8 E10/100-4 Card Specifications" section on page A-9.

This section describes the features and functions of the E10/100-4 card.

2.9.1 E10/100-4 Card Description

The E10/100-4 card provides four IEEE 802.3-compliant, 10/100 interfaces. Each interface supports full-duplex operation for a maximum bandwidth of 200 Mbps per port and 622 Mbps per card. Each port can independently detect (autosense) the speed of an attached device and automatically connects at the appropriate speed. The ports autoconfigure to operate at either half or full duplex and can determine whether to enable or disable flow control. You can manually set the port speed and duplex mode.

Figure 2-18 shows the card faceplate.

Figure 2-18 E10/100-4 Card Faceplate

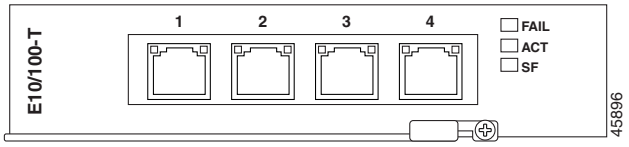
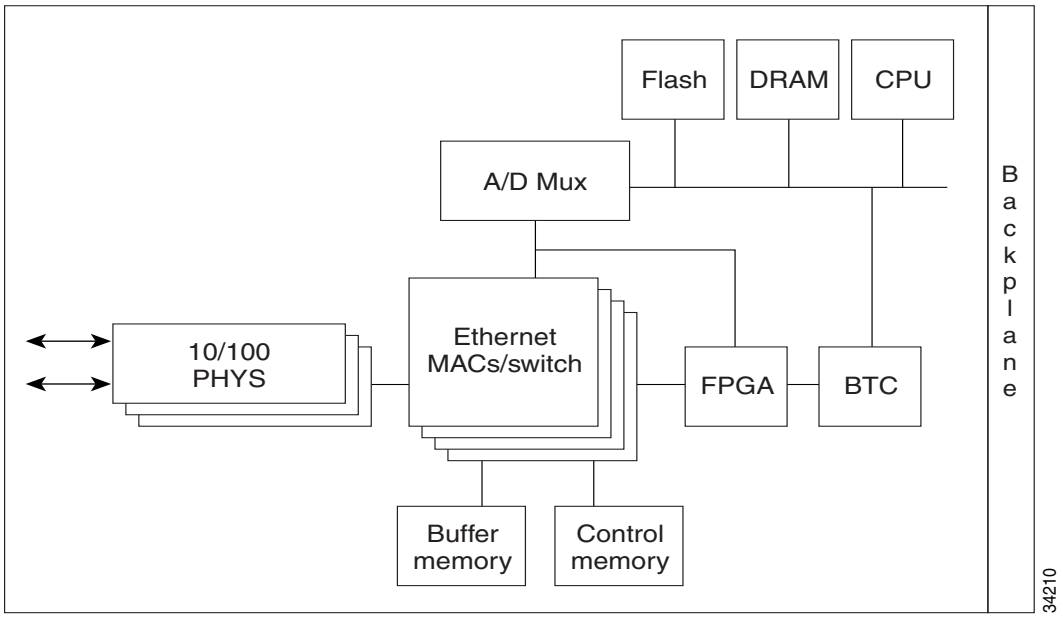


Figure 2-19 provides a block diagram of the E10/100-4 card.

Figure 2-19 E10/100-4 Block Diagram



The E10/100-4 Ethernet card provides high-throughput, low-latency packet switching of Ethernet traffic across a SONET network while providing a greater degree of reliability through SONET “self-healing” protection services. This Ethernet capability enables network operators to provide multiple 10/100 Mbps access drops for high-capacity customer LAN interconnects, Internet traffic, and cable modem traffic aggregation. Efficient transport and coexistence of traditional TDM traffic with packet-switched data traffic is provided.

Each E10/100-4 card supports standards-based, wire-speed, Layer 2 Ethernet switching between its Ethernet interfaces. IEEE 802.1Q-tag and port-based VLANs are supported in order to logically isolate traffic (typically subscribers). Priority queuing is also supported in order to provide multiple classes of service.

You can install the E10/100-4 card in any high-speed slot. Multiple Ethernet cards installed in an ONS 15327 can act as a single switch or multiple switches supporting a variety of SONET port configurations. To create logical SONET ports, provision a number of STS channels to the packet switch entity within the ADM. You can create logical ports with a bandwidth granularity of STS-1. The ONS 15327 can support six STS-1s, two STS-3cs, one STS-6c, or one STS-12c in single-card EtherSwitch mode. It supports three STS-1s or one STS-3c in multicard EtherSwitch mode.

2.9.2 E10/100-4 Card-Level Indicators

Table 2-8 describes the two card-level LED indicators The E10/100-4 card faceplate has three LEDs, described in Table 2-8.

Table 2-8 E10/100-4 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	Indicates that the card's processor is not ready or catastrophic software failure occurred on the E10/100-4 card. As part of the boot sequence, the FAIL LED is turned on until the software deems the card operational.
Green ACT LED	Provides the operational status of the E10/100-4. When the ACT LED is green it indicates that the E10/100-4 card is active and the software is operational.
SF LED	Not in use for this release.

2.9.3 E10/100-4 Port-Level Indicators

Table 2-9 describes the four pairs of LEDs (one pair for each port) on the E10/100-4 card that indicate status, such as signal or equipment failures.

Table 2-9 E10/100-4 Port-Level Indicators

LED State	Description
Amber	Transmitting and receiving
Solid Green	Idle and link integrity
Green Light Off	Inactive connection or unidirectional traffic

2.10 G1000-2 Card

Note For hardware specifications, see the "A.3.9 G1000-2 Card Specifications" section on page A-9.

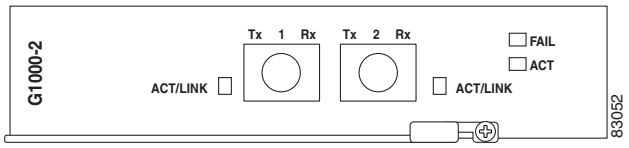
This section describes the features and functions of the ONS 15327 Gigabit Ethernet card, called the G1000-2 card.

2.10.1 G1000-2 Card Description

The G1000-2 provides two IEEE 802.3-compliant, 1000 Mbps ports for high-capacity customer LAN interconnections. Each port supports full-duplex operation for a maximum bandwidth of 2000 Mbps per port or support of Gigabit Ethernet traffic at full line rate. The SONET circuit sizes supported are STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, and STS-48c.

Figure 2-20 shows the card faceplate.

Figure 2-20 G1000-2 Card Faceplate



The G1000-2 Gigabit Ethernet card provides high-throughput, low latency transport of Ethernet encapsulated traffic (IP and other Layer 2 or Layer 3 protocols) across a SONET network. Carrier-class Ethernet transport is achieved by hitless (< 50 ms) performance in the event of any failures or protection switches (such as 1+1 APS, path protection, or BLSR) and software upgrades. Full provisioning support is possible via CTC, TL1, or CTM (refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide* for G-Series TL1 provisioning commands).

The card also features SONET-style alarms support, Ethernet PM and RMON functions, and serviceability options including enhanced port states, terminal and facility loopbacks on OC-N circuit paths, and J1 path trace. For additional information about terminal and facility loopbacks, refer to the *Cisco ONS 15327 Troubleshooting Guide.*

2.10.2 SFPs

The G1000-2 card uses standard Small Form-factor Pluggable (SFP) modules for the optical ports. SFPs are input/output devices that plug into a Gigabit Ethernet port to link the port to the fiber-optic network. Cisco provides two SFP modules: one for short-reach applications and one for long-reach applications. The short-reach model connects to multimode fiber and the long-reach model requires single-mode fiber.

Both SFP modules are offered as separate orderable products: an IEEE 1000BaseSX compliant, 85-nm optical module and an IEEE 1000BaseLX-compliant, 1300-nm optical module. The 850-nm SX optics are designed for multimode fiber and distances of up to 220 meters (721.8 feet) on 62.5 micron fiber and up to 550 meters (1,804.5 feet) on 50 micron fiber. The 1300-nm LX optics are designed for single-mode fiber and distances of up to 10 kilometers (6.2 miles).

See the "A.2 SFP Specifications" section on page A-4 for more information.

2.10.3 G1000-2 Card-Level Indicators

Table 2-10 describes the two card-level LED indicators on the G1000-2 card.

Table 2-10 G1000-2 Card-Level Indicators

Card-Level LEDs	Description
FAIL LED (red)	The red FAIL LED indicates that the card's processor is not ready or a catastrophic software failure occurred on the G1000-2 card. As part of the boot sequence, the FAIL LED is turned on, and it turns off if the software is deemed operational. The red FAIL LED blinks when the card is loading software.
ACT LED (green)	A green ACT LED provides the operational status of the G1000-2. If the ACT LED is green it indicates that the G1000-2 card is active and the software is operational.

2.10.4 G1000-2 Port-Level Indicators

The G1000-2 card also has one bicolor ACT/LINK LED per port. Table 2-11 describes the status that each color represents.

Table 2-11 G1000-2 Port-Level Indicators

Port-Level LED	Description
Off	No link exists to the Ethernet port.
Steady Amber	A link exists to the Ethernet port, but traffic flow is inhibited. For example, an unconfigured circuit, an error on line, or a nonenabled port may inhibit traffic flow.
Solid Green	A link exists to the Ethernet port, but no traffic is carried on the port.
Flashing Green	A link exists to the Ethernet port, and traffic is carried on the port. The LED flash rate reflects the traffic rate for the port.

Card Protection

This chapter explains the Cisco ONS 15327 card protection configurations. To provision card protection, refer to the *Cisco ONS 15327 Procedure Guide*. Chapter topics include:

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.

3.1 ONS 15327 Protection Groups

When you set up optical protection for ONS 15327 cards, you must choose between maximum protection and maximum slot availability. The highest protection reduces the number of available card slots; the highest slot availability reduces the protection. Table 3-1 shows the protection types that can be set up for ONS 15327 cards. Refer to the “Maintain the Node” chapter of the *Cisco ONS 15327 Procedure Guide* for information on setting up protection groups.

Table 3-1 Card Protection Group Types

Type	Cards	Description
1:1	XTC	Default electrical circuits protection (cannot be changed).

Table 3-1 Card Protection Group Types (continued)

Type	Cards	Description
1+1	Any optical	Pairs a working optical port with a protect optical port. Protect ports must match the working ports. For example, Port 1 of an OC-3 card can only be protected by Port 1 of another OC-3 card. Cards do not need to be in adjoining slots.
Unprotected	Any	Unprotected cards can cause signal loss if a card fails or incurs a signal error. However, because no card slots are reserved for protection, unprotected schemes maximize the service available for use on the ONS 15327. Unprotected is the default protection type for optical cards.

3.1.1 Electrical 1:1 Protection

A 1:1 (electrical) XTC protection group is preprovisioned on the ONS 15327. The name of the protection group is XTCPROTGRP and it cannot be edited or deleted. Therefore, you only need to create protection for optical cards.

3.1.2 Optical 1+1 Protection

With 1+1 port-to-port protection, ports on the protect card are assigned to protect the corresponding ports on the working card. The working and protect cards do not need to be installed side by side in the node. A working card must be paired with a protect card of the same type, for example, an OC-3 card should be paired with another OC-3 card. The protection takes place on the port level, so any port on the protect card can be assigned to protect the corresponding port on the working card.

For example, on a four-port card, you can assign one port as a protection port on the protect card (protecting the corresponding port on the working card) and leave three ports unprotected. Conversely, you can assign three ports as protection ports and leave one port unprotected.

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

Note The OC3-4 card can be provisioned for path protection and a 1+1 protection group using two ports on the same card.

3.1.3 Unprotected Cards

Unprotected optical cards are not included in a protection scheme; therefore, a card failure or a signal error results in lost data. Because no bandwidth lies in reserve for protection, unprotected schemes maximize the available ONS 15327 bandwidth.

3.2 Automatic Protection Switching

Unidirectional switching allows traffic on the transmit and receive fibers to switch independently. With bidirectional switching, transmit and receive lines switch together.

With nonrevertive 1+1 protection, automatic protection switching (APS) switches a signal after a failure from the working card to the protect card and the signal stays switched to the protect card until it is manually switched back. Revertive switching automatically switches the signal back to the working card when the working card comes back online. 1+1 protection is unidirectional and nonrevertive by default; revertive switching is easily provisioned using CTC. Refer to the "Create Circuits and VT Tunnels" chapter of the *Cisco ONS 15327 Procedure Guide* for information on provisioning unidirectional or bidirectional circuits .

3.3 External Switching Commands

The external switching commands on the ONS 15327 are Manual, Force, and Lock Out. A Manual switch will switch traffic if the path has an error rate less than the signal degrade (SD). A Force switch will switch traffic even if the path has SD or signal fail (SF) condition; however, a Force switch does not override an SF on a 1+1 protection channel. A Force switch has a higher priority than a Manual switch. Lockouts can only be applied to protect card ports in 1+1 configurations. They prevent traffic from switching from the working port to the protect port under any circumstance. Lockouts have the highest priority.

Note Force and Manual switches do not apply to 1:1 protection group for the XTC; these ports have a single Switch command.

Cisco Transport Controller Operation

This chapter describes Cisco Transport Controller (CTC), the Cisco ONS 15327 software interface. For CTC setup and login information, refer to the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

4.1 CTC Software Delivery Methods

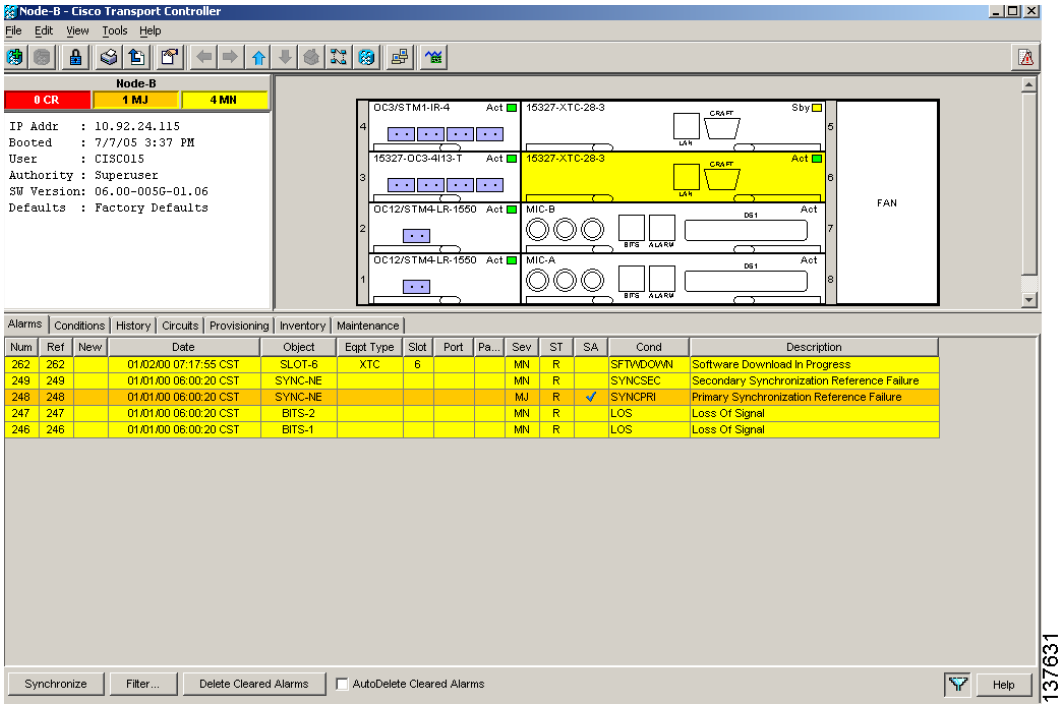
ONS 15327 provisioning and administration is performed using CTC software. CTC is a Java application that is installed in two locations; CTC is stored on the XTC card, and it is downloaded to your workstation the first time you log into the ONS 15327 with a new software release.

4.1.1 CTC Software Installed on the XTC Card

CTC software is preloaded on the ONS 15327 Cross-Connect, Timing, and Control (XTC) cards; therefore, you do not need to install software on the XTC cards. When a new CTC software version is released, use the release-specific software document to upgrade the ONS 15327 software on the XTC cards.

When you upgrade CTC software, the XTC cards store the new CTC version as the protect CTC version. When you activate the new CTC software, the XTC cards store the older CTC version as the protect CTC version, and the newer CTC release becomes the working version. You can view the software versions that are installed on an ONS 15327 by selecting the Maintenance > Software tabs in node view. Figure 4-1 shows a example of the node view. Select the tabs in network view to view the software versions installed on all the network nodes.

Figure 4-1 CTC Software Versions, Node View Example



4.1.2 CTC Software Installed on the PC or UNIX Workstation

CTC software is downloaded from the XTC cards and installed on your computer automatically when you connect to the ONS 15327 with a new software release for the first time. Downloading the CTC software files automatically ensures that your computer is running the same CTC software version as the XTC cards you are accessing. The CTC files are stored in the temporary directory designated by your computer operating system. You can use the Delete CTC Cache button to remove files stored in the temporary directory. If the files are deleted, they download the next time you connect to an ONS 15327. Downloading the Java archive (JAR) files for CTC takes several minutes depending on the bandwidth of the connection between your workstation and the ONS 15327. For example, JAR files downloaded from a modem or a data communications channel (DCC) network link require more time than JAR files downloaded over a LAN connection.

4.2 CTC Installation Overview

To connect to an ONS 15327 using CTC, enter the ONS 15327 IP address in the URL field of Netscape Navigator or Microsoft Internet Explorer. After connecting to an ONS 15327, the following events occur automatically:

1. A CTC launcher applet is downloaded from the XTC card to your computer.
2. The launcher determines whether your computer has a CTC release matching the release on the ONS 15327 XTC card.
3. If the computer does not have CTC installed, or if the installed release is older than the XTC card version, the launcher downloads the CTC program files from the XTC card.

4. The launcher starts CTC. The CTC session is separate from the web browser session, so the web browser is no longer needed. Always log into nodes having the latest software release. If you log into an ONS 15327 that is connected to ONS 15327s with older versions of CTC, or to Cisco ONS 15454s or Cisco ONS 15600s, CTC files are downloaded automatically to enable you to interact with those nodes. The CTC file download occurs only when necessary, such as during your first login. You cannot interact with nodes on the network that have a software version later than the node that you used to launch CTC.

Each ONS 15327 can handle up to five concurrent CTC sessions. CTC performance might vary, depending upon the volume of activity in each session, network bandwidth, and XTC card load.

Note You can also use TL1 commands to communicate with the Cisco ONS 15327 through VT100 terminals and VT100 emulation software, or you can telnet to an ONS 15327 using TL1 port 3083. Refer to the *Cisco ONS SONET TL1 Command Guide* for a comprehensive list of TL1 commands.

4.3 PC and UNIX Workstation Requirements

To use CTC in the ONS 15327, your computer must have a web browser with the correct Java Runtime Environment (JRE) installed for the software release in use. The correct JRE for each CTC software release is included on the Cisco ONS 15327 software CD. If you are running multiple CTC software releases on a network, the JRE installed on the computer must be compatible with the different software releases. You can change the JRE version on the Preferences dialog box JRE tab. When you change the JRE version on the JRE tab, you must exit and restart CTC for the new JRE version to take effect. Table 4-1 shows JRE compatibility with ONS software releases.

Table 4-1 JRE Compatibility

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible	JRE 1.4 Compatible
ONS 15327 Release 1.0	Yes	No	No
ONS 15327 Release 1.0.1	Yes	Yes	No
ONS 15327 Release 3.3	Yes	Yes	No
ONS 15327 Release 3.4	No	Yes	No
ONS 15327 Release 4.0[1]	No	Yes	No
ONS 15327 Release 4.1	No	Yes	No
ONS 15327 Release 4.6	No	Yes	Yes
ONS 15327 Release 5.0	No	No	Yes
ONS 15327 Release 6.0	No	No	Yes

1. Software Releases 4.0 and later will notify you if an older version JRE is running on your PC or UNIX workstation.

Table 4-2 lists the requirements for PCs and UNIX workstations. In addition to the JRE, the Java plug-in is also included on the ONS 15327 software CD.

Table 4-2 CTC Computer Requirements

Area	Requirements	Notes
Processor	Pentium III 700 MHz, UltraSPARC, or equivalent	700 Mhz is the recommended processor speed. You can use computers with a lower processor speed; however, you might experience longer response times and slower performance.
RAM	384 MB RAM recommended, 512 MB RAM optimum	Cisco recommends using 512 MG RAM for networks with 25 nodes or more to avoid longer response times and slower performance.
Hard drive	20 GB hard drive with 50 MB of space available	—
Operating system	• PC: Windows 98, Windows NT 4.0 with Service Pack 6a, Windows 2000, or Windows XP • UNIX Workstation: Solaris versions 8 or 9	—
Java Runtime Environment	JRE 1.4.2	JRE 1.4.2 is installed by the CTC Installation Wizard included on the Cisco ONS 15327 software CD. JRE 1.4.2 provides enhancements to CTC performance, especially for large networks with numerous circuits. Cisco requires that you use JRE 1.4.2 for networks with Software R6.0 (or R5.0) nodes. If CTC must be launched directly from nodes running software earlier than R5.0, Cisco recommends JRE 1.3.1_02.

Table 4-2 CTC Computer Requirements (continued)

Area	Requirements	Notes
Web browser	• PC: Netscape 4.76, Netscape 7.x, Internet Explorer 6.x • UNIX Workstation: Netscape 4.76, Netscape 7.x • Solaris 8 and 9: Mozilla application suite	For the PC, use JRE 1.4.2(or 1.3.1_02) with any supported web browser. For UNIX, use JRE 1.4.2 with Netscape 7.x or JRE 1.3.1_02 with Netscape 4.76. Netscape 4.76 or 7.x is available at the following site: http://channels.netscape.com/ns/browsers/default.jsp Internet Explorer 6.x is available at the following site: http://www.microsoft.com Mozilla is available at the following site: http://www.mozilla.org
Cable	User-supplied CAT-5 straight-through cable with RJ-45 connectors on each end to connect the computer to the ONS 15327 directly or though a LAN	—

4.4 ONS 15327 Connection Methods

You can connect to the ONS 15327 in multiple ways. You can connect your PC directly to the ONS 15327 (local craft connection) using the RJ-45 port on the XTC card or the LAN pins on the backplane, or by connecting your PC to a hub or switch that is connected to the ONS 15327. You can connect to the ONS 15327 through a LAN or modem, and you can establish TL1 connections from a PC or TL1 terminal. Table 4-3 lists the ONS 15327 connection methods and requirements.

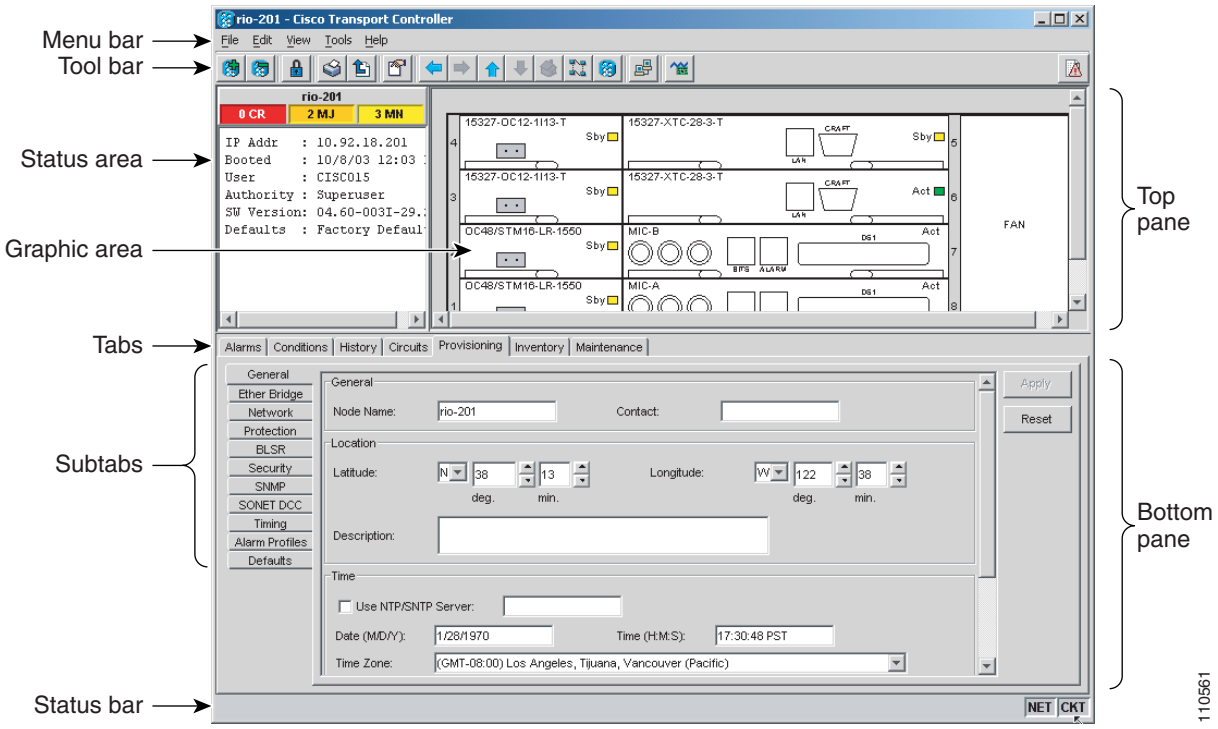
Table 4-3 ONS 15327 Connection Methods

Method	Description	Requirements
Local craft	Refers to onsite network connections between the CTC computer and the ONS 15327 using one of the following: • The RJ-45 (LAN) port on the XTC card • A hub or switch to which the ONS 15327 is connected	If you do not use Dynamic Host Configuration Protocol (DHCP), you must change the computer IP address, subnet mask, and default router, or use automatic host detection.
Corporate LAN	Refers to a connection to the ONS 15327 through a corporate or network operations center (NOC) LAN.	• The ONS 15327 must be provisioned for LAN connectivity, including IP address, subnet mask, and default gateway. • The ONS 15327 must be physically connected to the corporate LAN. • The CTC computer must be connected to the corporate LAN that has connectivity to the ONS 15327.
TL1	Refers to a connection to the ONS 15327 using TL1 rather than CTC. TL1 sessions can be started from CTC, or you can use a TL1 terminal. The physical connection can be a craft connection, corporate LAN, or a TL1 terminal. Refer to the *Cisco ONS SONET TL1 Command Guide*.	—
Remote	Refers to a connection made to the ONS 15327 using a modem.	• A modem must be connected to the ONS 15327. • The modem must be provisioned for ONS 15327. To run CTC, the modem must be provisioned for Ethernet access.

4.5 CTC Window

The CTC window appears after you log into an ONS 15327 (Figure 4-2). The window includes a menu bar, a toolbar, and a top and bottom pane. The top pane provides status information about the selected objects and a graphic of the current view. The bottom pane provides tabs and subtabs to view ONS 15327 information and perform provisioning and maintenance. From this window you can display three ONS 15327 views: network, node, and card.

Figure 4-2 Node View (Default Login View)



4.5.1 Node View

Node view, shown in Figure 4-2, is the first view that appears after you log into an ONS 15327. The login node is the first node shown, and it is the home view for the session. Node view allows you to view and manage one ONS 15327 node. The status area shows the node name; IP address; session boot date and time; number of Critical (CR), Major (MJ), and Minor (MN) alarms; the name of the current logged-in user; the security level of the user; software version, and the network element default setup.

4.5.1.1 CTC Card Colors

The graphic area of the CTC window depicts the ONS 15327 shelf assembly. The colors of the cards in the graphic reflect the real-time status of the physical card and slot (Table 4-4).

Table 4-4 Node View Card and Slot Colors

Card and Slot Color	Status
Gray	Slot is not provisioned; no card is installed.
Violet	Slot is provisioned; no card is installed.
White	Slot is provisioned; a functioning card is installed.
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 4-5 lists the port colors and their service states. For more information about port service states, refer to Appendix B, "Administrative and Service States."

Table 4-5 Node View Card Port Colors and Service States

Port Color	Service State	Description
Blue	OOS-MA,LPBK	(Out-of-Service and Management, 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 (refer to Figure 4-3 and Figure 4-4). 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	OOS-MA,MT	(Out-of-Service and Management, 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 OOS-MA,MT for testing or to suppress alarms temporarily. Change the state to IS-NR, OOS-MA,DSBLD, or OOS-AU,AINS when testing is complete.
Gray	OOS-MA,DSBLD	(Out-of-Service and Management, Disabled) The port is out of service and unable to carry traffic. Loopbacks are not allowed in this service state.
Green	IS-NR	(In-Service and Normal) The port is fully operational and performing as provisioned. The port transmits a signal and displays alarms; loopbacks are not allowed.
Violet	OOS-AU,AINS	(Out-of-Service and Autonomous, Automatic In-Service) The port is out of service, but traffic is carried. Alarm reporting is suppressed. The node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR. 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 IS-NR when a signal is received for the length of time provisioned in the soak field.

Figure 4-3 Terminal Loopback Indicator

Figure 4-4 Facility Loopback Indicator

Table 4-6 lists card status indications.

Table 4-6 Node View Card Statuses

Card Status	Description
Sby	Card is in standby mode.
Act	Card is active.
NP	Card is not present.
Ldg	Card is resetting.
Mis	Card is mismatched.

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; the 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, which you can use to open, reset, or delete a card. Right-click a slot to preprovision a card slot before installing the card.

4.5.1.3 Node View Tabs

Table 4-7 lists the tabs and subtabs available in the node view.

Table 4-7 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	Displays a list of standing conditions on the node.	—
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 Node subtab displays alarms and events retrieved from a fixed-size log on the node.	Session, Node
Circuits	Creates, deletes, edits, and maps circuits.	Circuits, Rolls
Provisioning	Provisions the ONS 15327 node.	General, Ether Bridge, OSI, Network, Protection, BLSR, Security, SNMP, Comm Channels, Timing, Alarm Profiles, Defaults

Table 4-7 Node View Tabs and Subtabs (continued)

Tab	Description	Subtabs
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, or change card service state. For more information on card service states, refer to Appendix B, "Administrative and Service States."	—
Maintenance	Performs maintenance tasks for the node.	Database, Ether Bridge, OSI, Protection, BLSR, Software, Cross-Connect, Overhead XConnect, Diagnostic, Timing, Audit, Routing Table, RIP Routing Table, Test Access

4.5.2 Network View

Network view allows you to view and manage ONS 15327s that have DCC connections to the node that you logged into and to any login node groups you have selected.

Note Nodes with DCC connections to the login node will not display if you checked the Disable Network Discovery check box in the Login dialog box.

The lines show DCC connections between the nodes. DCC connections can be green (active) or gray (fail). The lines can also be solid (circuits can be routed through this link) or dashed (circuits cannot be routed through this link). Circuit provisioning uses active, routable links. Selecting a node or span in the graphic area displays information about the node and span in the status area (Table 4-8).

The graphic area displays a background image with colored ONS 15327 icons. The icon colors indicate the node status (Table 4-9).

Table 4-8 DCC Colors Indicating State in Network View

Color and Line Style	State
Green and solid	Active, Routable
Green and dashed	Active, Nonroutable
Gray and solid	Failed, Routable
Gray and dashed	Failed, Nonroutable

The color of a node in network view indicates its node alarm status. Table 4-9 lists the node colors shown in network view and the associated alarm status.

Table 4-9 Node Colors Indicating State in Network View

Color	Alarm Status
Green	No alarms
Yellow	Minor alarms
Orange	Major alarms
Red	Critical alarms
Gray with "Unknown#"	Node initializing for the first time (CTC displays Unknown# because CTC has not yet discovered the name of the node)

Table 4-10 lists the tabs and subtabs available in the network view.

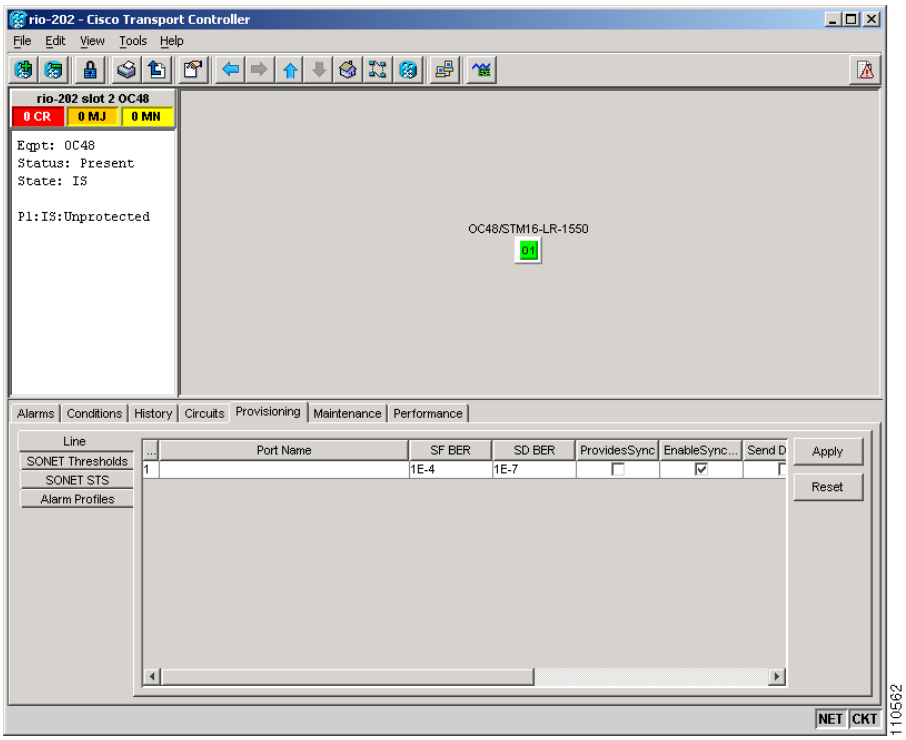
Table 4-10 Network View Tabs and Subtabs

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	Creates, deletes, edits, filters, and searches for network circuits.	Circuits, Rolls
Provisioning	Provision security, alarm profiles, bidirectional line switched rings (BLSRs), and overhead circuits.	Security, Alarm Profiles, BLSR, Overhead Circuits, Provisionable Patchcords (PPC)
Maintenance	Displays the type of equipment and the status of each node in the network; displays working and protect software versions, and allows software to be downloaded.	Software

4.5.3 Card View

Card view provides information about individual ONS 15327 cards. Use this view to perform card-specific maintenance and provisioning (Figure 4-5). A graphic showing the ports on the card appears in the graphic area. The status area provides 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), or port state (Table 4-5 on page 4-8). The information that appears and the actions you can perform depend on the card.

Figure 4-5 CTC Card View of an OC48 LR 1550 Card



Note CTC provides a card view for all ONS 15327 cards except the mechanical interface card (MIC).

Table 4-11 shows the tabs and subtabs available in card view. The subtabs, fields, and information shown under each tab depend on the card type selected.

Table 4-11 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	Creates, deletes, edits, and search circuits and rolls.	Circuits, Rolls

Table 4-11 Card View Tabs and Subtabs (continued)

Tab	Description	Subtabs
Provisioning	Provisions an ONS 15327 card.	XTC cards: DS1 (subtabs include Line, Line Thresholds, Elect Path Thresholds, and SONET Thresholds); DS3 (subtabs include Line, Line Thresholds, and SONET Thresholds); External Alarms; External Controls; Alarm Profiles OC-N cards: Line, SONET Thresholds, SONET STS, and Alarm Profiles E-Series and G-Series cards (subtabs depend on the card type): Ether Port, Ether VLAN, Ether Card, Ether Thresholds, RMON Thresholds, Alarm Profiles
Maintenance	Performs maintenance tasks for the card.	XTC cards: DS1 (subtabs include Loopback, Protection, AINS Soak, Path Trace); DS3 (subtabs include Loopback, Protection, AINS Soak); External Alarms; External Controls; Virtual Wires OC-N cards: Loopback, Info, Protection, AINS Soak, J1 Path Trace (options depend on the card type) G-Series cards: Path Trace, Loopback, Bandwidth
Performance	Performs performance monitoring for the card.	XTC cards: DS1, DS3 E-Series and G-Series cards (subtabs depend on the card type): Port, RMON Thresholds, Alarm Profiles

4.6 Print and Export CTC Data

In the card-, node-, or network-level CTC view, choose File > Print to print CTC information in graphical or tabular form on a Windows-provisioned printer. Choose File > Export to export card, node, or network information as editable delineated text files to other applications. Printing and exporting data are useful for record keeping or troubleshooting purposes.

Print card, node, or network CTC information in graphical or tabular form on a Windows-provisioned printer, or export card, node, or network information as editable delineated text files to other applications. This feature is useful for viewing the node inventory, circuit routing, or alarm data in network record-keeping and troubleshooting.

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 CTC data in table format without graphical representations of shelves, cards, or tabs. This option applies to all windows except:
  - Provisioning > General window
  - Provisioning > Network > General and RIP windows
  - Provisioning > Security > Policy, Access, and Legal Disclaimer windows
  - Provisioning > SNMP window
  - Provisioning > Timing window
  - Maintenance > Database window
  - Maintenance > Diagnostic window
  - Maintenance > Protection window
  - Maintenance > Timing > Source window

  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.

Note The above items are not available for the Export option.

4.7 XTC Card Reset

You can reset the ONS 15327 XTC card using CTC (a soft reset) or by physically reseating the XTC card (a hard reset). A soft reset reboots the XTC card and reloads the operating system and the application software. Additionally, a hard reset temporarily removes power from the XTC card and clears all buffer memory.

If you need perform a hard reset an active XTC card, put the XTC card into standby mode first by performing a soft reset using CTC.

4.8 XTC Card Database

When dual XTC cards are installed in the ONS 15327, each XTC card hosts a separate database; therefore, the protect card database is available if the database on the working XTC fails. You can also store a backup version of the database on the workstation running CTC. This operation should be part of a regular ONS 15327 maintenance program performed at approximately weekly intervals, and should also be completed when preparing an ONS 15327 for a pending natural disaster, such as a flood or fire.

Note The following parameters are not backed up and restored: node name, IP address, mask and gateway, and Internet Inter-ORB Protocol (IIOP) port. If you change the node name and then restore a backed up database with a different node name, the circuits will map to the new node name. Cisco recommends keeping a record of the old and new node names.

4.9 Software Revert

When you click the Activate button after a software upgrade, the XTC copies the current working database and saves it in a reserved location in the XTC flash memory. If you later need to revert to the original working software load from the protect software load, the saved database installs automatically. You do not need to restore the database manually or recreate circuits.

The revert feature is useful if a maintenance window closes while you are upgrading CTC software. You can revert to the standby software load without losing traffic. When the next maintenance window opens, complete the upgrade and activate the new software load.

Circuits that were created and provisioning that was performed after a software load is activated (upgraded to a higher release) will be lost with a revert. The database configuration at the time of activation is reinstated after a revert. This does not apply to maintenance reverts (for example 4.6.2 to 4.6.1), because maintenance releases use the same database.

To perform a supported (non-service-affecting) revert from Software R6.0, the release you want to revert to must have been working at the time you first activated Software R6.0 on that node. Because a supported revert automatically restores the node configuration at the time of the previous activation, any configuration changes made after activation will be lost when you revert the software. Downloading Release 6.0 a second time after you have activated the new load ensures that no actual revert to a previous load can take place (the TCC2/TCC2P cards will reset, but the download will not be traffic affecting and will not change your database).

Security

This chapter provides information about Cisco ONS 15327 user security. To provision security, refer to the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

5.1 Users IDs and Security

The CISCO15 ID is provided with the ONS 15327 system, but this user ID is not prompted when you sign into CTC. This ID can be used to set up other ONS 15327 users. (To do this, complete the "Create Users and Assign Security" procedure in the *Cisco ONS 15327 Procedure Guide*.)

You can have up to 500 user IDs on one ONS 15327. Each Cisco Transport Controller (CTC) or TL1 user can be assigned one of the following security levels:

- Retrieve—Users can retrieve and view CTC information but cannot set or modify parameters.
- Maintenance—Users can access only the ONS 15327 maintenance options.
- Provisioning—Users can access provisioning and maintenance options.
- Superusers—Users can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users.

See Table 5-3 on page 5-5 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 CTC Action

Table 5-1 shows the actions that each user privilege level can perform in node view.

Table 5-1 ONS 15327 Security Levels—Node View

CTC Tab	Subtab	[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
	Node	Retrieve/Filter	X	X	X	X
Circuits	Circuits	Create/Edit/Delete	—	—	X	X
		Filter/Search	X	X	X	X
	Rolls	Create/Edit/Delete	—	—	X	X
		Filter/Search	X	X	X	X
Provisioning	General	General: Edit	—	—	Partial[1]	X
		Power Monitor: Edit	—	—	X	X
	EtherBridge	Spanning trees: Edit	—	—	X	X
	Network	General: All	—	—	—	X
		Static Routing: Create/Edit/ Delete	—	—	X	X
		OSPF: Create/Edit/Delete	—	—	X	X
		RIP: Create/Edit/Delete	—	—	X	X
		Proxy: Create/Edit/Delete	—	—	—	X
		Firewall: Create/Edit/Delete	—	—	—	X
	OSI	Main Setup	—	—	—	X
		TARP	—	—	—	X
		Routers	—	—	—	X
		GRE Tunnel Routes	—	—	—	X
	Protection	Create/Delete/Edit	—	—	X	X
		View	X	X	X	X
	BLSR	All	—	—	X	X
	Security	Users: Create/Delete/Clear Security Intrusion	—	—	—	X
		Users: Change password	Same user	Same user	Same user	All users
		Active Logins: View/Logout	—	—	—	X
		Policy: Edit	—	—	—	X
		Access: Edit	—	—	—	X
		RADIUS Server	—	—	—	X
		Legal Disclaimer: Edit	—	—	—	X

Table 5-1 ONS 15327 Security Levels—Node View (continued)

CTC Tab	Subtab	[Subtab]: Actions	Retrieve	Maintenance	Provisioning	Superuser
Provisioning (cont.)	SNMP	Trap destinations/Selected Destination: Create/Edit/Delete	—	—	X	X
		Trap destinations/Selected Destination: View	X	X	X	X
	Comm Channels	SDCC/PPC: Create/Edit/Delete	—	—	X	X
	Timing	General/BITS Facilities: Edit	—	—	X	X
	Alarm Profiles	Alarm Behavior: Edit	—	—	X	X
		Alarm Profile Editor: Store/Delete[2]	—	—	X	X
		Alarm Profile Editor: New/Load/Compare/Available/ Usage	X	X	X	X
	Defaults	Edit/Import	—	—	—	X
		Export	X	X	X	X
Inventory	—	Delete	—	—	X	X
		Reset	—	X	X	X

Table 5-1 ONS 15327 Security Levels—Node View (continued)

CTC Tab	Subtab	[Subtab]: Actions	Retrieve	Maintenance	Provisioning	Superuser
Maintenance	Database	Backup	—	X	X	X
		Restore	—	—	—	X
	EtherBridge	Spanning Trees: View	X	X	X	X
		MAC Table: Retrieve	X	X	X	X
		MAC Table: Clear/Clear All	—	X	X	X
		Trunk Utilization: Refresh	X	X	X	X
		Circuits: Refresh	X	X	X	X
	OSI	IS-IS RIB	—	—	—	X
		ES-IS RIB	—	—	—	X
		TDC	—	—	—	X
	Protection	Switch/Lock out/Lockon/Clear/ Unlock	—	X	X	X
	BLSR	West/East Switches	—	X	X	X
	Software	Download	—	X	X	X
		Activate/Revert	—	—	—	X
	Cross-Connect	Resource Usage: Delete/Refresh	—	—	X	X
	Overhead XConnect	View	X	X	X	X
	Diagnostic	Retrieve/Lamp Test	—	X	X	X
	Timing	Source: Edit	—	X	X	X
		Report: View/Refresh	X	X	X	X
	Audit	Retrieve	—	—	—	X
		Archive	—	—	X	X
	Routing Table	Retrieve	X	X	X	X
	RIP Routing Table	Retrieve	X	X	X	X
	Test Access	Read-only	X	X	X	X

1. Provisioner user cannot change node name, contact, location, or AIS-V insertion on STS-1 signal degrade (SD) 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 15327 Security Levels—Network View

CTC Tab	Subtab	[Subtab]: Actions	Retrieve	Maintenance	Provisioning	Superuser
Alarms	—	Synchronize/Filter/Delete cleared alarms	X	X	X	X
Conditions	—	Retrieve/Filter	X	X	X	X

Table 5-2 ONS 15327 Security Levels—Network View (continued)

CTC Tab	Subtab	[Subtab]: Actions	Retrieve	Maintenance	Provisioning	Superuser
History	—	Filter	X	X	X	X
Circuits	Circuits	Create/Edit/Delete	—	—	X	X
		Filter/Search	X	X	X	X
	Rolls	Create/Edit/Delete	—	—	X	X
		Filter/Search	X	X	X	X
Provisioning	Security	Users: Create/Delete	—	—	—	X
		Users: Change	Same User	Same User	Same User	All Users
		Active Logins: Logout	—	—	—	X
		Policy: Change	—	—	—	X
	Alarm Profiles	Store/Delete[1]	—	—	X	X
		New/Load/Compare/Available/ Usage	—	X	X	X
	BLSR	Create/Delete/Edit/Upgrade	—	—	X	X
	Overhead Circuits	Create/Delete/Edit/Merge	—	—	X	X
		Search	X	X	X	X
	Provisionable Patchcords (PPC)	Create/ Delete	—	—	X	X
Maintenance	Software	Download/Cancel	—	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 privilege can provision security policies on the ONS 15327. These security policies include idle user timeouts, password changes, password aging, and user lockout parameters. In addition, a Superuser can access the ONS 15327 through the XTC RJ-45 port.

5.2.2.1 Idle User Timeout

Each ONS 15327 CTC or TL1 user can be idle during his or her login session for a specified amount of time before the CTC window is locked. Timed-out users must re-enter their password to access the CTC session. The lockouts prevent unauthorized users from making changes. Higher-level users have shorter default idle periods and lower-level users have longer or unlimited default idle periods, as shown in Table 5-3. The user idle period can be modified by a Superuser; refer to the *Cisco ONS 15327 Procedure Guide* for instructions.

Table 5-3 ONS 15327 Default User Idle Times

Security Level	Idle Time
Superuser	15 minutes
Provisioning	30 minutes

Table 5-3 ONS 15327 Default User Idle Times (continued)

Security Level	Idle Time
Maintenance	60 minutes
Retrieve	Unlimited

5.2.2.2 User Password, Login, and Access Policies

Superusers can view real-time lists of users who are logged into CTC or TL1 user logins by node. Superusers can also provision the following password, login, and node access policies.

- Password expirations and reuse—Superusers can specify when users must change and when they can reuse their passwords.
- Login attempts and Locking out users—Superusers can specify the maximum number of invalid login attempts that a user is allowed before they are locked out of CTC.
- Disabling users—Superusers can provision the length of time before inactive users are disabled.
- Node access and user sessions—Superusers can limit the number of CTC sessions one user can have, and they can prohibit access to the ONS 15327 using the XTC RJ-45 LAN connection.

  In addition, a Superuser can select secure shell (SSH) instead of Telnet at the CTC Provisioning > Security > Access tabs. SSH is a terminal-remote host Internet protocol that uses encrypted links. It provides authentication and secure communication over unsecure channels. Port 22 is the default port and cannot be changed.

5.3 Audit Trail

The ONS 15327 XTC maintains a GR-839-CORE.-compliant, 640-entry, human-readable audit trail of user or system actions such as login, logout, circuit creation or deletion, and user- or system-generated actions. 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. The log includes authorized Cisco logins and logouts using the operating system command line interface, CTC, and TL1; the log also includes FTP actions, circuit creation/deletion, and user/system generated actions. You can move the log to a local or network drive for later review.

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.

To view the Audit Trail log, refer to *Cisco ONS 15327 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.

5.3.1 Audit Trail Log Entries

Table 5-4 contains the columns listed in Audit Trail window.

Table 5-4 Audit Trail Window Columns

Heading	Explanation
Date	Date when the action occurred
Num	Incrementing count of actions
User	User ID that initiated the action
P/F	Pass/Fail (whether or not the action was executed)
Operation	Action that was taken

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—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 15327 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 15327 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 15327 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 16 characters long.
- You can use any standard alphanumeric and special characters.
- You can use a shared secret of up to 16 characters in length. To protect your server and your RADIUS clients from brute force attacks, use long shared secrets.
- 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 5-5.

Table 5-5 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.

Timing

This chapter provides information about Cisco ONS 15327 SONET timing. To provision timing, refer to the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

6.1 Timing Parameters

SONET timing parameters must be set for each ONS 15327. Each ONS 15327 independently accepts its timing reference from one of three sources:

- The building integrated timing supply (BITS) pins on the ONS 15327 Mechanical Interface card (MIC).
- An OC-N card installed in the ONS 15327. The card is connected to a node that receives timing through a BITS source.
- The internal ST3 clock on the XTC card.

You can set ONS 15327 timing to one of three modes: external, line, or mixed. If timing is coming from the BITS port, set ONS 15327 timing to external. If the timing comes from an OC-N card, set the timing to line. Typical ONS 15327 networks have the following timing configurations:

- One node is set to external. The external node derives its timing from a BITS source wired to the BITS MIC port. The BITS source derives its timing from a primary reference source (PRS) such as a Stratum 1 clock or global positioning satellite (GPS) signal.
- The other nodes are set to line. The line nodes derive timing from the externally timed node through the OC-N trunk (span) cards.

You can set three timing references for each ONS 15327. The first two references are typically two BITS-level sources, or two line-level sources optically connected to a node with a BITS source. The third reference is usually assigned to the internal clock provided on every ONS 15327 XTC card. However, if you assign all three references to other timing sources, the internal clock is always available as a backup timing reference. The internal clock is a Stratum 3 (ST3), so if an ONS 15327 node becomes isolated, timing is maintained at the ST3 level.

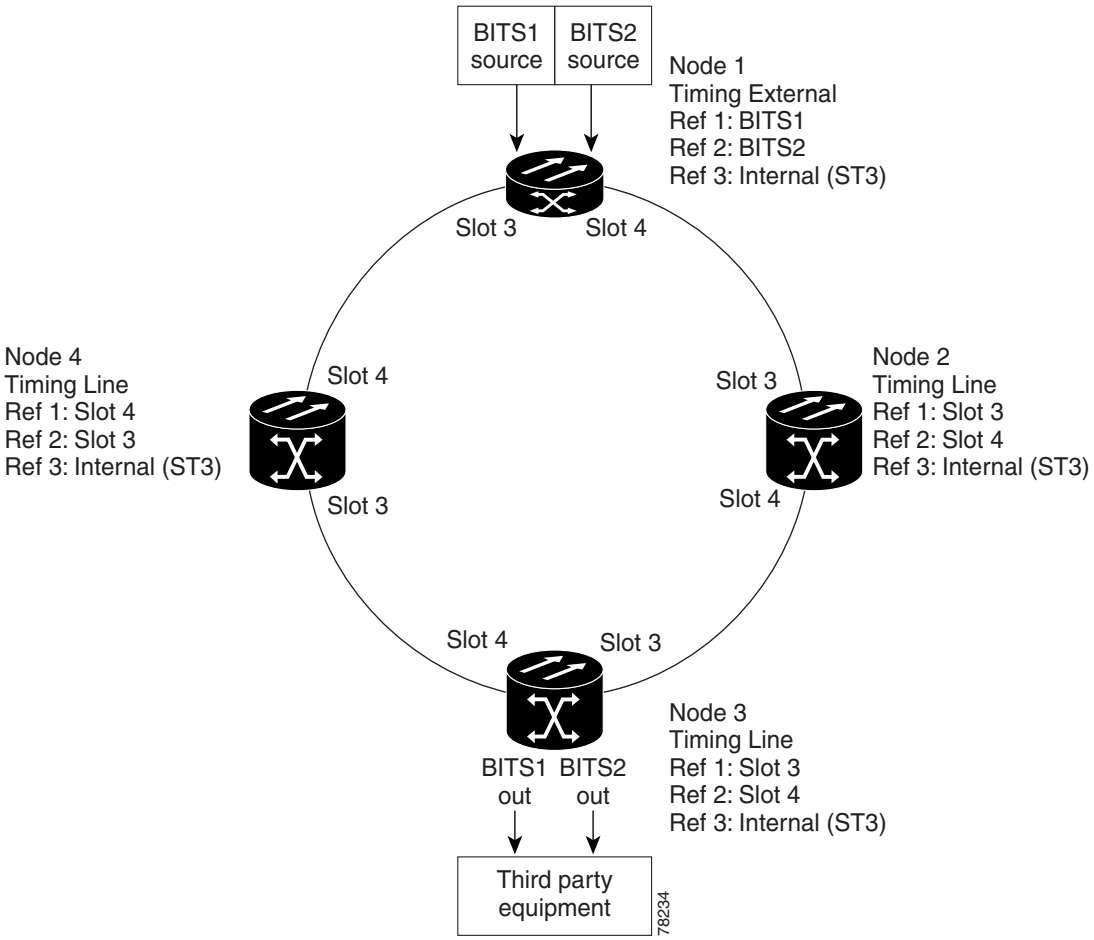
The CTC Maintenance > Timing > Report tabs show current timing information for an ONS 15327, including the timing mode, clock state and status, switch type, and reference data.

Caution Mixed timing allows you to select both external and line timing sources. However, Cisco does not recommend its use because it can create timing loops. Use mixed timing mode with caution.

6.2 Network Timing

Figure 6-1 shows an example of an ONS 15327 network timing setup. Node 1 is set to external timing. Two references are set to BITS, and the third reference is set to internal. The BITS output pins on the MIC cards of Node 3 provide timing to outside equipment, such as a digital access line access multiplexer.

Figure 6-1 ONS 15327 Timing Example



6.3 Synchronization Status Messaging

Synchronization status messaging (SSM) is a SONET protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SONET line layer. They enable SONET devices to automatically select the highest quality timing reference and to avoid timing loops.

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 SSM for the ONS 15327, consult your timing reference documentation to determine which message set to use. Table 6-1 and Table 6-2 show the Generation 1 and Generation 2 message sets.

Table 6-1 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 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

Circuits and Tunnels

This chapter explains Cisco ONS 15327 synchronous transport signal (STS) and Virtual Tributary (VT) circuits, and VT and data communications channel (DCC) tunnels. To provision circuits and tunnels, refer to the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

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.

7.1 Circuit Properties

On the ONS 15327 you can create unidirectional and bidirectional circuits. For path protection circuits, you can create revertive or nonrevertive circuits. Circuits are routed automatically or you can manually route them. With the autorange feature, you do not need to build multiple circuits of the same type individually; the Cisco Transport Controller (CTC) can create additional sequential circuits if you specify the number of circuits you need and build the first circuit.

You can provision circuits either before or after cards are installed if the ONS 15327 slots are provisioned for the card that carries the circuit. However, circuits do not carry traffic until the cards are installed and the ports are In-Service and Normal (IS-NR); Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS); or Out-of-Service and Management, Maintenance (OOS-MA,MT).

The ONS 15327 Circuits window, which appears in network, node, and card view, is where you can view information about circuits. The Circuits window shows the following information:

- Name—The name of the circuit. The circuit name can be manually assigned or automatically generated.
- Type—The circuit types are: STS (STS circuit), VT (VT circuit), VTT (VT tunnel), or VAP (VT aggregation point).
- Size—The circuit size. VT circuits are 1.5. ONS 15327 STS circuit sizes are 1, 3c, 6c, 9c, 12c, 24c, or 48c.
- Protection—The type of circuit protection. See the "7.1.3 Circuit Protection Types" section on page 7-5.
- Direction—The circuit direction, either two-way or one-way.
- Status—The circuit status. See the "7.1.1 Circuit Status" section on page 7-2.
- Source—The circuit source in the format: *node/slot/port "port name"/STS/VT*. (Port name appears in quotes.) Node and slot always appear; *port "port name"/STS/VT* might appear, depending on the source card, circuit type, and whether a name is assigned to the port. If the circuit size is a concatenated size (3c, 6c, 12c, etc.), STSs used in the circuit are indicated by an ellipsis, for example, S7..9, (STSs 7, 8, and 9) or S10..12 (STSs 10, 11, and 12). If the source is located on an XTC card, *port* specifies DS1 or DS3; each STS on the XTC card is numbered 1.
- Destination—The circuit destination in same format (*node/slot/port "port name"/STS/VT*) as the circuit source.
- # of VLANS—The number of VLANs used by an Ethernet circuit.
- # of Spans—The number of internode links that constitute the circuit. Right-clicking the column opens a shortcut menu from which you can choose to show or hide circuit span detail.
- State—The circuit state. See the "7.1.2 Circuit States" section on page 7-3.

7.1.1 Circuit Status

The circuit statuses that appear in the Circuit window Status column are generated by CTC based on conditions along the circuit path. Table 7-1 shows the statuses that can appear in the Status column.

Table 7-1 ONS 15327 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.

Table 7-1 ONS 15327 Circuit Status (continued)

Status	Definition/Activity
PARTIAL	A CTC-created circuit is missing a cross-connect or network span or a complete path from source to destinations does not exist. In CTC, circuits are represented using cross-connects and network spans. If a network span is missing from a circuit, the circuit status is PARTIAL. However, a PARTIAL status does not necessarily mean a circuit traffic failure has occurred, because traffic may flow on a protect path. Network spans are in one of two states: up or down. On CTC circuit and network maps, up spans appear as green lines, and down spans appear as gray lines. If a failure occurs on a network span during a CTC session, the span remains on the network map but its color changes to gray to indicate that the span is down. If you restart your CTC session while the failure is active, the new CTC session cannot discover the span and its span line does not appear on the network map. Subsequently, circuits routed on a network span that goes down appear as DISCOVERED during the current CTC session, but appear as PARTIAL to users who log in after the span failure.
DISCOVERED_TL1	A TL1-created circuit or a TL1-like, CTC-created circuit is complete. A complete path from source to destinations exists.
PARTIAL_TL1	A TL1-created circuit or a TL1-like, CTC-created circuit is missing a cross-connect or circuit span (network link), and a complete path from source to destinations does not exist.
CONVERSION_PENDING	An existing circuit in a topology upgrade is set to this state. The circuit returns to the DISCOVERED status once the topology upgrade is complete. For more information about topology upgrades, see Chapter 8, “SONET Topologies and Upgrades.”
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, “SONET Topologies and Upgrades.”
DROP_PENDING	A circuit is set to this status when a new circuit drop is being added.

7.1.2 Circuit States

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

- If all cross-connects in a circuit are in the IS-NR service state, the circuit service state is In-Service (IS).

- If all cross-connects in a circuit are in an OOS service state, such as OOS-MA,MT; Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS); or Out-of-Service and Management, Disabled (OOS-MA,DSBLD), the circuit service state is Out-of-Service (OOS).
- PARTIAL is appended to the OOS circuit service state when circuit cross-connects state are mixed and not all in IS-NR. The OOS-PARTIAL state can occur during automatic or manual transitions between states. OOS-PARTIAL 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 15327 Troubleshooting Guide* for troubleshooting procedures.

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 on the Edit Circuit window State tab or from the Tools > Circuits > Set Circuit State menu.

During circuit creation, you can apply a service state to the drop ports in a circuit; however, CTC does not apply a requested state other than IS-NR to drop ports if:

- The port is a timing source.
- The port is provisioned for orderwire or tunnel orderwire.
- The port is provisioned as a DCC or DCC tunnel.
- The port supports 1+1 protection or a bidirectional line switched ring (BLSR).

Circuits do not use the soak timer, but ports do. The soak period is the amount of time that the port remains in the OOS-AU,AINS service state after a signal is continuously received. When the cross-connects in a circuit are in the OOS-AU,AINS service state, the ONS 15327 monitors the cross-connects for an error-free signal. It changes the state of the circuit from OOS to IS or to OOS-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. Two common examples of state changes that you see when provisioning circuits using CTC are:

- When assigning the IS,AINS administrative state to cross-connects in VT1.5 circuits and VT tunnels, the source and destination ports on the VT1.5 circuits remain in the OOS-AU,AINS service state until an alarm-free signal is received for the duration of the soak timer. When the soak timer expires and an alarm-free signal is found, the VT1.5 source port and destination port service states change to IS-NR and the circuit service state becomes IS.
- When assigning the IS,AINS administrative state to cross-connects in STS circuits, the circuit source and destination ports transition to the OOS-AU,AINS service state. When an alarm-free signal is received, the source and destination ports remain OOS-AU,AINS for the duration of the soak timer. After the port soak timer expires, STS source and destination ports change to IS-NR and the circuit service state to IS.

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 OOS-AU,AINS service state and has a good signal, the Time Until IS column shows the soak count down status. If the port is OOS-AU,AINS 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 port and cross-connect service states, see the"Administrative and Service States"appendix.

7.1.3 Circuit Protection Types

The Protection column in the Circuit window shows the card (line) and SONET topology (path) protection used for the entire circuit path. Table 7-2 shows the protection type indicators that you see in this column.

Table 7-2 Circuit Protection Types

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

7.1.4 Edit Circuits Window

Use the Edit Circuits window to view general circuit information, create monitor circuits, change a circuit state, and merge circuits. For path protection circuits, use the Edit Circuits window to change path protection selectors and switch protection paths.

In the UPSR Selectors subtab on the Edit Circuits window, you can:

- View the path protection circuit's working and protection paths.
- Edit the reversion time.
- Set the hold-off timer.
- Edit the signal fail (SF)/signal degrade (SD) bit error rate (BER) thresholds.
- Change path payload defect indication (PDI-P) settings.

Note In the UPSR Selectors tab, the SF Ber Level and SD Ber Level columns display "N/A" for those nodes that do not support VT signal BER monitoring. In Software Release 6.0, only the Cisco ONS 15310-CL supports VT signal BER monitoring.

In the UPSR Switch Counts subtab, you can:

- Perform maintenance switches on the circuit selector.
- View switch counts for the selectors.

Using the Edit Circuits window you can view a detailed circuit map by checking Show Detailed Map. The detailed map allows you to view information about ONS 15327 circuits graphically. Routing information that appears includes:

- Circuit direction (unidirectional/bidirectional)
- The nodes, STSs, and VTs through which circuit passes including slots and port numbers
- The circuit source and destination points
- Open Shortest Path First (OSPF) area IDs
- Link protection (path protection, unprotected, BLSR, 1+1 protection) and bandwidth (OC-N)

For BLSRs, the detailed map shows the number of BLSR fibers and the BLSR ring ID. For path protection configurations, the map shows the active and standby paths from circuit source to destination, and it also shows the working and protect paths.

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 selectors states

By default, the working path on the detailed circuit map 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. Port states are indicated by colors, shown in Table 7-3.

Table 7-3 Port State Color Indicators

Port Color	State
Green	IS-NR
Gray	OOS-MA,DSBLD
Purple	OOS-AU,AINS
Light blue	OOS-MA,MT

Notation within or by the squares or selector pentagons on each node indicate switches and other conditions. For example:

- F = Force switch
- M = Manual switch
- L = Lockout switch
- T = Terminal loopback
- Arrow = Facility 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 a path protection span to change the state of the path selectors in the path protection circuit.

7.2 VT1.5 Bandwidth

The ONS 15327 XTC card performs port-to-port, time-division multiplexing (TDM). Because VT1.5 multiplexing is STS-based, understanding how VT1.5 circuits use the XTC VT matrix resources is necessary to avoid unexpected depletion of the VT matrix capacity. The key VT matrix principles are as follows:

- The VT matrix has 24 logical STS ports. All VT1.5 multiplexing is achieved through these logical STS ports.
- Each VT matrix STS port has capacity for 28 VT1.5s. Therefore, the VT matrix has a capacity for 672 VT1.5 terminations.
- Because each logical STS termination on the VT matrix can carry 28 VT1.5s, the VT matrix capacity is 672 VT 1.5s (24 times 28).

The XTC card can map up to 24 STSs for VT1.5 traffic. Because one STS can carry 28 VT1.5s, the XTC card can terminate up to 672 VT1.5s or 336 VT1.5 cross-connects. However, to terminate 336 VT1.5 cross-connects:

- Each STS mapped for VT1.5 traffic must carry 28 VT1.5 circuits. If you assign each VT1.5 circuit to a different STS, the XTC card VT1.5 cross-connect capacity is reached after you create 12 VT1.5 circuits.
- ONS 15327s must be in a BLSR. Source and drop nodes in path protection have capacity for only 224 VT1.5 cross-connects because an additional VT is used for the protect path.

7.3 VT Tunnels and Aggregation Points

To maximize XTC VT1.5 cross-connect resources, you can tunnel VT1.5 circuits through ONS 15327 nodes. VT1.5 tunnels do not use VT matrix capacity at ONS 15327 pass-through nodes, thereby freeing the XTC card cross-connect resources for other VT1.5 circuits.

VAPs allow you to provision BLSR circuits from multiple VT1.5 sources to a single STS destination. Like circuits, a VAP has a source and a destination. The source is the STS grooming end, the node where the VT1.5 circuits are aggregated into a single STS. The VAP STS must be a port on an OC-N card. VT matrix resources are not used on the VAP source node, which is the key advantage of VAPs. The VAP destination is the node where the VT1.5 circuits originate. Circuits can originate on any ONS 15327 card.

7.4 DCC Tunnels

SONET provides four DCCs for network element (NE) operations, administration, maintenance, and provisioning (OAM&P): one on the SONET Section layer (DCC1) and three on the SONET Line layer (DCC2, DCC3, DCC4). The ONS 15327 uses the Section DCC for ONS 15327 management and provisioning. When multiple DCC channels exist between two neighboring nodes, the ONS 15327 balances traffic over the existing DCC channels using a load balancing algorithm. This algorithm chooses a DCC for packet transport by considering packet size and DCC utilization.

You can use the three Line DCCs (LDCCs) and the Section DCC (SDCC), when not used for ONS 15327 DCC terminations, to tunnel third-party SONET equipment across ONS 15327 networks. A DCC tunnel endpoint is defined by Slot, Port, and DCC, where DCC can be either the SDCC or one of the LDCCs. You can link an SDCC to an LDCC and an LDCC to an SDCC. You can also link LDCCs to LDCCs and link SDCCs to SDCCs. To create a DCC tunnel, you connect the tunnel endpoints from one ONS 15327 optical port to another.

Table 7-4 shows the DCC tunnels that you can create.

Table 7-4 DCC Tunnels

DCC	SONET Layer	SONET Bytes	OC-3, OC-12, OC-48
DCC1	Section	D1 to D3	Yes
DCC2	Line	D4 to D6	Yes
DCC3	Line	D7 to D9	Yes
DCC4	Line	D10 to D12	Yes

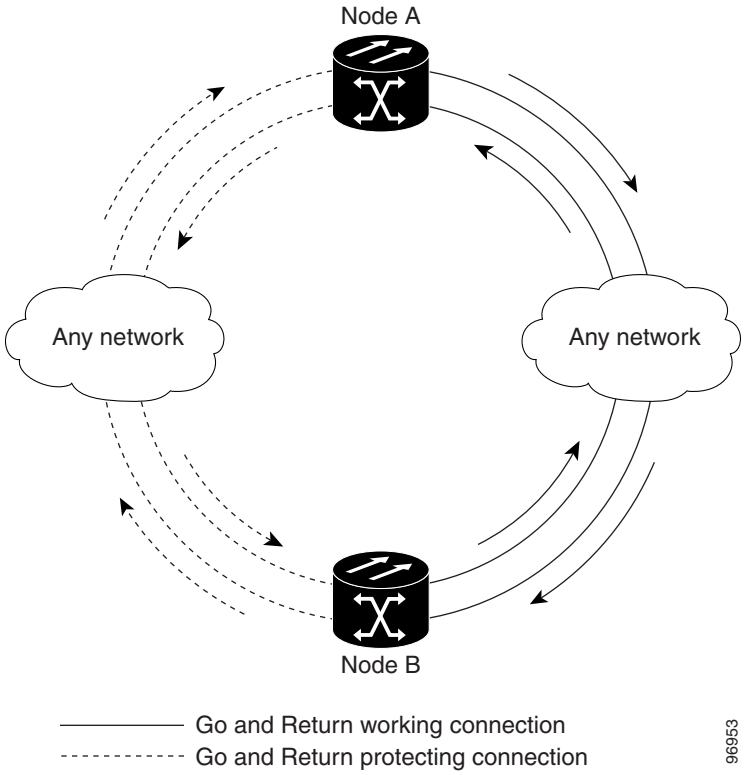
When you create DCC tunnels, keep the following guidelines in mind:

- Each ONS 15327 can have up to 32 DCC tunnel connections.
- Each ONS 15327 can have up to 10 SDCC terminations.
- An SDCC that is terminated cannot be used as a DCC tunnel endpoint, and an SDCC that is used as a DCC tunnel endpoint cannot be terminated.
- All DCC tunnel connections are bidirectional.

7.5 Go-and-Return Path Protection Routing

The go-and-return path protection routing option allows you to route the path protection working path on one fiber pair and the protect path on a separate fiber pair (Figure 7-1). The working path will always be the shortest path. If a fault occurs, both the working and protection fibers are not affected. This feature only applies to bidirectional path protection circuits. The go-and-return routing option appears on the Circuit Attributes page of the Circuit Creation wizard.

Figure 7-1 Path Protection Go-and-Return Routing



7.6 BLSR Protection Channel Access Circuits

You can provision circuits to carry traffic on BLSR PCA circuits when conditions are fault-free. Traffic routed on BLSR PCA circuits, called extra traffic, has lower priority than the traffic on the working channels and is unprotected. During ring or span switches, PCA circuits are preempted and squelched. For example, in an OC-48 BLSR, STSs 25 to 48 can carry extra traffic when no ring switches are active, but PCA circuits on these STSs are preempted when a ring switch occurs. When the conditions that caused the ring switch are remedied and the ring switch is removed, PCA circuits are restored. If the BLSR is provisioned as revertive, this occurs automatically after the fault conditions are cleared and the reversion timer has expired.

Traffic provisioning on BLSR PCA circuits is performed during circuit provisioning. The Protection Channel Access check box appears whenever Fully Protected Path is unchecked on the Circuit Creation wizard. Refer to the *Cisco ONS 15327 Procedure Guide* for more information.

7.7 Path Trace

The SONET J1 Path Trace is a repeated, fixed-length string comprised of 64 consecutive J1 bytes. You can use the string to monitor interruptions or changes to circuit traffic. Table 7-5 shows the ONS 15327 cards that support path trace.

Table 7-5 ONS 15327 Cards Capable of Path Trace

J1 Function	Cards
Transmit and receive	XTC (DS-1) G1000-2
Receive only	OC3 IR 4 1310 OC12 IR 1310 OC12 LR 1550 OC48-1-IR OC48 LR 1550

The J1 path trace transmits a repeated, fixed-length string. If the string received at a circuit drop port does not match the string the port expects to receive, an alarm is raised. Two path trace modes are available:

- 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.

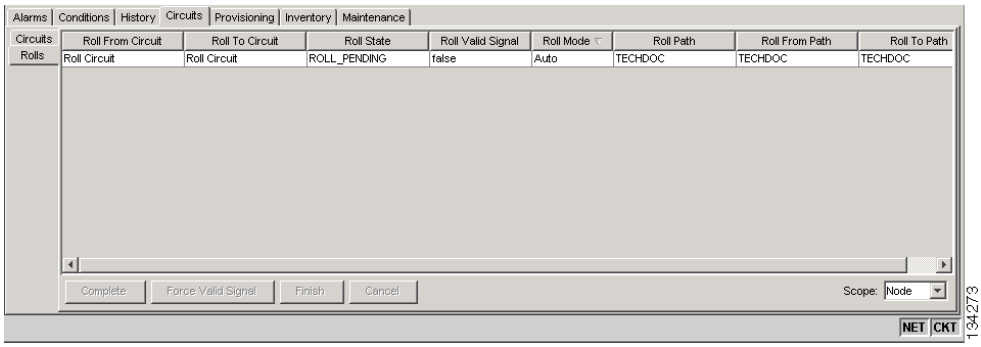
7.8 Bridge and Roll

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, ONS 15454, ONS 15454 SDH, ONS 15327, and ONS 15310-CL.

7.8.1 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 7-2 shows the Rolls window.

Figure 7-2 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 "7.8.2 Roll Status" section on page 7-12 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 when 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.

7.8.2 Roll Status

Table 7-6 lists the roll statuses. You can only reroute circuits that have a DISCOVERED status. (See Table 7-1 on page 7-2 for a list of circuit statuses.) You cannot reroute circuits that are in the ROLL_PENDING status.

Table 7-6 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.

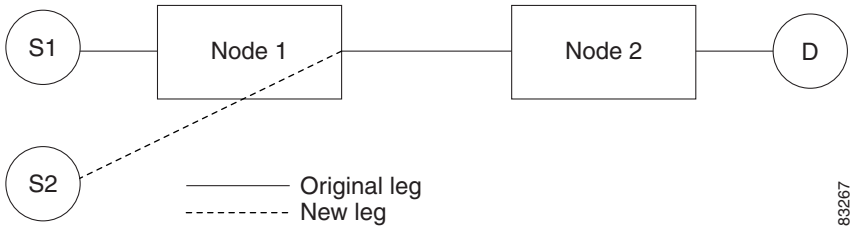
7.8.3 Single and Dual Rolls

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 7-3 and Figure 7-4, respectively).
- Roll a segment of the circuit onto another chosen circuit (Figure 7-5 on page 7-13). This roll also results in a new destination or a new source.

In Figure 7-3, you can select any available STS on Node 1 for a new source.

Figure 7-3 Single Source Roll



In Figure 7-4, you can select any available STS on Node 2 for a new destination.

Figure 7-4 Single Destination Roll

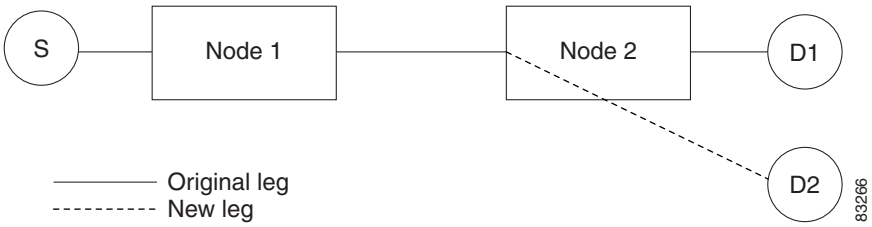


Figure 7-5 shows one circuit rolling onto another circuit at the destination. The new circuit has cross-connects on Node 1, Node 3, and Node 4. CTC deletes the cross-connect on Node 2 after the roll.

Figure 7-5 Single Roll from One Circuit to Another Circuit (Destination Changes)

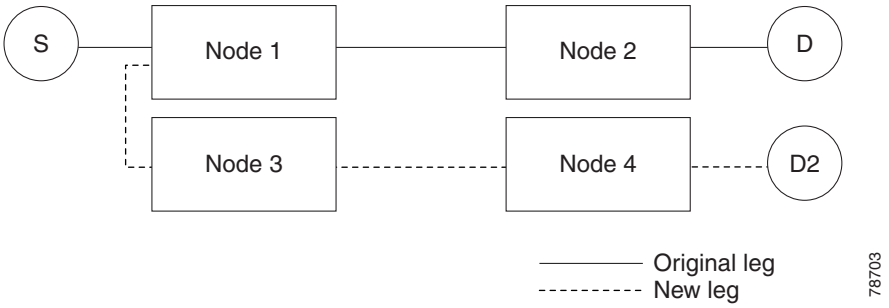
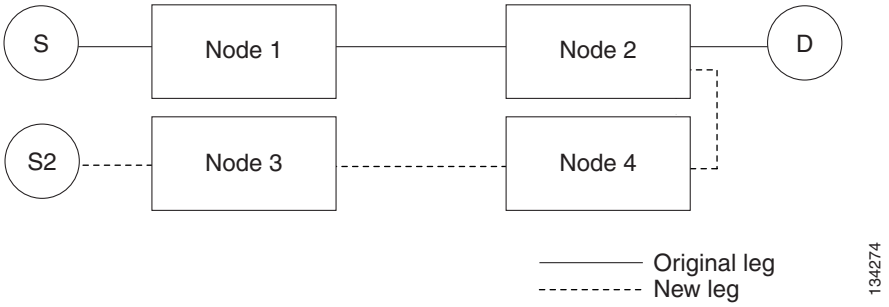


Figure 7-6 shows one circuit rolling onto another circuit at the source.

Figure 7-6 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.

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

Figure 7-7 Dual Roll to Reroute a Link

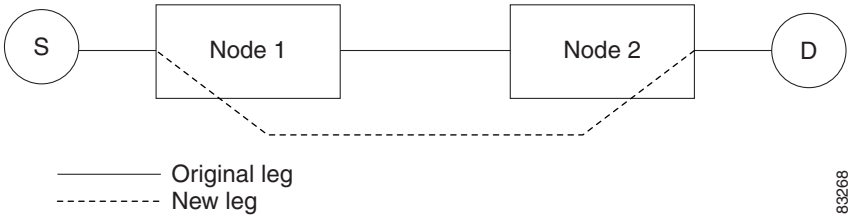
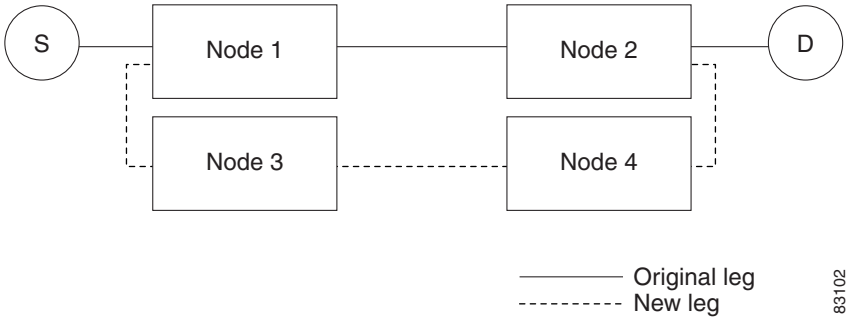


Figure 7-8 illustrates a dual roll involving two circuits.

Figure 7-8 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.

7.8.4 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.

7.8.5 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 a path protection circuit. When using bridge and roll on path protection circuits, you can roll the source or destination or both path selectors in a dual roll. However, you cannot roll a single path selector.

7.9 Merge Circuits

A circuit merge combines a single selected circuit with one or more circuits. You can merge VT tunnels, VAP circuits, user data channel (UDC) overhead circuits, CTC-created traffic circuits, and TL1-created traffic circuits. To merge circuits, you choose a circuit on the CTC Circuits window and the circuits that you want to merge with the chosen (master) circuit on the Merge tab in the Edit Circuits 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. For example, you can combine an STS circuit with a VAP circuit to create a longer VAP circuit, but you cannot combine a VT circuit with an STS circuit.
- 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.
- VLAN assignments 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 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.

7.10 Reconfigure Circuits

You can reconfigure multiple circuits, which is typically necessary when a large number of circuits are in the PARTIAL status. When reconfiguring multiple circuits, the selected circuits can be any combination of DISCOVERED, PARTIAL, DISCOVERED_TL1, or PARTIAL_TL1 circuits. You can reconfigure tunnels, VAP circuits, VLAN-assigned circuits, CTC-created circuits, and TL1-created circuits.

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 merge and others 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 and PARTIAL VLAN-capable circuits do not split into multiple circuits during reconfiguration.

SONET Topologies and Upgrades

This chapter explains Cisco ONS 15327 SONET topologies and upgrades. To provision topologies, refer to the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

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.

8.1 Bidirectional Line Switched Rings

One ONS 15327 can support two concurrent bidirectional line switched rings (BLSRs). Each BLSR can have up to 32 ONS 15327s. Because the working and protect bandwidths must be equal, you can create only OC-12 or OC-48 BLSRs. For information about BLSR protection channels, see the "7.6 BLSR Protection Channel Access Circuits" section on page 7-9.

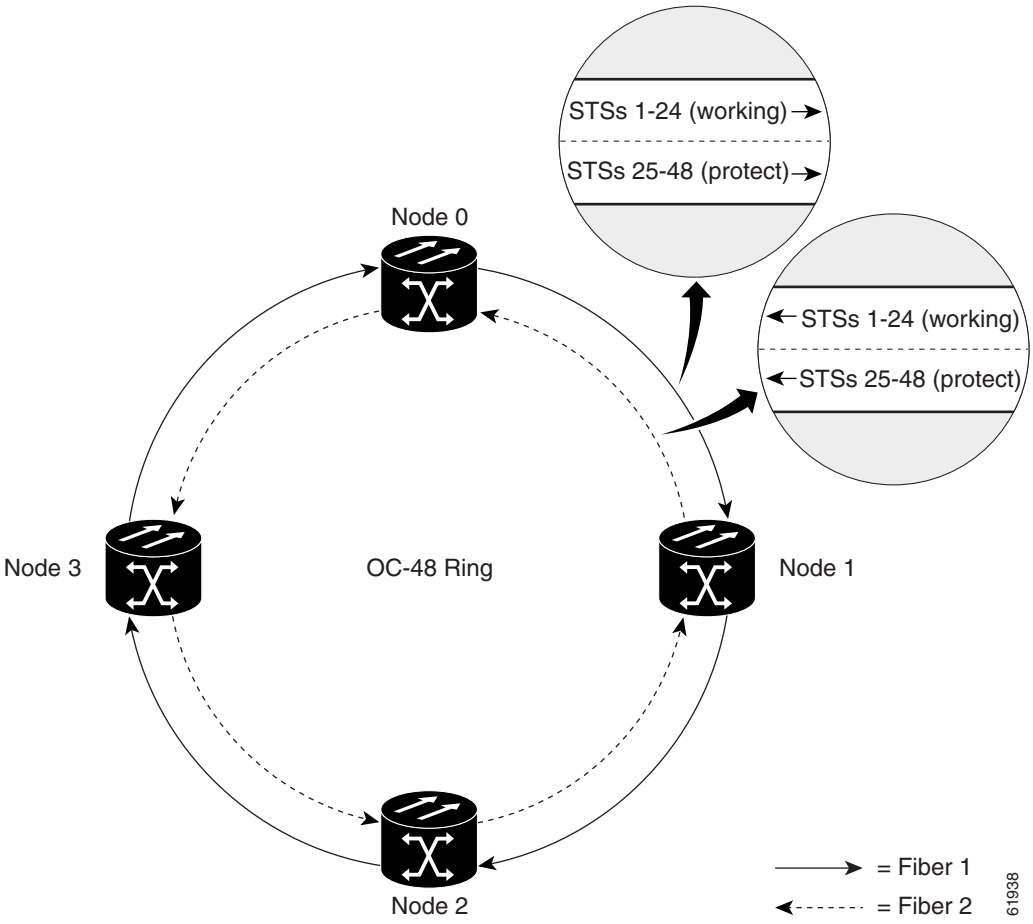
Note For best performance, BLSRs should have one LAN connection for every ten nodes in the BLSR.

8.1.1 BLSR Functionality

The Cisco ONS 15327 supports two-fiber BLSRs (the ONS 15454 also supports four-fiber BLSRs); each fiber in a two-fiber BLSR is divided into working and protect bandwidths. For example, in an OC-48 BLSR (Figure 8-1), STSs 1 to 24 carry the working traffic, and STSs 25 to 48 are reserved for

protection. Working traffic (STSs 1 to 24) travels in one direction on one fiber and in the opposite direction on the second fiber. The 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 8-1, circuits going from Node 0 to Node 1 typically travel on Fiber 1, unless that fiber is full, in which case circuits are routed on 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 8-1 Four-Node BLSR



The SONET K1, K2, and K3 bytes carry the information that governs BLSR protection switches. Each BLSR node monitors the K bytes to determine when to switch the SONET 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 8-2 shows a traffic pattern example on a four-node BLSR.

Figure 8-2 Four-Node BLSR Traffic Pattern Example

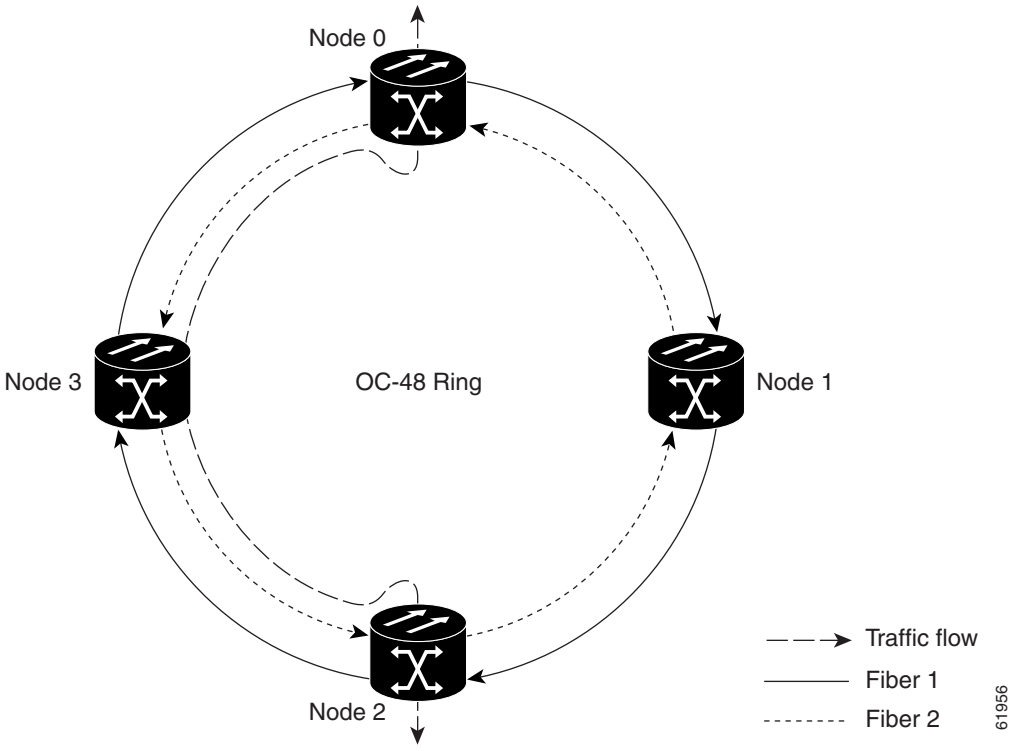
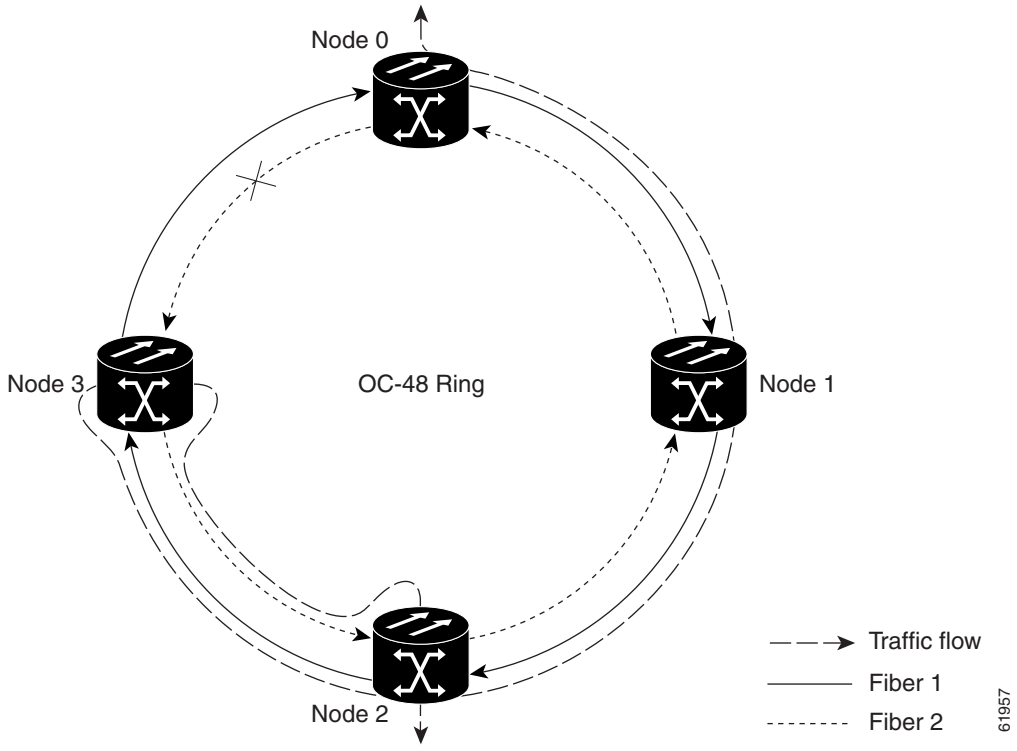


Figure 8-3 on page 8-4 shows how traffic is rerouted following a line break between Node 0 and Node 3.

- All circuits originating on Node 0 carried traffic to Node 2 on Fiber 2 are switched to the protect bandwidth of Fiber 1. For example, a circuit carrying traffic on STS-1 on Fiber 2 is switched to STS-25 on Fiber 1. A circuit carried on STS-2 on Fiber 2 is switched to STS-26 on Fiber 1. Fiber 1 carries the circuit to Node 3 (the original routing destination). Node 3 switches the circuit back to STS-1 on Fiber 2 where it is routed to Node 2 on STS-1.
- Circuits originating on Node 2 that normally carried traffic to Node 0 on Fiber 1 are switched to the protect bandwidth of Fiber 2 at Node 3. For example, a circuit carrying traffic on STS-2 on Fiber 1 is switched to STS-26 on Fiber 2. Fiber 2 carries the circuit to Node 0 where the circuit is switched back to STS-2 on Fiber 1 and then dropped to its destination.

Figure 8-3 Four-Node BLSR Traffic Pattern Following a Line Break



8.1.2 BLSR Bandwidth

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

BLSRs allow bandwidth to be reused around the ring and can carry more traffic than a network with traffic flowing through one central hub. BLSRs can also carry more traffic than a path protection operating at the same OC-N rate. Table 8-1 shows the bidirectional bandwidth capacities of BLSRs. The capacity is the OC-N rate divided by two, multiplied by the number of nodes in the ring minus the number of pass-through STS-1 circuits.

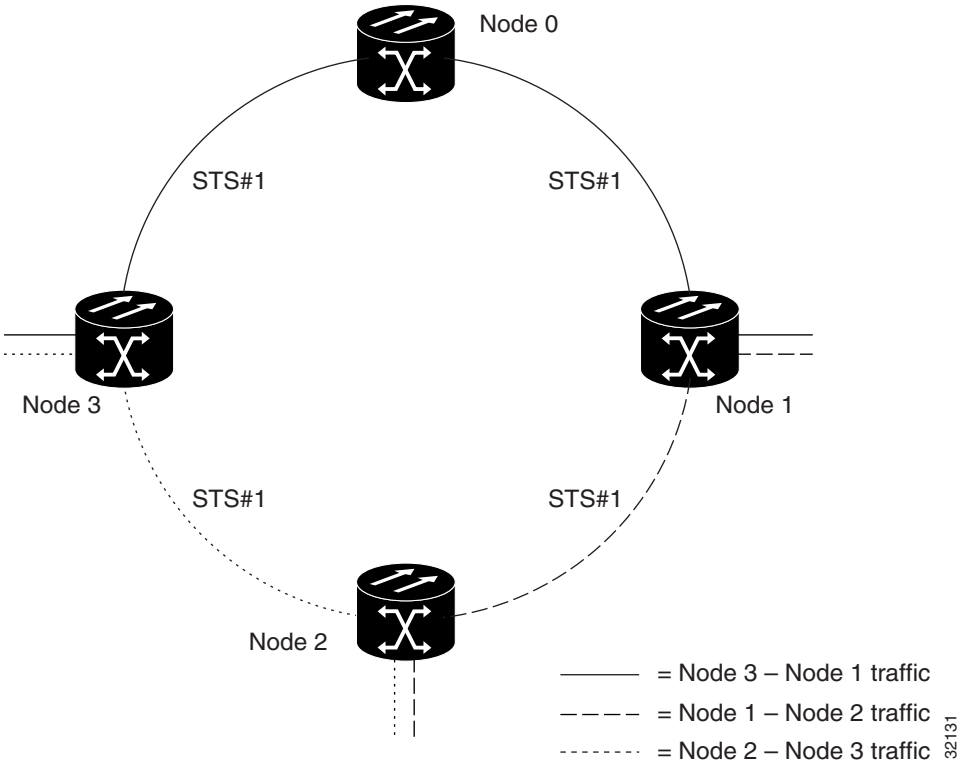
Table 8-1 BLSR Capacity

OC Rate	Working Bandwidth	Protection Bandwidth	Ring Capacity
OC-12	STS1 – 6	STS 7 – 12	6 x N[1] – PT[2]
OC-48	STS 1 – 24	STS 25 – 48	24 x N – PT

1. N is the number of ONS 15327 nodes configured as BLSR nodes.
2. PT is the number of STS-1 circuits passed through ONS 15327 nodes in the ring (capacity can vary depending on the traffic pattern).

Figure 8-4 shows an example of BLSR bandwidth reuse. The same synchronous transport signal (STS) 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 8-4 BLSR Bandwidth Reuse



8.1.3 BLSR Application Example

Figure 8-5 shows a BLSR implementation example. A regional long-distance network connects to other carriers at Node 0. Traffic is delivered to the service provider's major hubs.

- Carrier 1 delivers two DS-3s over one OC-3 spans to Node 0. Carrier 2 provides two DS-3s directly. Node 0 receives the signals and delivers them around the ring to the appropriate node.
- The ring also brings 14 DS-1s back from each remote site to Node 0. Intermediate nodes serve these shorter regional connections.
- The ONS 15327 OC-3 card supports a total of four OC-3 ports so that two additional OC-3 spans can be added at little cost.

Figure 8-5 Five-Node BLSR

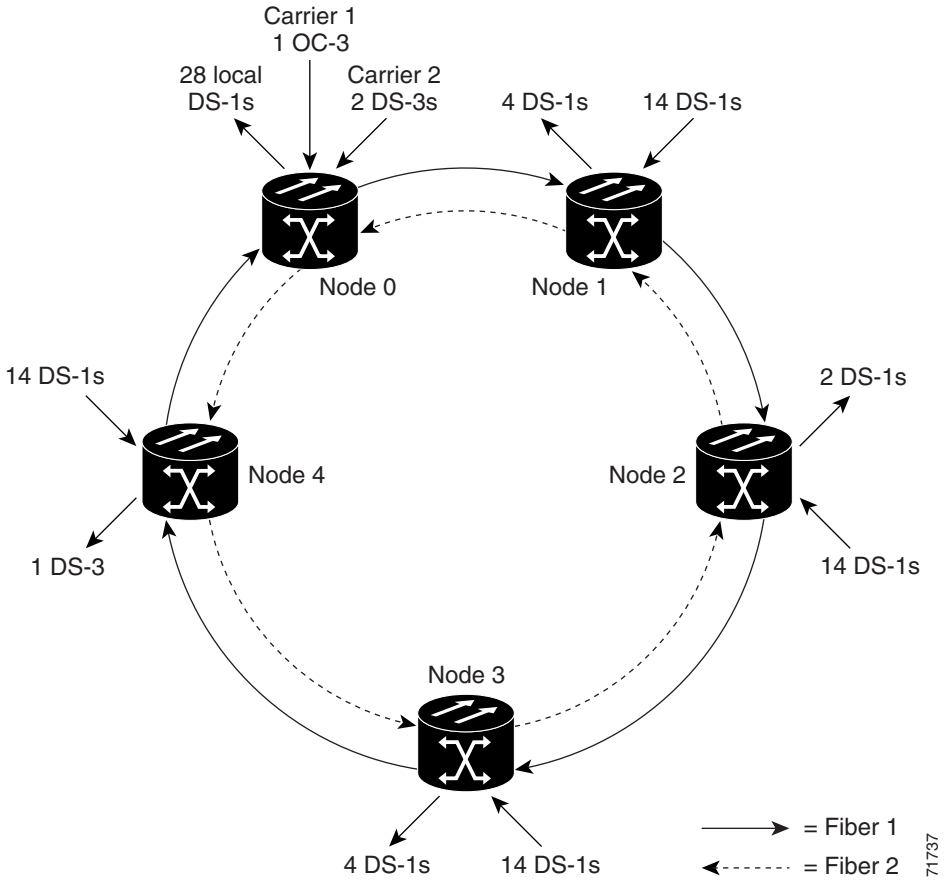


Figure 8-6 shows the shelf assembly layout for Node 0, which has no free slots.

Figure 8-6 Shelf Assembly Layout for Node 0 in Figure 8-5

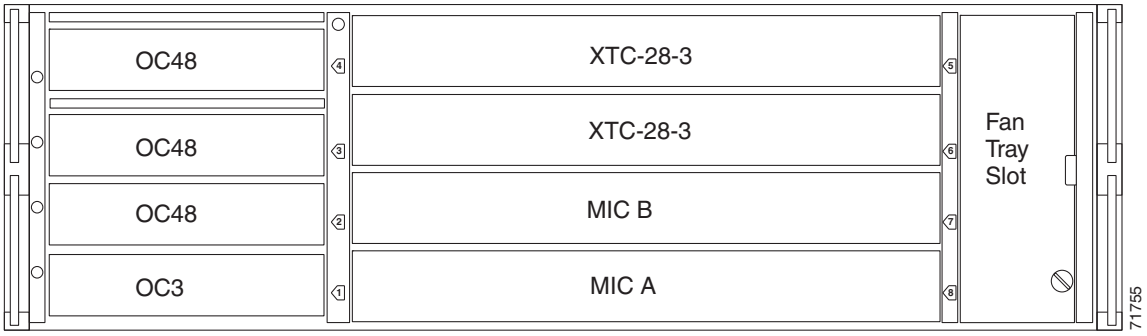
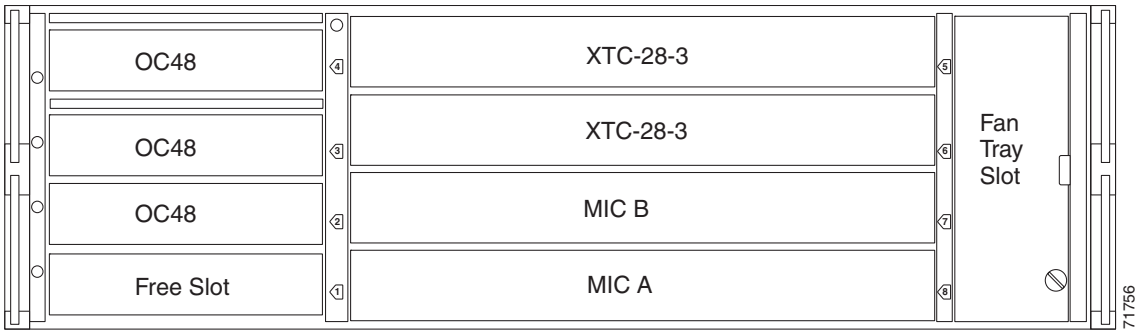


Figure 8-7 shows the shelf assembly layout for the remaining sites in the ring. In this BLSR configuration, an additional three DS-3s at Nodes 1, 2, 3, and 4 can be activated. Each site has free slots for future traffic needs.

Figure 8-7 Shelf Assembly Layout for Nodes 1 to 4 in Figure 8-5

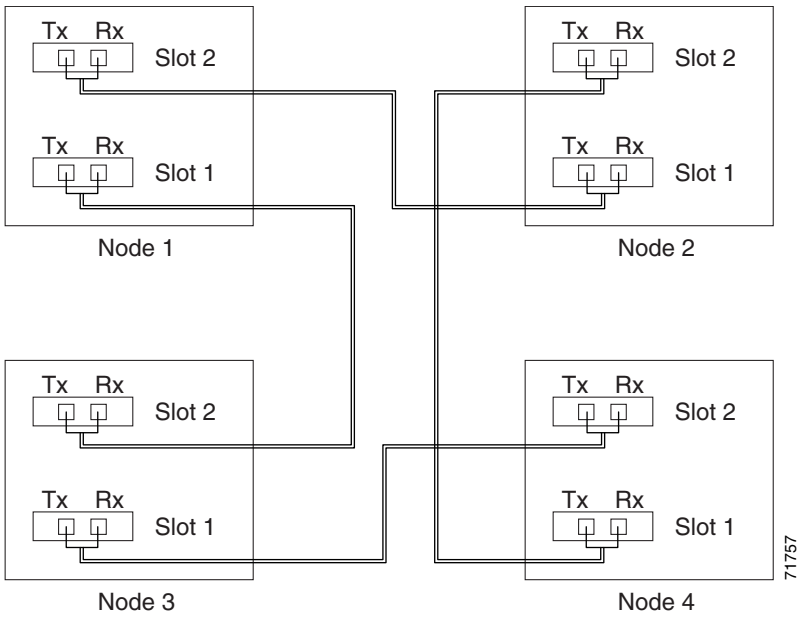


8.1.4 BLSR Fiber Connections

Plan your fiber connections and use the same plan for all BLSR 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 8-8 shows fiber connections for a BLSR with trunk (span) cards in Slot 1 (west) and Slot 2 (east). See the *Cisco ONS 15327 Procedure Guide* for fiber connection procedures.

Note Always plug the transmit (Tx) connector of an OC-N card at one node into the receive (Rx) connector of an OC-N card at the adjacent node. Cards display a signal fail (SF) LED when Tx and Rx connections are mismatched.

Figure 8-8 Connecting Fiber to a Four-Node, Two-Fiber BLSR



8.2 Connecting ONS 15327 Nodes and ONS 15454 Nodes

You can install ONS 15327 nodes into a network comprised entirely of ONS 15327 nodes or into a network that has a mix of ONS 15327 and ONS 15454 nodes. The ONS 15327 interoperates with the ONS 15454 in linear, path protection, and 2-fiber BLSR configurations. Because connection procedures for both types of nodes are the same (for example, adding or dropping nodes from a path protection or linear configuration, or creating DCCs), follow the instructions in the *Cisco ONS 15327 Procedure Guide* whenever you make connections between ONS 15454 and ONS 15327 nodes. Figure 8-9 shows a basic linear or path protection connection between ONS 15327 and ONS 15454 nodes.

Figure 8-9 Linear or Path Protection Connection between ONS 15454 and ONS 15327 Nodes

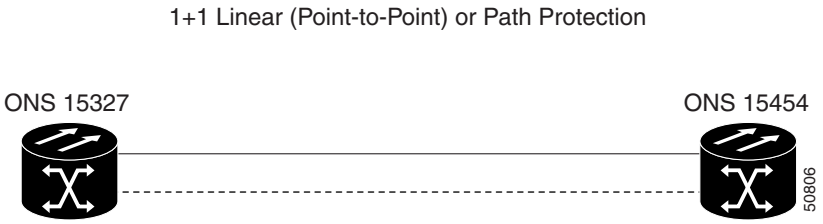
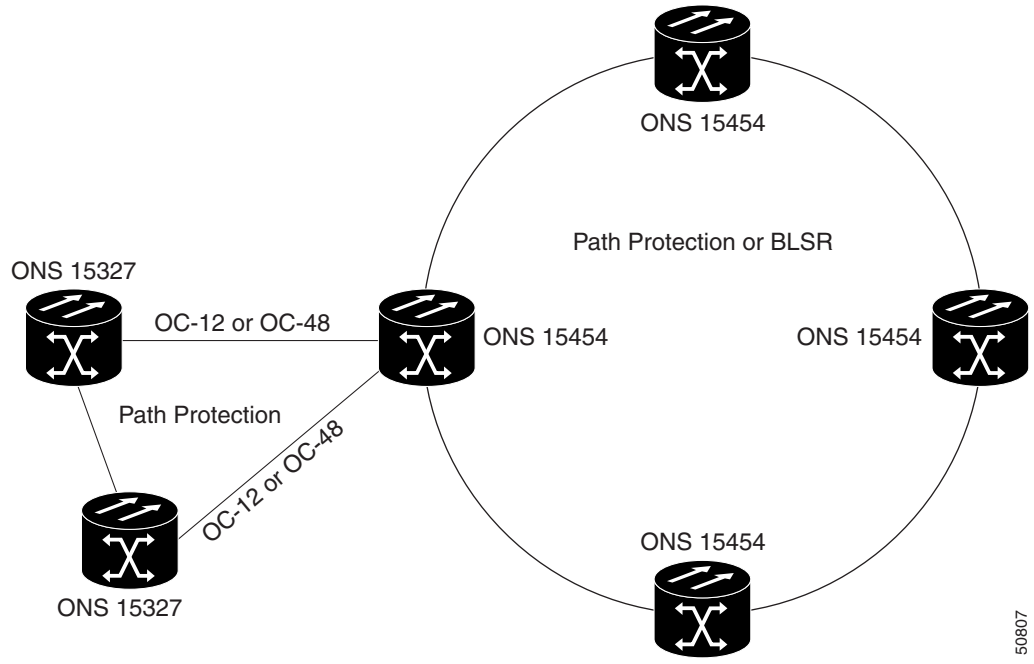


Figure 8-10 shows a ring of ONS 15327s subtended from a ring of ONS 15454s.

Figure 8-10 ONS 15327 Ring Subtended from an ONS 15454 Ring

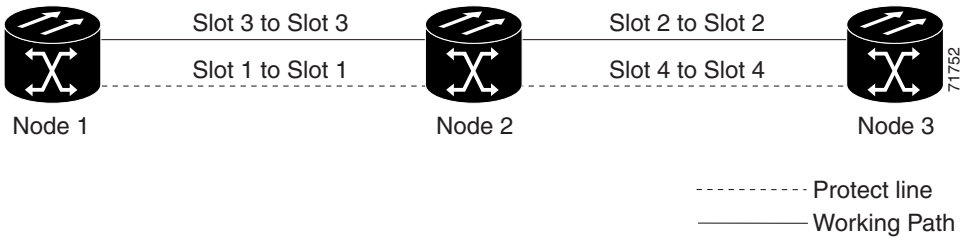


8.3 Terminal Point-to-Point and Linear ADM Configurations

You can configure ONS 15327s in a terminal point-to-point network (2 nodes) or as a line of add/drop multiplexers (ADMs) (3 or more nodes) by configuring one set of OC-N cards as the working path and a second set as the protect path. Unlike rings, terminal and linear ADMs require that the OC-N cards at each node be in 1+1 protection to ensure that a break to the working line is automatically routed to the protect line.

Figure 8-11 shows three ONS 15327s in a linear ADM configuration. Working traffic flows from Slot 3/Node 1 to Slot 3/Node 2, and from Slot 2/Node 2 to Slot 2/Node 3. You create the protect path by placing Slot 3 in 1+1 protection with Slot 1 at Nodes 1 and 2, and Slot 2 in 1+1 protection with Slot 4 at Nodes 2 and 3.

Figure 8-11 Linear ADM Configuration



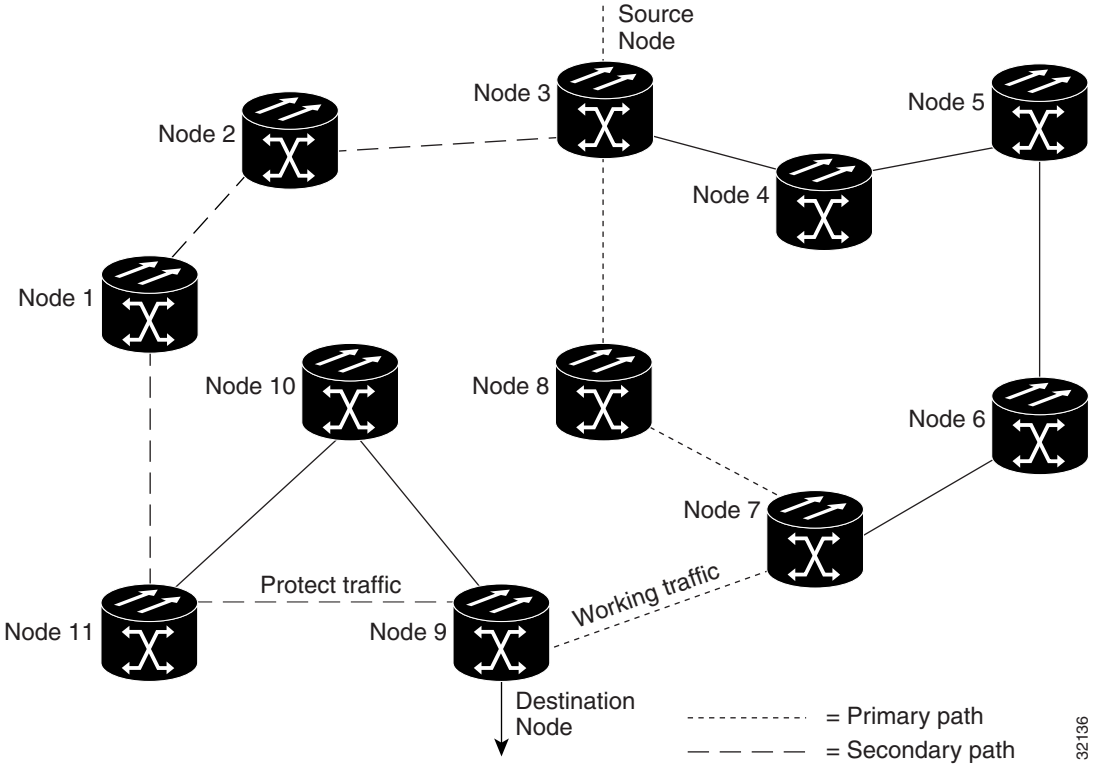
8.4 Path-Protected Mesh Networks

In addition to single BLSRs, path protection configurations, and terminal point-to-point or linear ADMs, you can extend ONS 15327 traffic protection by creating path-protected mesh networks (PPMNs). PPMNs include multiple ONS 15327 SONET topologies and extend the protection provided by a single path protection to the meshed architecture of several interconnecting rings. In a PPMN, circuits travel diverse paths through a network of single or multiple meshed rings. When you create circuits, you can have CTC automatically route circuits across the PPMN, 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 8-12, 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.

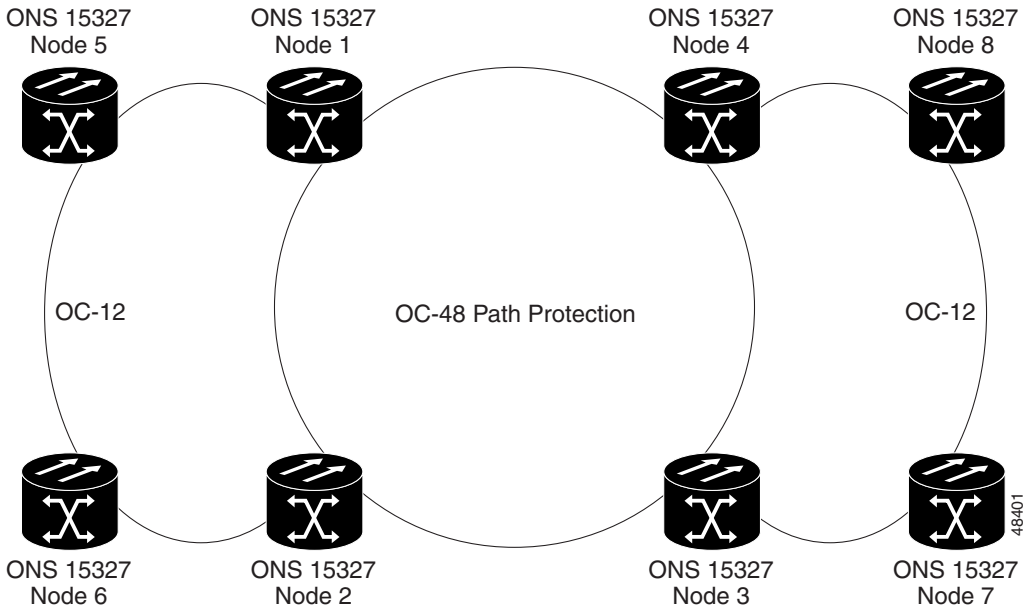
If full protection is selected, CTC creates a second unique route between Nodes 3 and 9 which, in this example, passes through Nodes 2, 1, and 11. Cross-connections are automatically created at Nodes 3, 2, 1, 11, and 9, shown by the dashed line. If a failure occurs on the primary path, traffic switches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

Figure 8-12 Path-Protected Mesh Network



PPMN also allows spans with different SONET speeds to be mixed together in "virtual rings." Figure 8-13 shows Nodes 1, 2, 3, and 4 in a standard OC-48 ring. Nodes 5, 6, 7, and 8 link to the backbone ring through OC-12 fiber. The "virtual ring" formed by Nodes 5, 6, 7, and 8 uses both OC-48 and OC-12 cards.

Figure 8-13 PPMN Virtual Ring



8.5 Four Node Configurations

You can link multiple ONS 15327s using their OC-N cards (also known as creating a fiber-optic bus) to accommodate more access traffic than a single ONS 15327 can support. For example, to drop more than 28 DS-1s or 3 DS-3s (the maximum that can be aggregated in a single node), you can link the nodes but not merge multiple nodes into a single ONS 15327. You can link nodes with OC-12 or OC-48 fiber spans as you would link any other two network nodes. The nodes can be grouped in one facility to aggregate more local traffic.

8.6 OC-N Speed Upgrades

A span is the optical fiber connection between two ONS 15327 nodes. In a span (optical speed) upgrade, the transmission rate of a span is upgraded from a lower to a higher OC-N signal but all other span configuration attributes remain unchanged. With multiple nodes, a span upgrade is a coordinated series of upgrades on all nodes in the ring or protection group.

To perform a span upgrade, the higher-rate optical card must replace the lower-rate card in the same slot. All spans in the network must be upgraded. The protection configuration of the original lower-rate optical card (BLSR, path protection, and 1+1) is retained for the higher-rate optical card.

When performing span upgrades on a large number of nodes, Cisco recommends that you upgrade all spans in a network consecutively and in the same maintenance window. Until all spans are upgraded, mismatched card types are present.

Cisco recommends using the Span Upgrade Wizard to perform span upgrades. Although you can also use the manual span upgrade procedures, the manual procedures are mainly provided as error recovery for the wizard. The Span Upgrade Wizard and the manual span upgrade procedures require at least two technicians (one at each end of the span) who can communicate with each other during the upgrade. Upgrading a span is non-service affecting and causes no more than three switches, each of which is less than 50 ms in duration.

Note Span upgrades do not upgrade SONET topologies, for example, a 1+1 group to a BLSR. See the *Cisco ONS 15327 Procedure Guide* for topology upgrade procedures.

8.6.1 Span Upgrade Wizard

The Span Upgrade Wizard automates all steps in the manual span upgrade procedure (BLSR, path protection, and 1+1). The wizard can upgrade both lines of a 1+1 group; the wizard upgrades path protection configurations and BLSRs one line at a time. The Span Upgrade Wizard requires that spans have DCCs enabled.

The Span Upgrade Wizard provides no way to back out of an upgrade. In the case of an error, you must exit the wizard and initiate the manual procedure to either continue with the upgrade or back out of it. To continue with the manual procedure, examine the standing conditions and alarms to identify the stage in which the wizard failure occurred.

8.6.2 Manual Span Upgrades

Manual span upgrades are mainly provided as error recovery for the Span Upgrade Wizard, but they can be used to perform span upgrades. You can perform a manual span upgrade on a BLSR, path protection, and on a 1+1 protection group.

Downgrading can be performed to back out of a span upgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate card type and install a lower-rate card. You cannot downgrade if circuits exist on the STSs to be removed (the higher STSs).

8.7 In-Service Topology Upgrades

Topology upgrades can be performed 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 may not be protected during the upgrade. The following in-service topology upgrades are supported:

- Unprotected point-to-point or linear ADM to path protection
- Point-to-point or linear ADM to two-fiber BLSR
- Path protection to two-fiber BLSR
- 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 a circuit must have a DISCOVERED status.

Circuit types supported for in-service topology upgrades are:

- STS, VT, and VT tunnels

- virtual concatenated (VCAT)
- 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. For in-service topology upgrade procedures, refer to the "Convert Network Configurations" chapter in the *Cisco ONS 15327 Procedure Guide*. For procedures to add or remove a node, refer to the "Add and Remove Nodes" chapter of the *Cisco ONS 15327 Procedure Guide*.

Note A database restore on all nodes in a topology returns converted circuits to their original topology.

Note Open-ended path protection and DRI configurations do not support in-service topology upgrades.

8.7.1 Unprotected Point-to-Point or Linear ADM to Path Protection

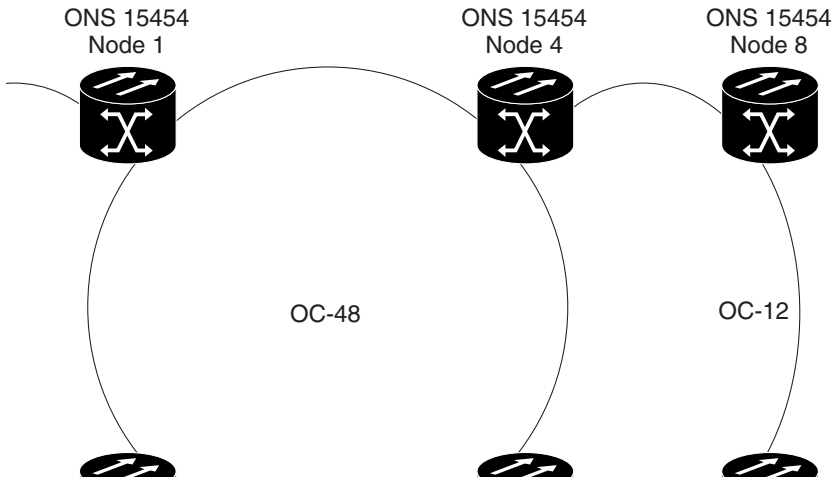
CTC provides a topology conversion wizard for converting an unprotected point-to-point or linear ADM topology to path protection. This conversion occurs at the circuit level. CTC calculates the additional path protection circuit route automatically or you can do it manually. When routing the path protection circuit, you can provision the path protection as go-and-return or unidirectional.

When performing an in-service topology upgrade on a configuration with VCAT circuits, CTC allows you to select member circuits to upgrade individually. When upgrading VT tunnels, CTC does not convert the VT tunnel to path protection, but instead creates a secondary tunnel for the alternate path. The result is two unprotected VT tunnels using alternate paths.

To convert from point-to-point or linear ADM to a path protection, the topology requires an additional circuit route to complete the ring. When the route is established, CTC creates circuit connections on any intermediate nodes and modifies existing circuit connections on the original circuit path. The number and position of network spans in the topology remains unchanged during and after the conversion.

Figure 8-14 shows an unprotected point-to-point ADM configuration converted to a path protection. An additional circuit routes through Node 3 to complete the path protection.

Figure 8-14 Unprotected Point-to-Point ADM to Path Protection Conversion



8.7.2 Point-to-Point or Linear ADM to Two-Fiber BLSR

A 1+1 point-to-point or linear ADM to a two-fiber BLSR 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 is to become the protection portion of the two-fiber BLSR and recreate them in the appropriate bandwidth. Finally, you must provision the nodes as BLSR nodes.

To complete a conversion from an unprotected point-to-point or linear ADM to a two-fiber BLSR, use the CTC Convert Unprotected/UPSR to BLSR wizard from the Tools > Topology Upgrade menu.

8.7.3 Path Protection to Two-Fiber BLSR

CTC provides a topology conversion wizard to convert a path protection to a two-fiber BLSR. An upgrade from a path protection to a two-fiber BLSR changes path protection to line protection. A path protection can have a maximum of 16 nodes before conversion. Circuits paths must occupy the same time slots around the ring. Only the primary path through the path protection is needed; the topology conversion wizard removes the alternate path protection path during the conversion. Because circuit paths can begin and end outside of the topology, the conversion might create line-protected segments within path protection paths of circuits outside the scope of the ring. The physical arrangement of the ring nodes and spans remains the same after the conversion.

8.7.4 Add or Remove a Node from a Topology

You can add or remove a node from a linear ADM, BLSR, or path protection configuration. Adding or removing nodes from BLSRs is potentially service affecting, however adding and removing nodes from an existing 1+1 linear ADM or path protection 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.

Management Network Connectivity

This chapter provides an overview of ONS 15327 data communications network (DCN) connectivity. Cisco ONS network communication is based on IP, including communication between Cisco Transport Controller (CTC) computers and ONS 15327s, and communication among networked Cisco ONS 15327 nodes. This chapter provides scenarios showing ONS 15327s in common IP network configurations as well as information about provisionable patchcords, 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 15327 networking setup instructions, refer to the "Turn Up Node" chapter of the *Cisco ONS 15327 Procedure Guide*.

Although ONS 15327 DCN communication is based on IP, ONS 15327s can be networked to equipment that is based on the Open System Interconnection (OSI) protocol suites. This chapter describes the ONS 15327 OSI implementation and provides scenarios that show how ONS 15327 can be networked within a mixed IP and OSI environment.

Chapter topics include:

Note To connect ONS 15327s to 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 15327s can be connected in many different ways within an IP environment:

- They can be connected to LANs through direct connections or a router.

- IP subnetting can create ONS 15327 login node groups, which allow you to provision non-data communications channel (DCC) connected nodes in a network.
- Different IP functions and protocols can be used to achieve specific network goals. For example, Proxy Address Resolution Protocol (ARP) enables one LAN-connected ONS 15327 to serve as a gateway for ONS 15327s that are not connected to the LAN.
- You can create static routes to enable connections among multiple CTC sessions with ONS 15327s that reside on the same subnet with multiple CTC sessions.
- If ONS 15327s are connected to Open Shortest Path First (OSPF) networks, ONS 15327 network information is automatically communicated across multiple LANs and WANs.
- The ONS 15327 proxy server controls the visibility and accessibility between CTC computers and ONS 15327 element nodes.

9.2 IP Addressing Scenarios

ONS 15327 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 15327s in IP networks.

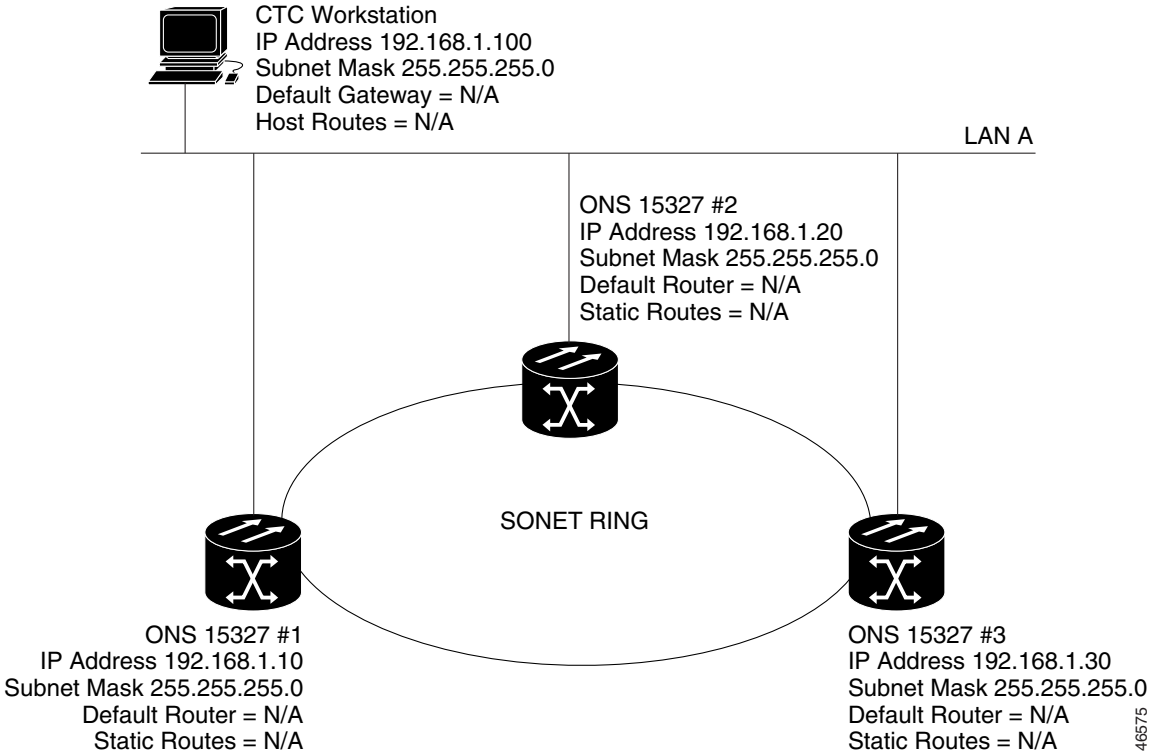
Table 9-1 General ONS 15327 IP Troubleshooting Checklist

Item	What to Check
Link integrity	Verify that link integrity exists between: • The CTC computer and network hub/switch. • ONS 15327s (wire-wrap pins or RJ-45 port) and network hub/switch. • Router ports and hub/switch ports.
ONS 15327 hub/switch ports	Verify connectivity. If connectivity problems occur, set the hub or switch port that is connected to the ONS 15327 to 10 Mbps half-duplex.
Ping	Ping the node to test connections between computers and ONS 15327s.
IP addresses/subnet masks	Verify that ONS 15327 IP addresses and subnet masks are set up correctly.
Optical connectivity	Verify that ONS 15327 optical trunk ports are in service and that a DCC is enabled on each trunk port.

9.2.1 Scenario 1: CTC and ONS 15327s on the Same Subnet

Scenario 1 shows a basic ONS 15327 LAN configuration (Figure 9-1). The ONS 15327s and CTC computer reside on the same subnet. All ONS 15327s connect to LAN A, and all ONS 15327s have DCC connections.

Figure 9-1 Scenario 1: CTC and ONS 15327s on the Same Subnet

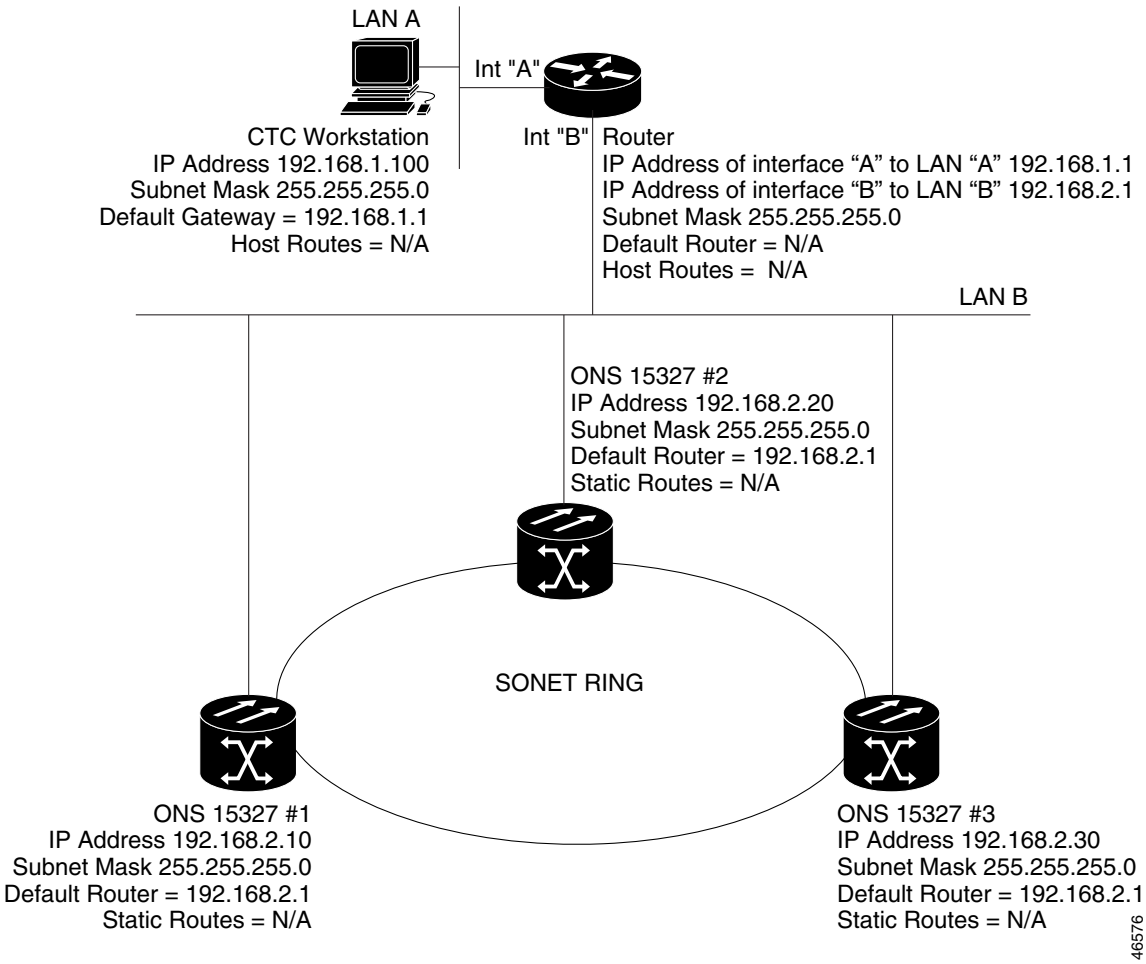


9.2.2 Scenario 2: CTC and ONS 15327s Connected to a Router

In Scenario 2 the CTC computer resides on a subnet (192.168.1.0) and attaches to LAN A (Figure 9-2). The ONS 15327s 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 Figure 9-2, a DHCP server is not available.

Figure 9-2 Scenario 2: CTC and ONS 15327s Connected to Router



9.2.3 Scenario 3: Using Proxy ARP to Enable an ONS 15327 Gateway

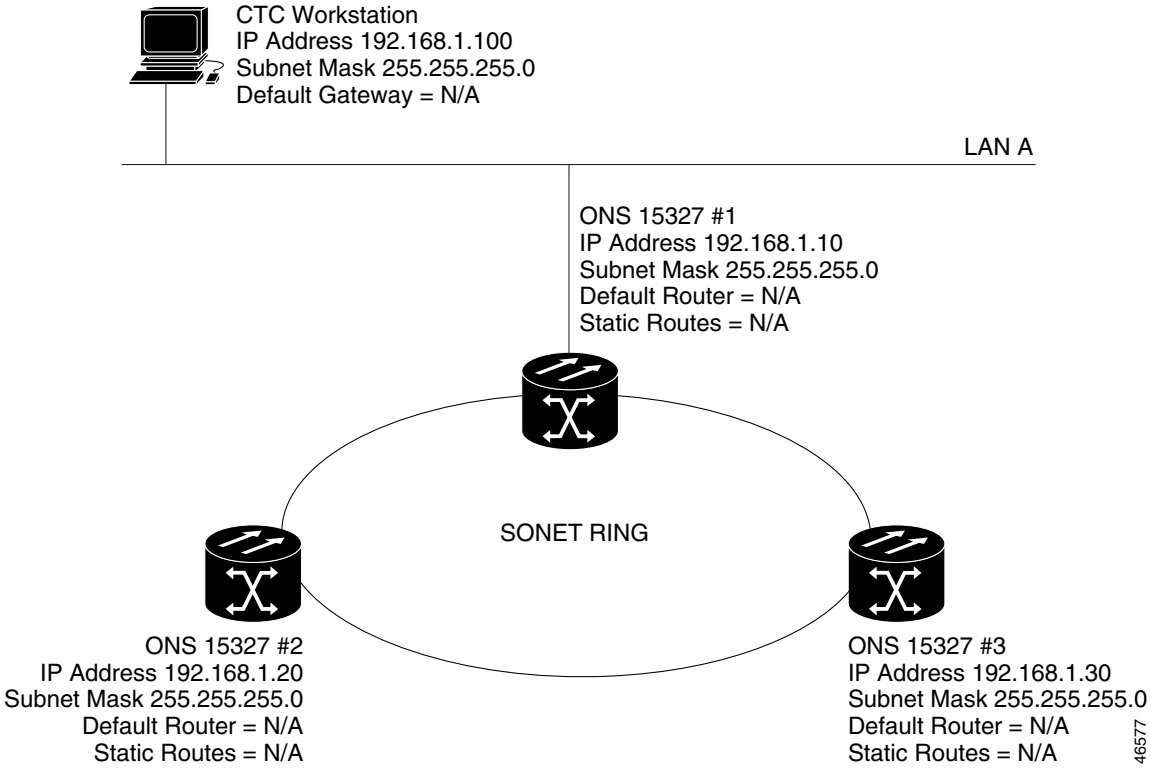
ARP matches higher-level IP addresses to the physical addresses of the destination host. It uses a lookup table (called ARP cache) to perform the translation. When the address is not found in the ARP cache, a broadcast is sent out on the network with a special format called the ARP request. If one of 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 15327 to respond to the ARP request for ONS 15327s not connected to the LAN. (ONS 15327 proxy ARP requires no user configuration.) For this to occur, The DCC-connected ONS 15327s must reside on the same subnet. When a LAN device sends an ARP request to an ONS 15327 that is not connected to the LAN, the gateway ONS 15327 returns its MAC address to the LAN device. The LAN device then sends the datagram for the remote ONS 15327 to the MAC address of the proxy ONS 15327. The proxy ONS 15327 uses its routing table to forward the datagram to the non-LAN ONS 15327.

Scenario 3 is similar to Scenario 1, but only one ONS 15327 (#1) connects to the LAN (Figure 9-3). Two ONS 15327s (#2 and #3) connect to ONS 15327 #1 through the SONET DCC. Because all three ONS 15327s are on the same subnet, Proxy ARP enables ONS 15327 #1 to serve as a gateway for ONS 15327 #2 and #3.

Note This scenario assumes all CTC connections are to ONS 15327 #1. If you connect a laptop computer to either #2 or #3, network partitioning occurs, and neither the laptop nor the CTC computer is able to see all nodes. If you want laptops to connect directly to end network elements, you need to create static routes (see Scenario 5) or enable the ONS 15327 proxy server (see Scenario 7).

Figure 9-3 Scenario 3: Using Proxy ARP

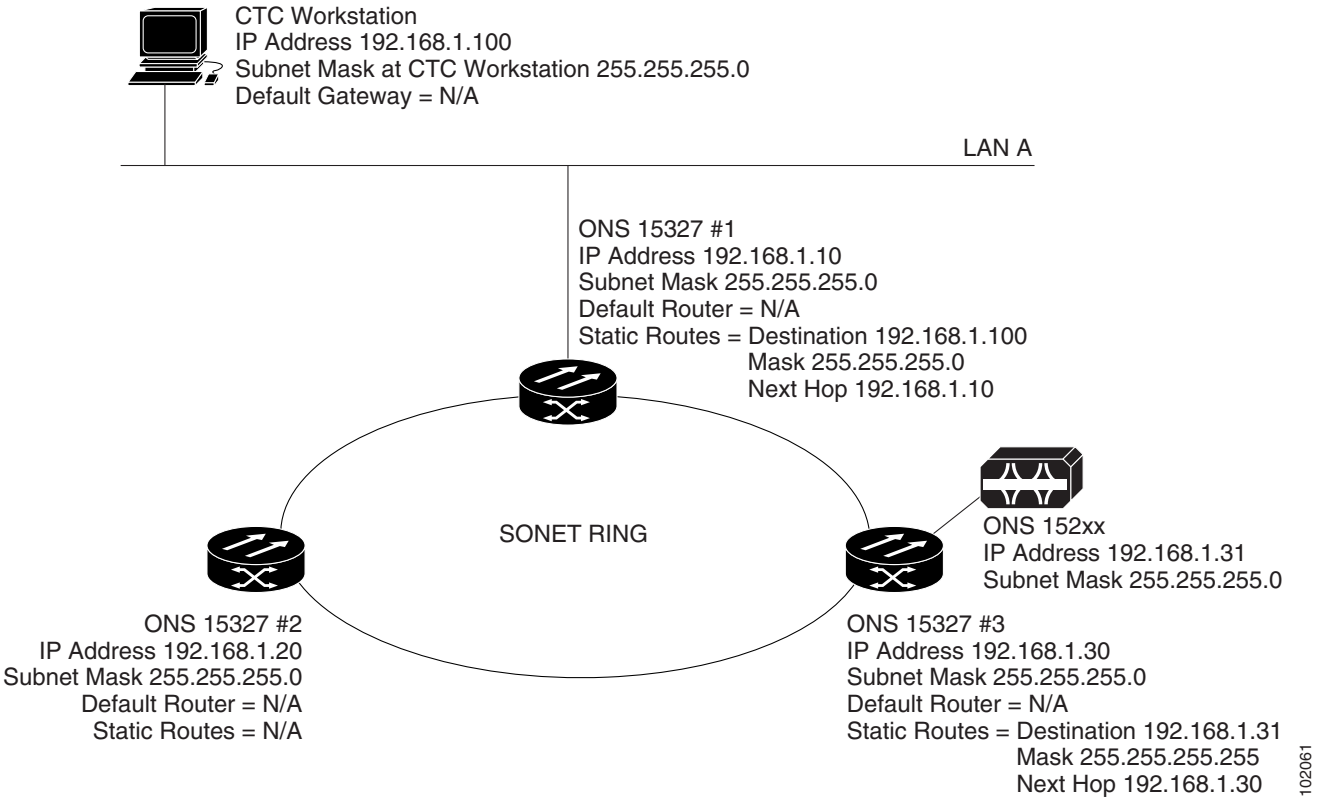


You can also use proxy ARP to communicate with hosts attached to the craft Ethernet ports of DCC-connected nodes (Figure 9-4). The node with an attached host must have a static route to the host. Static routes are propagated to all DCC peers using OSPF. The existing proxy ARP node is the gateway for additional hosts. Each node examines its routing table for routes to hosts that are not connected to the DCC network but are within the subnet. The existing proxy server replies to ARP requests for these additional hosts with the node MAC address. The existence of the host route in the routing table ensures that the IP packets addressed to the additional hosts are routed properly. Other than establishing a static route between a node and an additional host, no provisioning is necessary. The following restrictions apply:

- Only one node acts as the proxy ARP server for any given additional host.
- A node cannot be the proxy ARP server for a host connected to its Ethernet port.

In Figure 9-4, Node #1 announces to Node #2 and #3 that it can reach the CTC host. Similarly, Node #3 announces that it can reach the ONS 152xx. The ONS 152xx is shown as an example; any network element can be set up as an additional host.

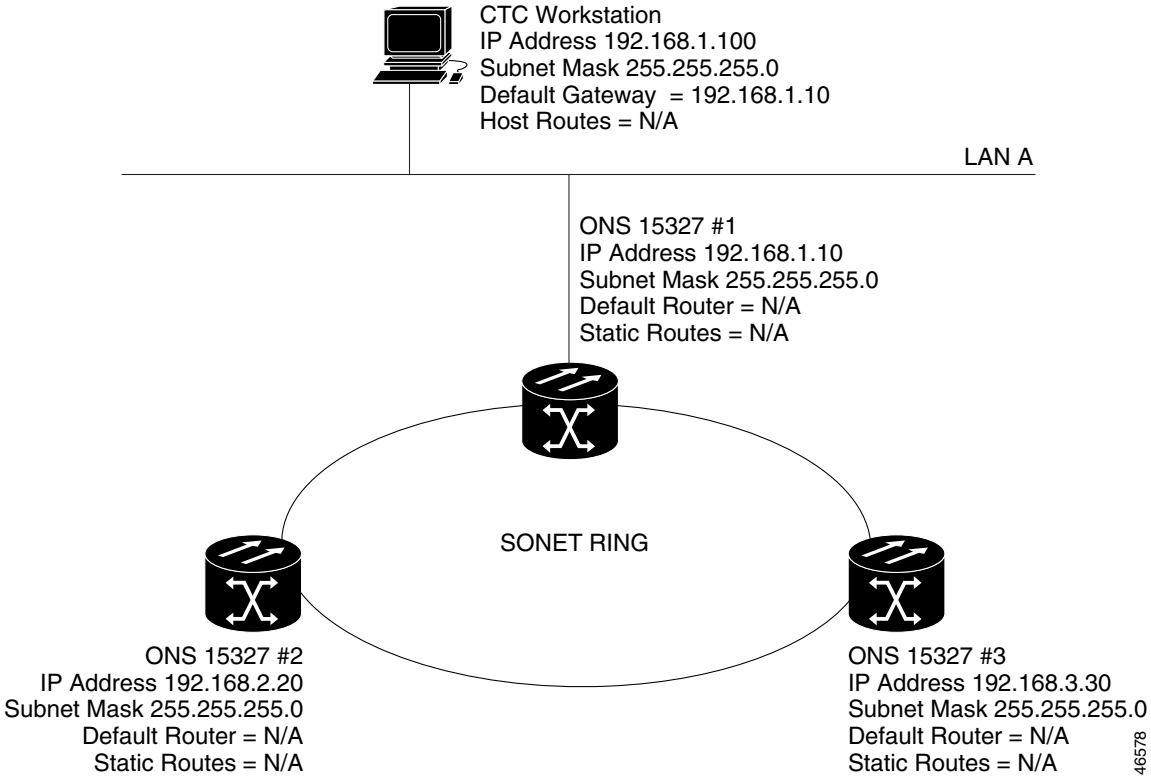
Figure 9-4 Scenario 3: Using Proxy ARP with Static Routing



9.2.4 Scenario 4: Default Gateway on CTC Computer

Scenario 4 is similar to Scenario 3, but ONS 15327 #2 and #3 reside on different subnets, 192.168.2.0 and 192.168.3.0, respectively (Figure 9-5). Node #1 and the CTC computer are on subnet 192.168.1.0. Proxy ARP is not used because the network includes different subnets. In order for the CTC computer to communicate with Nodes #2 and #3, Node #1 is entered as the default gateway on the CTC computer.

Figure 9-5 Scenario 4: Default Gateway on a CTC Computer



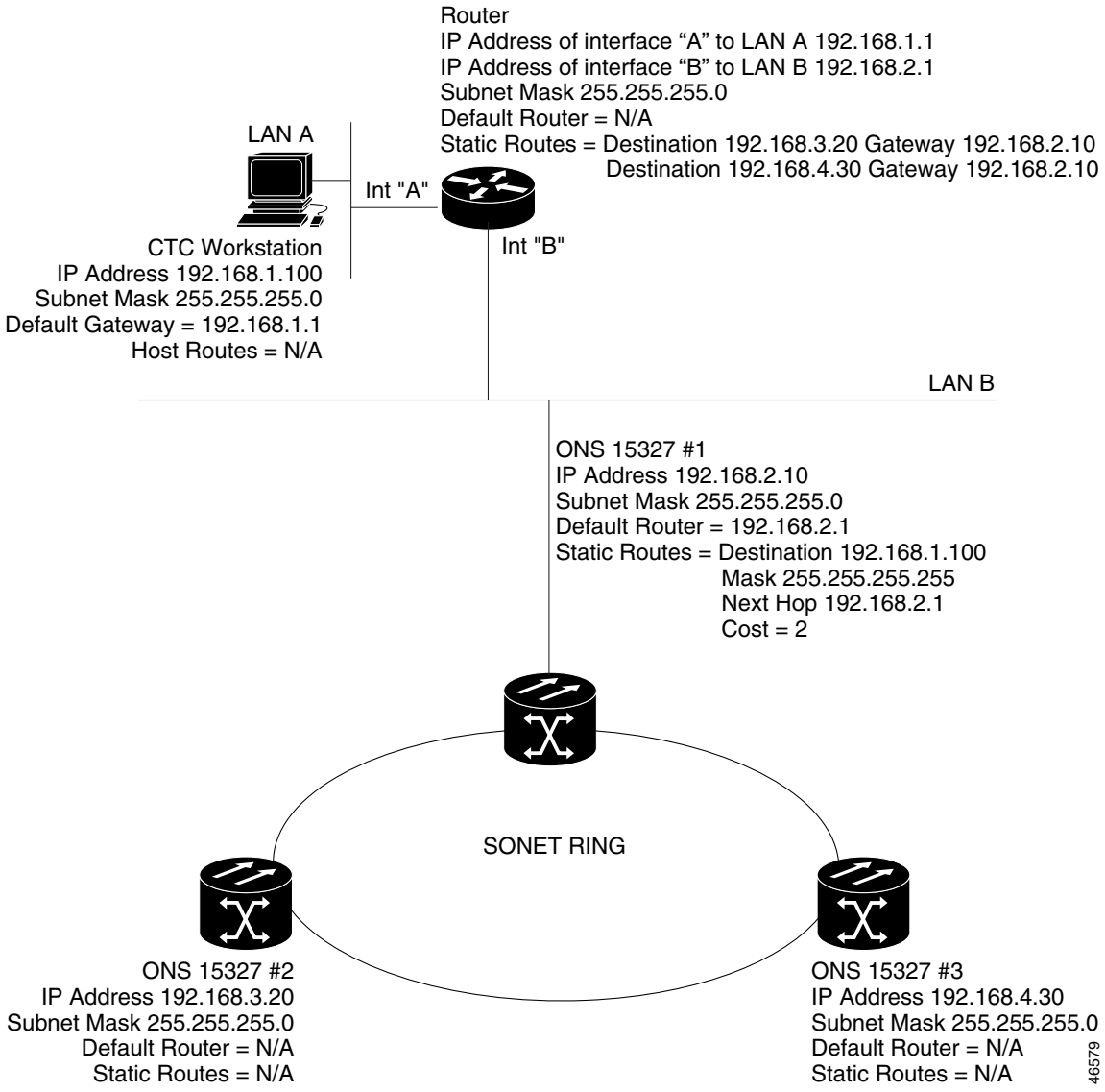
9.2.5 Scenario 5: Using Static Routes to Connect to LANs

Static routes are used for two purposes:

- To connect ONS 15327s to CTC sessions on one subnet that are connected by a router to ONS 15327s 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 15327s residing on the same subnet.

In Figure 9-6, one CTC computer residing on subnet 192.168.1.0 connects to a router through interface A. (The router is not set up with OSPF.) ONS 15327s residing on different subnets are connected through Node #1 to the router through interface B. Because Nodes #2 and #3 are on different subnets, proxy ARP does not enable Node #1 as a gateway. To connect to CTC computers on LAN A, a static route is created on Node #1.

Figure 9-6 Scenario 5: Static Route with One CTC Computer Used as a Destination

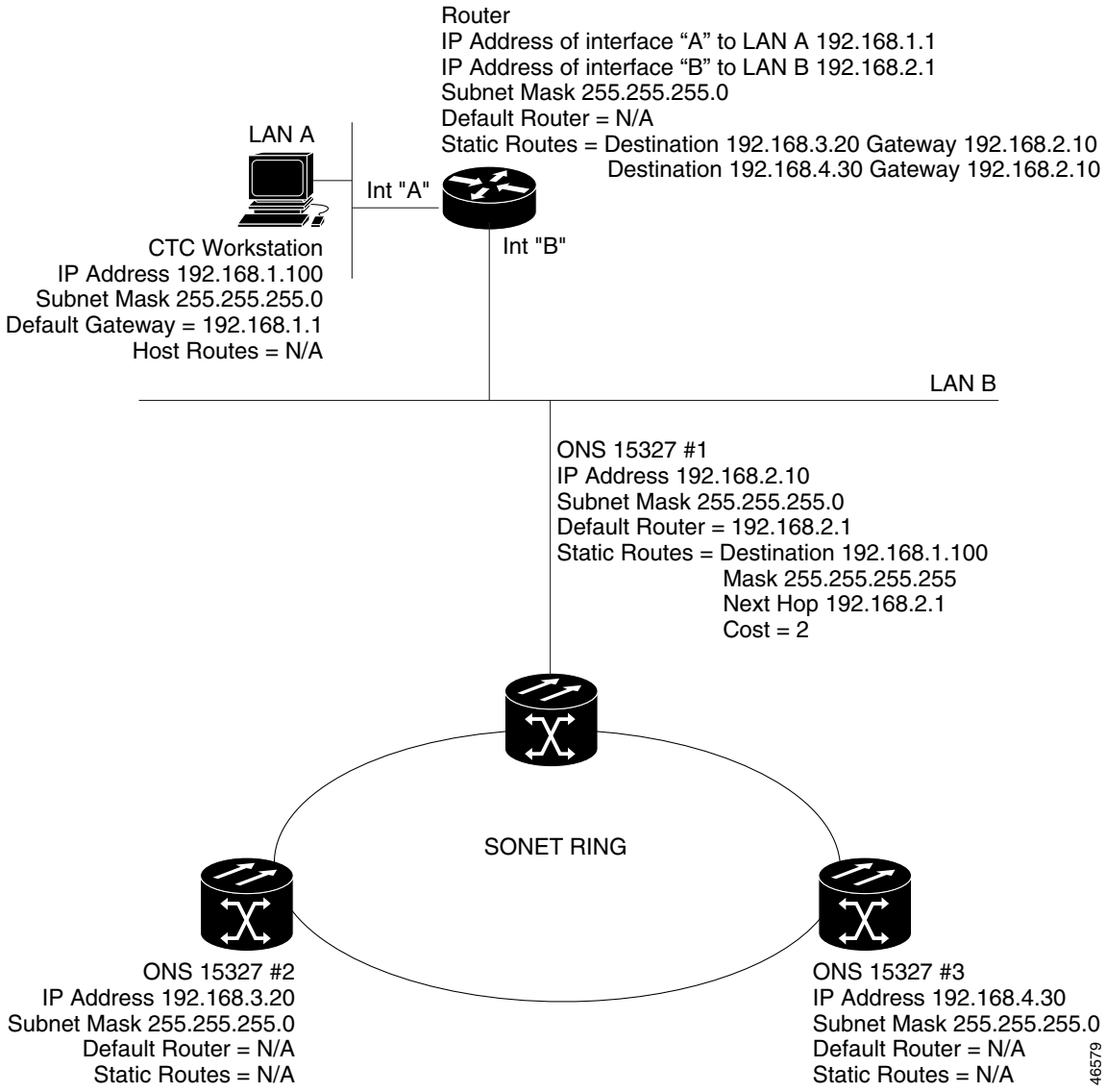


The destination and subnet mask entries control access to the ONS 15327s. Depending upon your configuration, take one of the following actions:

- If a single CTC computer is 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 a router, enter a destination of 0.0.0.0 and a subnet mask of 0.0.0.0. Figure 9-7 shows an example.

The IP address of router interface B is entered as the next hop, and the cost (number of hops from source to destination) is 2.

Figure 9-7 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 the status of their links to their neighbors. Link state protocols advertise their directly connected networks and their active links. Each link state router captures the 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. Routes are recalculated when topology changes occur.

The ONS 15327 uses OSPF protocol in internal ONS 15327 networks for node discovery, circuit routing, and node management. You can enable OSPF on the ONS 15327 so that the ONS 15327 topology is sent to OSPF routers on a LAN. Advertising the ONS 15327 network topology to LAN routers eliminates the need to enter static routes for ONS 15327 subnetworks manually.

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. Every OSPF network has one backbone area called “area 0.” All other OSPF areas must connect to area 0.

When you enable an ONS 15327 OSPF topology for advertising to an OSPF network, you must assign an OSPF area ID in decimal format to the ONS 15327 network. Coordinate the area ID number assignment with your LAN administrator. All DCC-connected ONS 15327s should be assigned the same OSPF area ID.

Figure 9-8 shows a network enabled for OSPF.

Figure 9-8 Scenario 6: OSPF Enabled

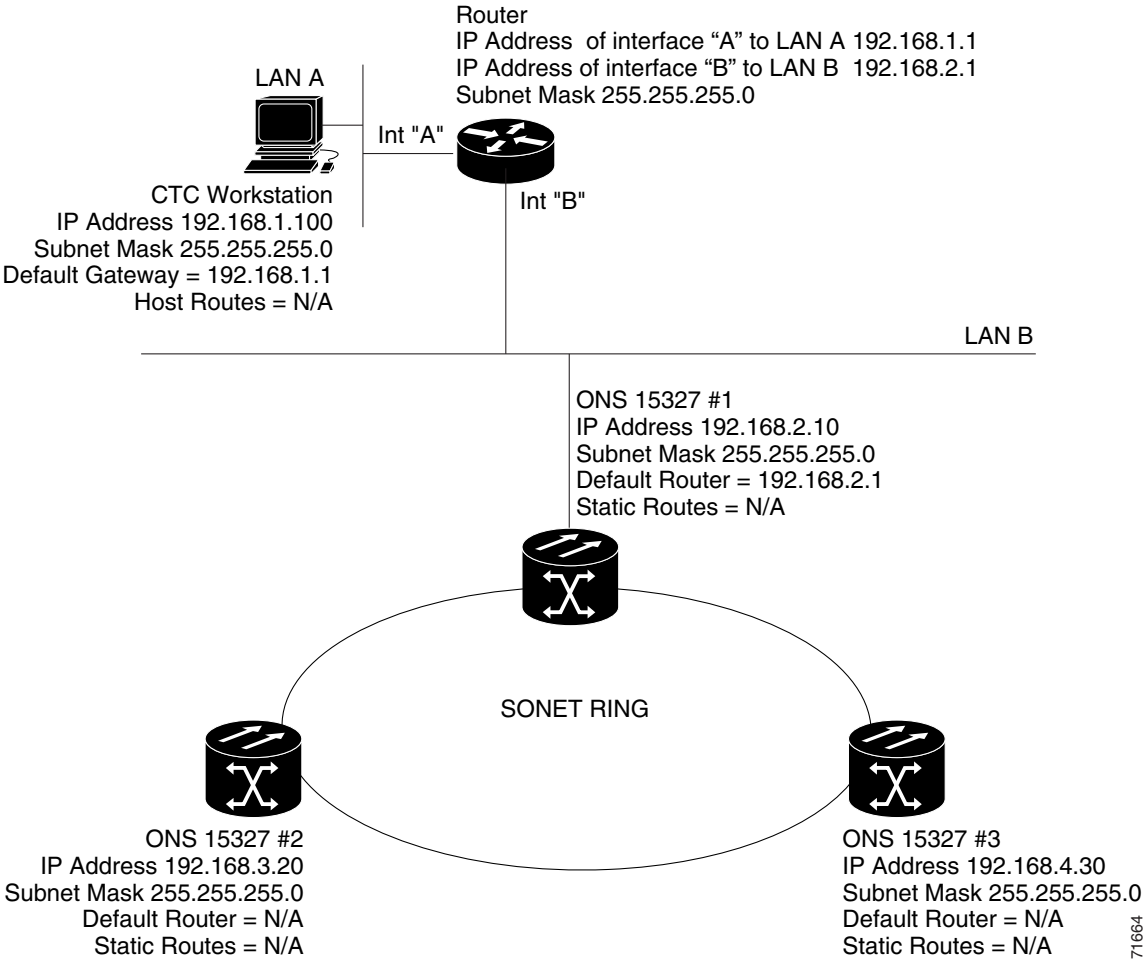
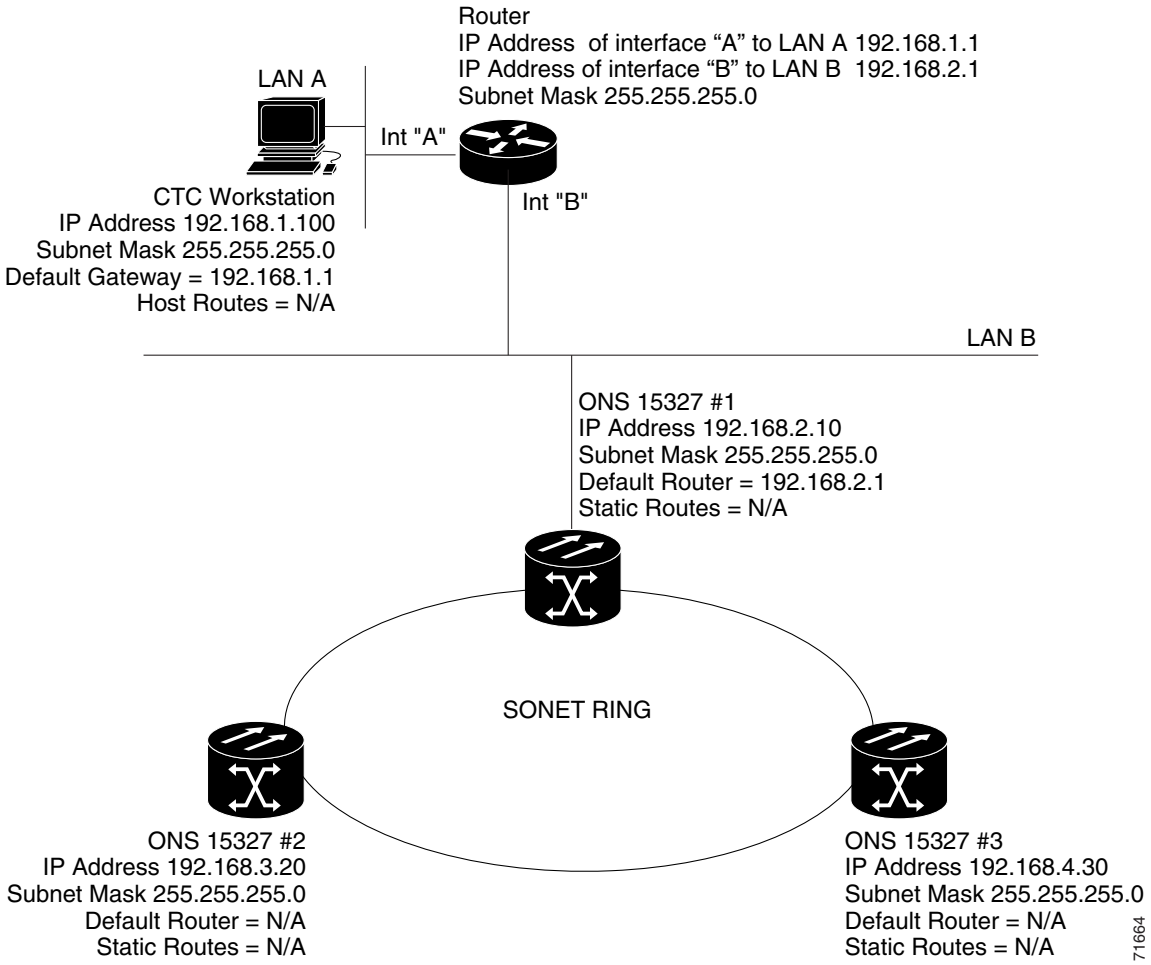


Figure 9-9 shows the same network without OSPF. Static routes must be manually added to the router for CTC computers on LAN A to communicate with Nodes #2 and #3 because these nodes reside on different subnets.

Figure 9-9 Scenario 6: OSPF Not Enabled



9.2.7 Scenario 7: Provisioning the ONS 15327 Proxy Server

The ONS 15327 proxy server is a set of functions that allows you to network ONS 15327s in environments where visibility and accessibility between ONS 15327s and CTC computers must be restricted. For example, you can set up a network so that field technicians and network operating center (NOC) personnel can both access the same ONS 15327s while preventing the field technicians from accessing the NOC LAN. To do this, one ONS 15327 is provisioned as a GNE and the other ONS 15327s are provisioned as end network elements (ENEs). The GNE tunnels connections between CTC computers and ENEs, which provide management capability while preventing access for non-ONS 15327 management purposes.

The ONS 15327 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 9-15 and Table 9-4 on page 9-16) depend on whether the packet arrives at the ONS 15327 DCC or at the Integrated Cross-Connect, Timing, and Control (XTC) card Ethernet interface.

- Processes Simple Network Timing Protocol (SNTP) and Network Timing Protocol (NTP) requests. Element ONS 15327 NEs can derive time-of-day information from an SNTP/NTP LAN server through the GNE.
- Process Simple Network Management Protocol Version 1 (SNMPv1) traps. The GNE receives SNMPv1 traps from the ENE and forwards them to all provisioned SNMPv1 trap destinations.

The ONS 15327 proxy server is provisioned using the Enable proxy server on port check box on the Provisioning > Network > General tab. If checked, the ONS 15327 serves as a proxy for connections between CTC clients and ONS 15327s that are DCC-connected to the proxy ONS 15327. 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. In addition, you can set the proxy server as an ENE or a GNE by selecting one of the following options:

Note If you launch CTC for 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.

- End Network Element (ENE)—If set as an ENE, the ONS 15327 neither installs nor advertises default or static routes. CTC computers can communicate with the ONS 15327 using the TCC2 craft port, but they cannot communicate directly with any other DCC-connected ONS 15327.

  In addition, firewall is enabled, which means that the node prevents IP traffic from being routed between the DCC and the LAN port. The ONS 15327 can communicate with machines connected to the LAN port or connected through the DCC. However, the DCC-connected machines cannot communicate with the LAN-connected machines, and the LAN-connected machines cannot communicate with the DCC-connected machines. A CTC client using the LAN to connect to the firewall-enabled node can use the proxy capability to manage the DCC-connected nodes that would otherwise be unreachable. A CTC client connected to a DCC-connected node can only manage other DCC-connected nodes and the firewall itself.
- Gateway Network Element (GNE)—If set as a GNE, the CTC computer is visible to other DCC-connected nodes and firewall is enabled.
- Proxy-only—If Proxy-only is selected, CTC cannot communicate with any other DCC-connected ONS 15327s and firewall is not enabled.

Figure 9-10 shows an ONS 15327 proxy server implementation. A GNE is connected to a central office LAN and to 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 ENEs. However, the craft technicians must be prevented from accessing or seeing the NOC or central office LANs.

In the example, the GNE is assigned an IP address within the central office LAN and is physically connected to the LAN through its LAN port. ENEs are assigned IP addresses that are outside the central office LAN and given private network IP addresses. If the 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 15327 Proxy Server with GNE and ENEs on the Same Subnet

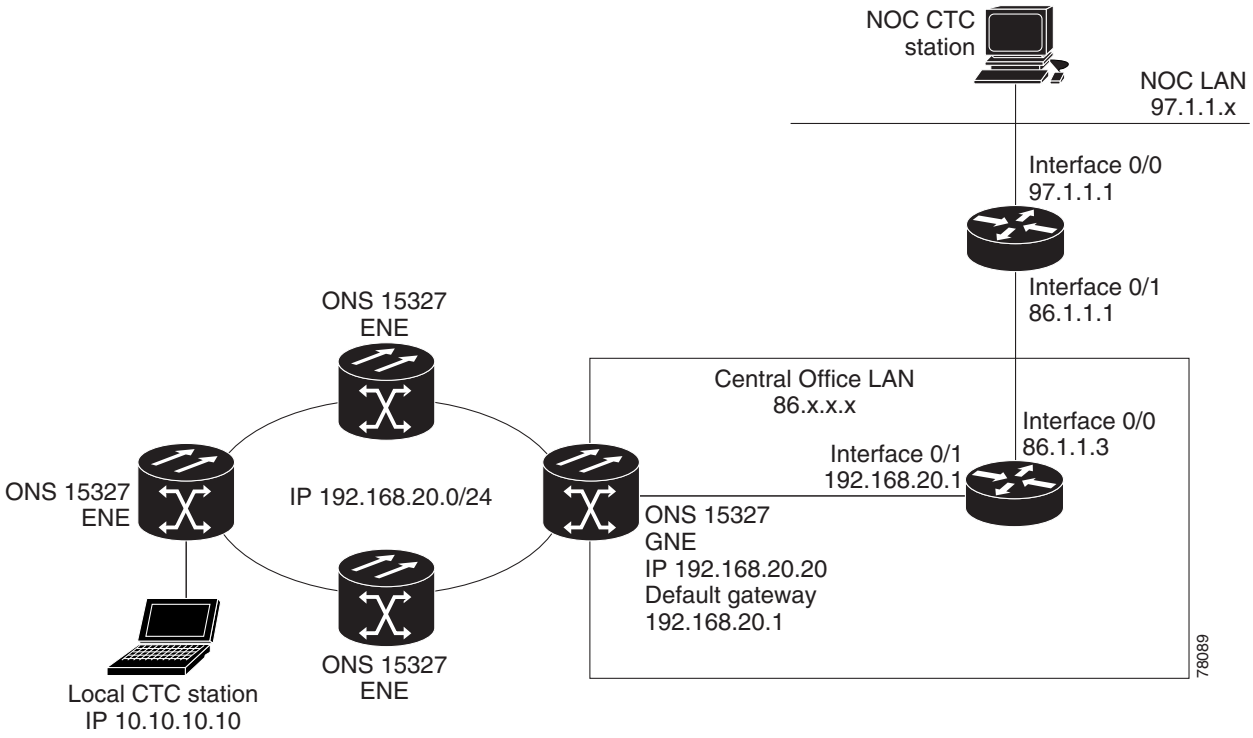


Table 9-2 shows recommended settings for ONS 15327 GNEs and ENEs in the configuration shown in Figure 9-10.

Table 9-2 ONS 15327 GNE and ENE Settings

Setting	ONS 15327 GNE	ONS 15327 ENE
Craft Access Only	Off	On
Enable Proxy	On	On
Enable Firewall	On	On
Ospf	Off	Off
Sntp Server (if used)	SNTP server IP address	Set to ONS 15327 GNE IP address
SNMP (if used)	SNMPv1 trap destinations	Set SNMPv1 trap destinations to ONS 15327 GNE

Figure 9-11 shows the same proxy server implementation with ONS 15327 ENEs on different subnets. In this example, ONS 15327 GNEs and ENEs are provisioned with the settings shown in Table 9-2.

Figure 9-11 Scenario 7: ONS 15327 Proxy Server with GNE and ENEs on Different Subnets

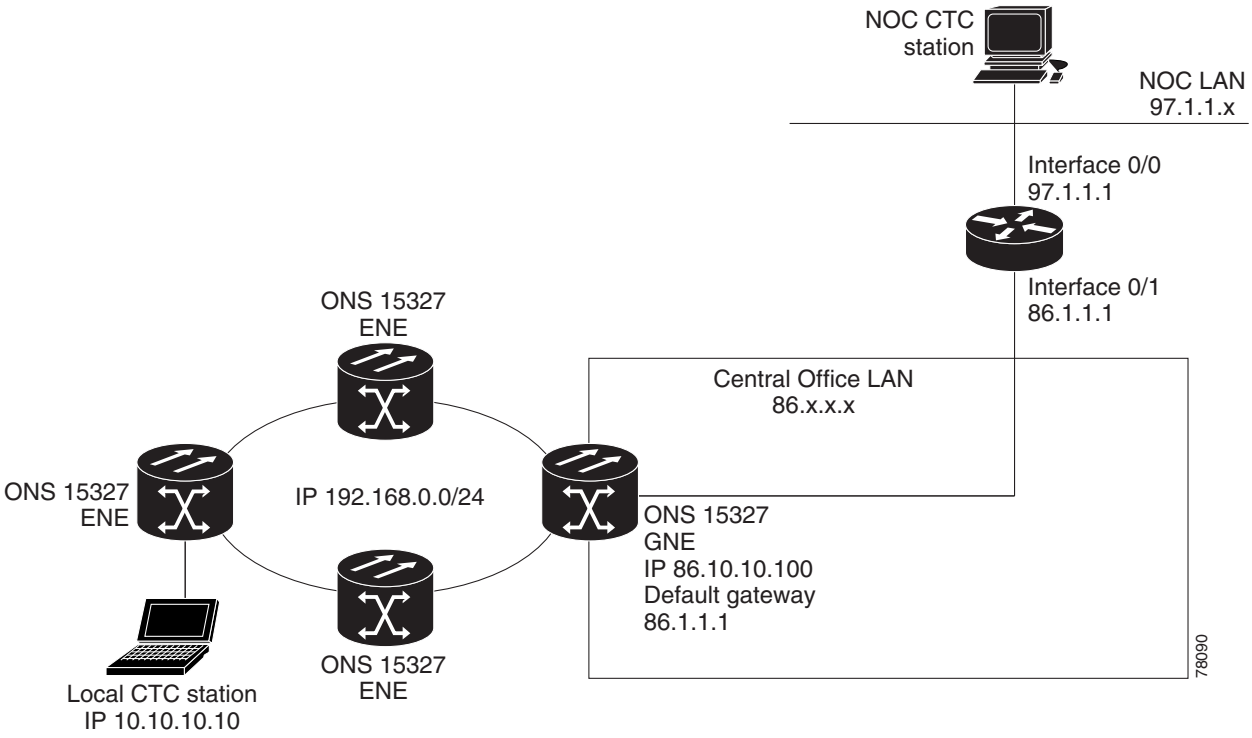


Figure 9-12 shows the implementation with ONS 15327 ENEs in multiple rings. In this example, ONS 15327 GNEs and ENEs are provisioned with the settings shown in Table 9-2.

Figure 9-12 Scenario 7: ONS 15327 Proxy Server with ENEs on Multiple Rings

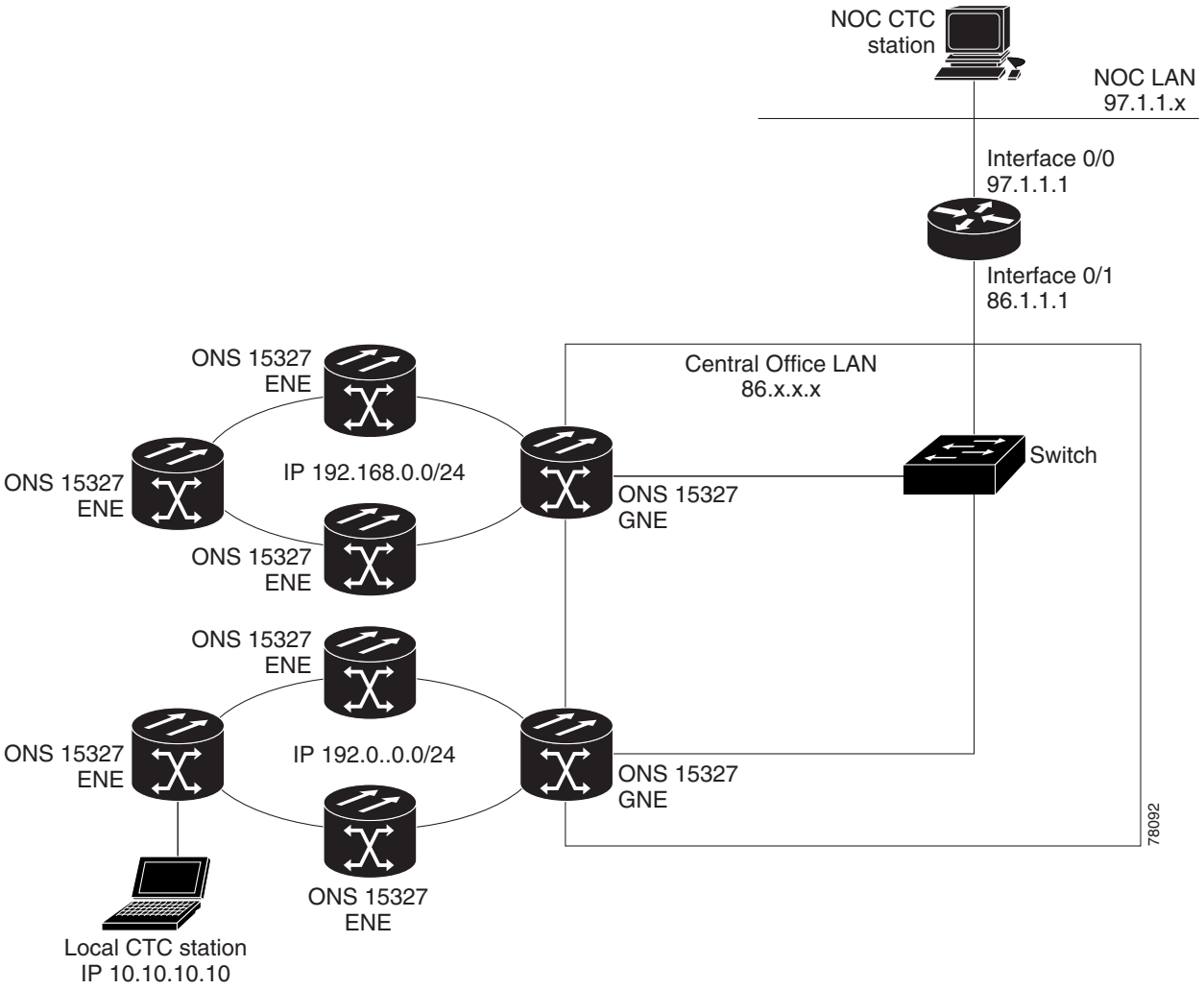


Table 9-3 shows the rules the ONS 15327 follows to filter packets when * is enabled.

Table 9-3 Proxy Server Firewall Filtering Rules

Packets arriving at:	Are accepted if the IP destination address is:
XTC Ethernet interface	• The ONS 15327 shelf itself • The ONS 15327's subnet broadcast address • Within the 224.0.0.0/8 network (reserved network used for standard multicast messages) • Subnet mask = 255.255.255.255
DCC interface	• The ONS 15327 itself • Any destination that is connected through another DCC interface • Within the 224.0.0.0/8 network

Table 9-4 shows additional rules that apply if the packet addressed to the ONS 15327 is discarded. Rejected packets are silently discarded.

Table 9-4 Proxy Server Firewall Filtering Rules When Packet Addressed to ONS 15327

Packets Arrive At	Accepted	Rejected
XTC Ethernet interface	• All User Datagram Protocol (UDP) packets except those in the Rejected column	• UDP packets addressed to the SNMP trap relay port (391)
DCC interface	• All UDP packets • All TCP packets except those in the Rejected column • OSPF packets • Internet Control Message Protocol (ICMP) packets	• TCP packets addressed to the Telnet port • TCP packets addressed to the proxy server port • All packets other than UDP, TCP, OSPF, ICMP

If you implement the proxy server, keep the following rules in mind:

1. All DCC-connected ONS 15327s on the same Ethernet segment must have the same Craft Access Only setting. Mixed values produce unpredictable results, and might leave some nodes unreachable through the shared Ethernet segment.
2. All DCC-connected ONS 15327s on the same Ethernet segment must have the same Enable Firewall setting. Mixed values produce unpredictable results. Some nodes might become unreachable.
3. If you check Enable Firewall, always check Enable Proxy. If Enable Proxy is unchecked, CTC is not able to see nodes on the DCC side of the ONS 15327.
4. If Craft Access Only is checked, check Enable Proxy. If Enable Proxy is not checked, CTC is not able to see nodes on the DCC side of the ONS 15327.

If nodes become unreachable in cases 1, 2, and 3, you can correct the setting by performing one of the following actions:

- Disconnect the craft computer from the unreachable ONS 15327. Connect to the ONS 15327 through another ONS 15327 in the network that has a DCC connection to the unreachable ONS 15327.
- Disconnect the Ethernet cable from the unreachable ONS 15327. Connect a CTC computer directly to the ONS 15327.

9.2.8 Scenario 8: Dual GNEs on a Subnet

The ONS 15327 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 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, both of which enhance CTC performance. Figure 9-13 shows a network with dual GNEs on the same subnet.

Figure 9-13 Scenario 8: Dual GNEs on the Same Subnet

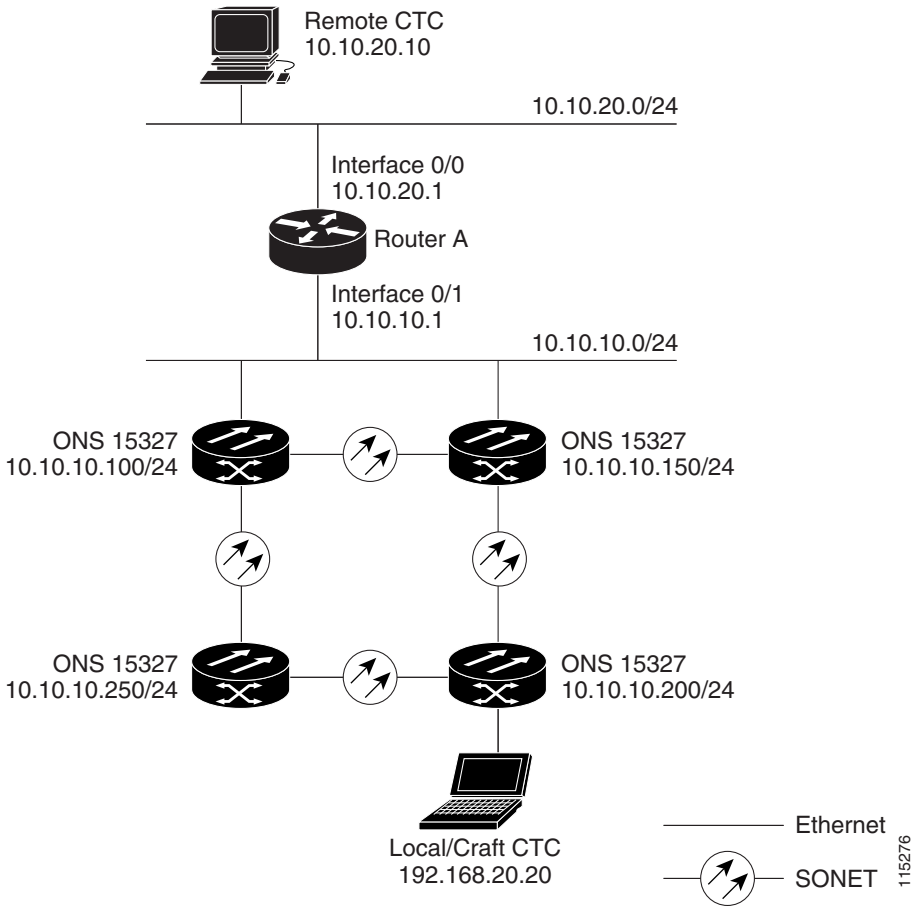
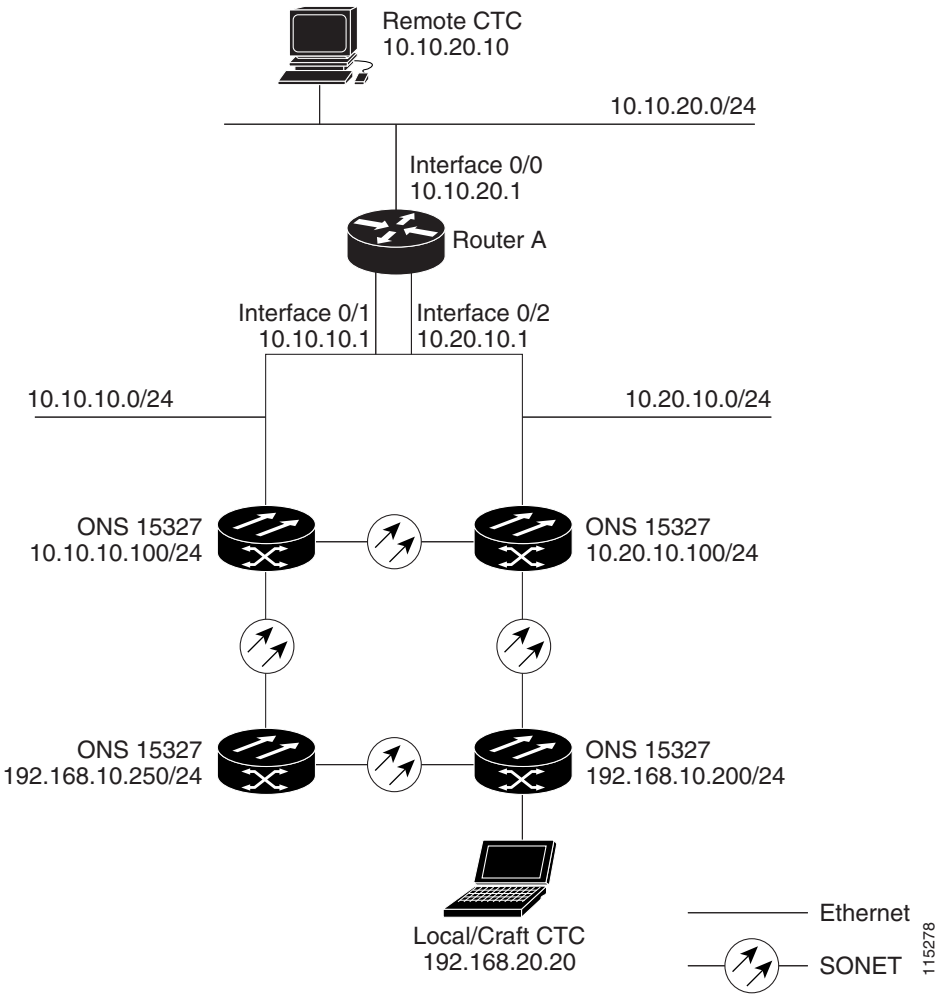


Figure 9-14 shows a network with dual GNEs on different subnets.

Figure 9-14 Scenario 8: Dual GNEs on Different Subnets



9.3 Provisionable Patchcords

A provisionable patchcord is a user-provisioned link that is advertised by OSPF throughout the network. Provisionable patchcords, also called virtual links, are needed if an ONS 15327 optical port is connected to an ONS 15454 transponder or muxponder client port provisioned in transparent mode.

Provisionable patchcords are required on both ends of a physical link. The provisioning at each end includes a local patchcord ID, slot/port information, remote IP address, and remote patchcord ID. Patchcords appear as dashed lines in CTC network view.

Table 9-5 lists the supported card combinations for ONS 15327 optical cards and the ONS 15454 transponder/muxponder cards used in a provisionable patchcord. For more information about the ONS 15454 transponder and muxponder cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Table 9-5 Client and Trunk Card Combinations in Provisionable Patchcords

	ONS 15454 Client Cards		
ONS 15327 Trunk Cards	**MXP_2.5G_10G/ TXP_MR_10G**	**TXP(P)_MR_2.5G**	**MXP_2.5G_10E/ TXP_MR_10E**
OC-3	—		—
OC-12	—	Yes	—
OC-48	Yes	Yes	Yes

Optical ports have the following requirements when used in a provisionable patchcord:

- An optical port connected to an ONS 15454 transponder/muxponder port requires Section DCC/Line DCC (SDCC/LDCC) termination.
- If the optical port is the protection port in a 1+1 protection group, the working port must have SDCC/LDCC termination provisioned.
- If the remote end of a patchcord is Y-cable protected, an optical port requires two patchcords.

9.4 Routing Table

ONS 15327 routing information is displayed on the Maintenance > Routing Table tabs. 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 the listed route has been used.
- Interface—Shows the ONS 15327 interface used to access the destination:
  - cpm0—The ONS 15327 Ethernet interface, that is, the RJ-45 jack and the LAN pin on the XTC card
  - pdcc0—An SDCC interface, that is, an OC-N trunk card identified as the SDCC termination
  - lo0—A loopback interface

Table 9-6 shows sample routing entries for an ONS 15327.

Table 9-6 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
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 is 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 is sent to this gateway.
- Interface (cpm0) indicates that the ONS 15327 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 a destination.
- 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 15327 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 SONET SDCC 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 IP address 172.20.214.93.
- Interface (pdcc0) indicates that a SONET SDCC interface is used to reach the gateway.

9.5 External Firewalls

Table 9-7 shows the ports that are used by the XTC.

Table 9-7 Ports Used by the XTC

Port	Function
0	Never used
21	FTP control
23	Telnet
80	HTTP
111	rpc (not used; but port is in use)
513	rlogin (not used; but port is in use)
=<1023	Default CTC listener ports
1080	Proxy server
2001-2017	I/O card Telnet
2018	DCC processor on active XTC
2361	TL1
3082	TL1
3083	TL1
5001	Bidirectional line switch ring (BLSR) server port
5002	BLSR client port
7200	SNMP input port
9100	EQM port
9101	EQM port 2
9401	TCC boot port
9999	Flash manager
57790	Default TCC listener port

The following access control list (ACL) examples show a firewall configuration when the proxy server gateway setting is not enabled. In the example, the CTC workstation address is 192.168.10.10 and the ONS 15327 address is 10.10.10.100. The firewall is attached to the GNE, so the inbound path is CTC to the GNE and the outbound path is from the GNE to CTC. The CTC 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 the 15327 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 the 15327 GNE (port 57790) ***
access-list 100 remark

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 15327 (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 15327 GNE to CTC ***
```

The following ACL examples show a firewall configuration when the proxy server gateway setting is enabled. As with the first example, the CTC workstation address is 192.168.10.10 and the ONS 15327 address is 10.10.10.100. The firewall is attached to the GNE, so the inbound path is CTC to the GNE and the outbound path is from the GNE to CTC. The CTC 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 the 15327 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 15327 GNE proxy server (port
1080) ***
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 from CTC to the 15327 GNE ***
access-list 101 remark *** Outbound ACL, NE -> CTC ***
access-list 101 remark
access-list 101 permit tcp host 10.10.10.100 eq 1080 host 192.168.10.10
access-list 101 remark *** allows alarms and other communications from the 15327 (proxy
server) 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 15327 GNE to CTC ***
```

9.6 Open GNE

The ONS 15327 can communicate with non-ONS nodes that do not support point-to-point protocol (PPP) vendor extensions or OSPF type 10 opaque 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 SDCC and LDCC 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 SDCC and LDCC 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 and Firewalls subtabs. 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 9-15 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 9-15 Proxy and Firewall Tunnels for Foreign Terminations

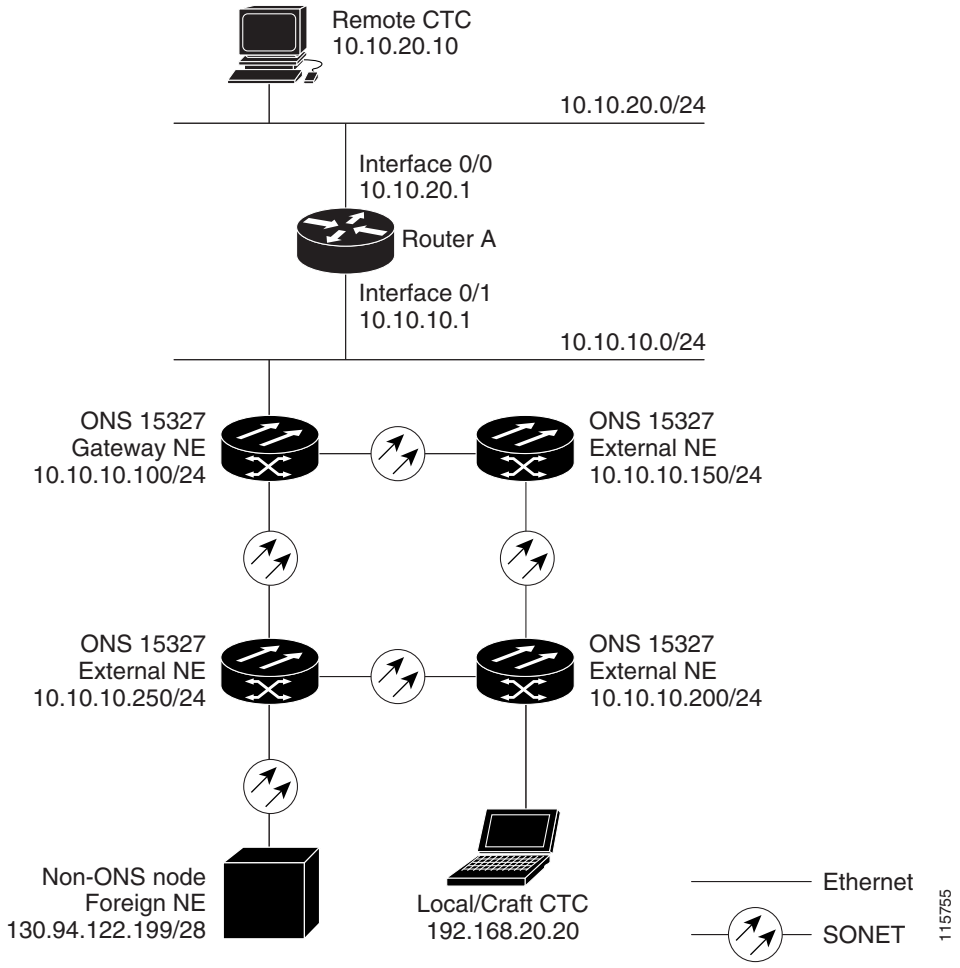
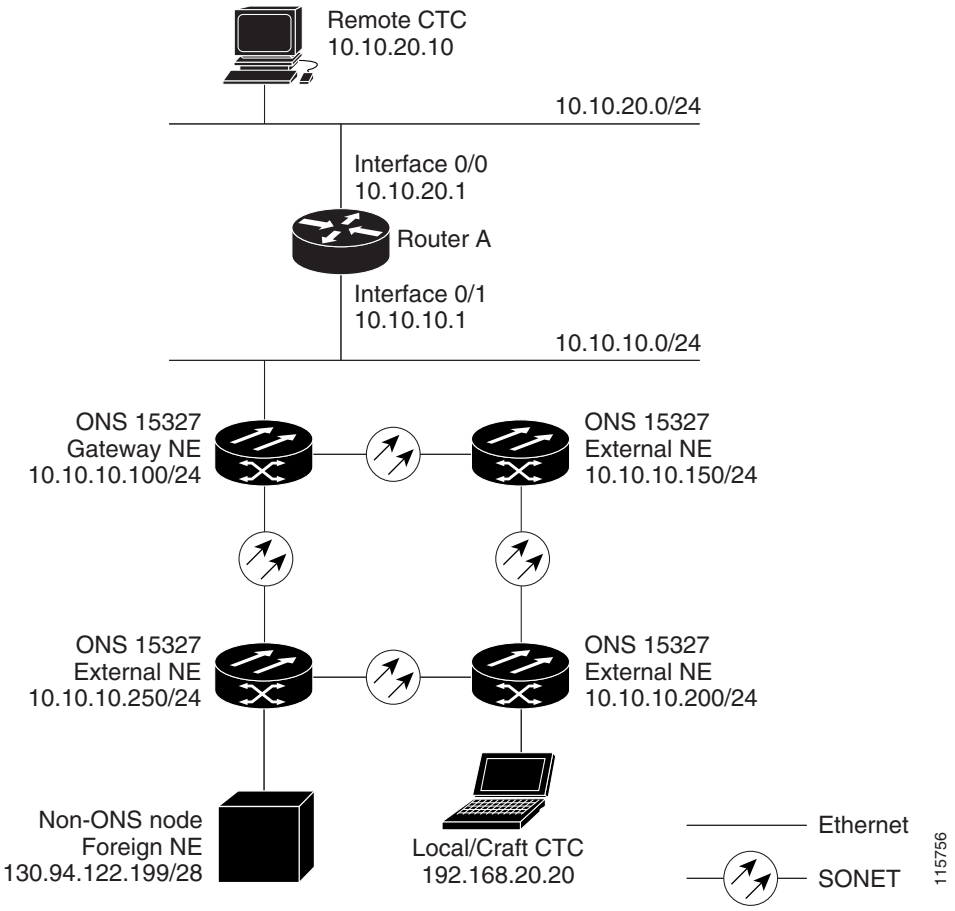


Figure 9-16 shows a remote node connected to an ENE Ethernet port. Proxy and firewall tunnels are useful in this example because the GNE would otherwise block IP access between the PC and foreign node. This configuration also requires a firewall tunnel on the ENE.

Figure 9-16 Foreign Node Connection to an ENE Ethernet Port



9.7 TCP/IP and OSI Networking

ONS 15327 DCN communication is based on the TCP/IP protocol suite. However, ONS 15327 nodes 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 9-8 shows the protocols that are involved when TCP/IP-based NEs are networked with OSI-based NEs.

Table 9-8 TCP/IP and OSI Protocols

OSI Model	IP Protocols	OSI Protocols		IP-OSI Tunnels
Layer 7 Application	• TL1 • FTP • HTTP • Telnet • IIOP	• TARP[1]	• TL1 (over OSI) • FTAM[2] • ACSE[3]	—
Layer 6 Presentation			• PST[4]	—
Layer 5 Session			• Session	—
Layer 4 Transport	• TCP • UDP		• TP (Transport) Class 4	• IP-over-CLNS[5] tunnels
Layer 3 Network	• IP • OSPF	• CLNP[6] • ES-IS[7] • IS-IS[8]		
Layer 2 Data link	• PPP	• PPP • LAP-D[9]		
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. PST = Presentation layer
5. CLNS = Connectionless Network Layer Service
6. CLNP = Connectionless Network Layer Protocol
7. ES-IS = End System-to-Intermediate System
8. IS-IS = Intermediate System-to-Intermediate System
9. LAP-D = Link Access Protocol on the D Channel

9.7.1 Point-to-Point Protocol

Point-to-Point (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 SDCC or LDCC. The SDCC or LDCC can be provisioned to support OSI over PPP.

9.7.2 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 15327 SDCC 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.

9.7.3 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 15327 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 9-9. 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 9-9 NSAP Fields

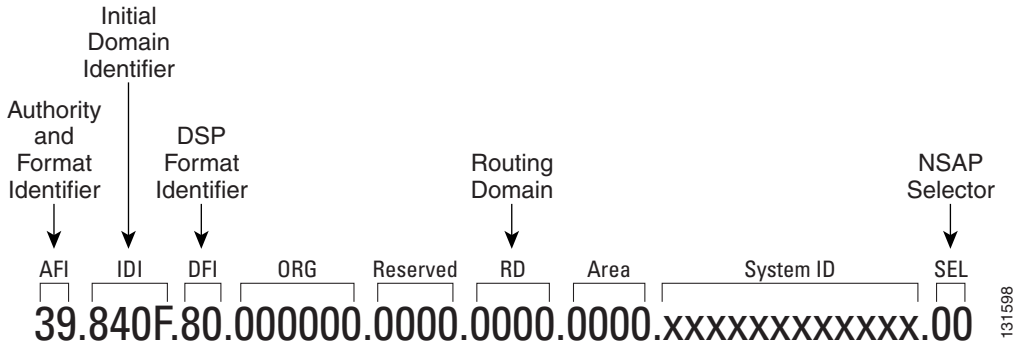
Field	Definition	Description
IDP		
AFI	Authority and format identifier	Specifies the NSAP address format. The initial value is 39 for the ISO-DCC address format.
IDI	Initial domain identifier	Specifies the country code. The initial value is 840F, the United States country code padded with an F.
DSP		
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 9-9 NSAP Fields (continued)

Field	Definition	Description
System	System identifier	The ONS 15327 system identifier is set to its IEEE 802.3 MAC address. Each ONS 15327 supports one OSI virtual router.
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 15327 include: • 00—Network Entity Title (NET). Used to exchange PDUs in the ES-IS and IS-IS routing exchange protocols. (See the "9.7.4.1 End System-to-Intermediate System Protocol" section on page 9-30, and "9.7.4.2 Intermediate System-to-Intermediate System" section on page 9-30.) • 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 9-17 shows the ISO-DCC NSAP address with the default values delivered with the ONS 15327. The System ID is automatically populated with the node MAC address.

Figure 9-17 ISO-DCC NSAP Address



The ONS 15327 main NSAP address is shown on the node view Provisioning > OSI > Main Setup subtab. This address is also the Router 1 primary manual area address, which is viewed and edited on Provisioning > OSI > Routers subtab. See the "9.7.6 OSI Virtual Routers" section on page 9-34 for information about the OSI router and manual area addresses in CTC.

9.7.4 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.

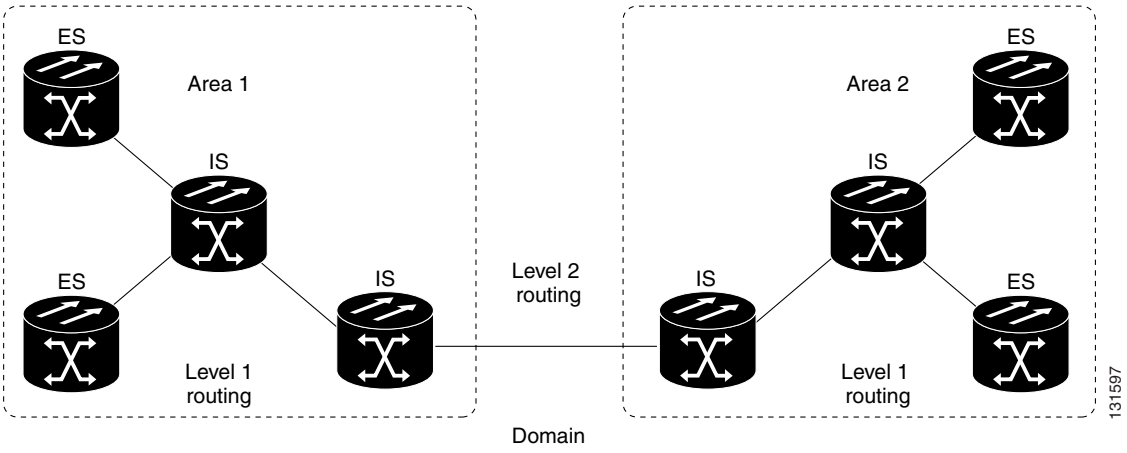
An IS composes intermediate system hello (ISH) messages to announce its configuration information to ISs and ESs that are connected to the same broadcast subnetwork. Like the ESHs, the ISH contains the addressing information for the IS (the NET and the subnetwork point-of-attachment address [SNPA]) and 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 9-18 shows an example of Level 1 and Level 2 routing.

Note The ONS 15327 does not support Level 1/Level 2 routing. Level 1/Level 2 routing is supported by the ONS 15454, ONS 15454 SDH, and the ONS 15600.

Figure 9-18 Level 1 and Level 2 OSI Routing



When you provision an ONS 15327 for a network with NEs that use both the TCP/IP and OSI protocol stacks, you will provision it as one of the following:

- End System—The ONS 15327 performs OSI ES functions and relies upon an IS for communication with nodes that reside within its OSI area.
- Intermediate System Level 1—The ONS 15327 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.

9.7.4.1 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.

9.7.4.2 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 15327. 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.

9.7.5 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 9-9 on page 9-27).

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 9-10.

Table 9-10 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 9-11, are defined.
TID Target Length	tar-tln	1	The number of octets that are in the tar-ttg field.
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.

Table 9-10 TARP PDU Fields (continued)

Field	Abbreviation	Size (bytes)	Description
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 9-11 shows the TARP PDUs types that govern TARP interaction and routing.

Table 9-11 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 a 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.

9.7.5.1 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 subtab. The TDC subtab 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 9-12, control TARP processing.

Table 9-12 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 9-13 shows the main TARP processes and the general sequence of events that occurs in each process.

Table 9-13 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. 2. If no match is found, a TARP Type 1 PDU is generated and Timer T1 is started. 3. If Timer T1 expires before a match if found, a Type 2 PDU is generated and Timer T2 is started. 4. If Timer T2 expires before a match is found, Timer T4 is started. 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.

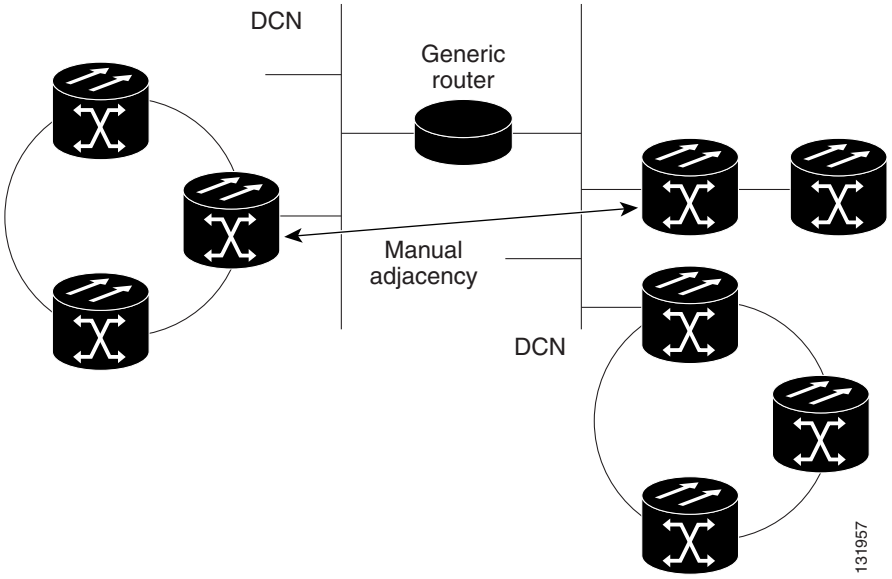
9.7.5.2 TARP Loop Detection Buffer

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 Cisco ONS 15327 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.

9.7.5.3 Manual TARP Adjacencies

TARP adjacencies can be manually provisioned in networks where ONS 15327s must communicate across routers or non-SONET NEs that lack TARP capability. In CTC, manual TARP adjacencies are provisioned on the node view Provisioning > OSI > TARP > MAT (Manual Area Table) subtab. The manual adjacency causes a TARP request to hop through the general router or non-SONET NE, as shown in Figure 9-19.

Figure 9-19 Manual TARP Adjacencies



9.7.5.4 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.

9.7.6 OSI Virtual Routers

The ONS 15327 supports one OSI virtual router. The router is provisioned on the Provisioning > OSI > Routers tab. The router has an editable manual area address and a unique NSAP System ID that is set to the node MAC address. The router can be enabled and connected to different OSI routing areas. The Router 1 manual area address and System ID create the NSAP address assigned to the node's TID. Router 1 supports OSI TARP and tunneling functions. These include:

- TARP data cache
- IP-over-CLNS tunnels
- LAN subnet

In addition to the 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.

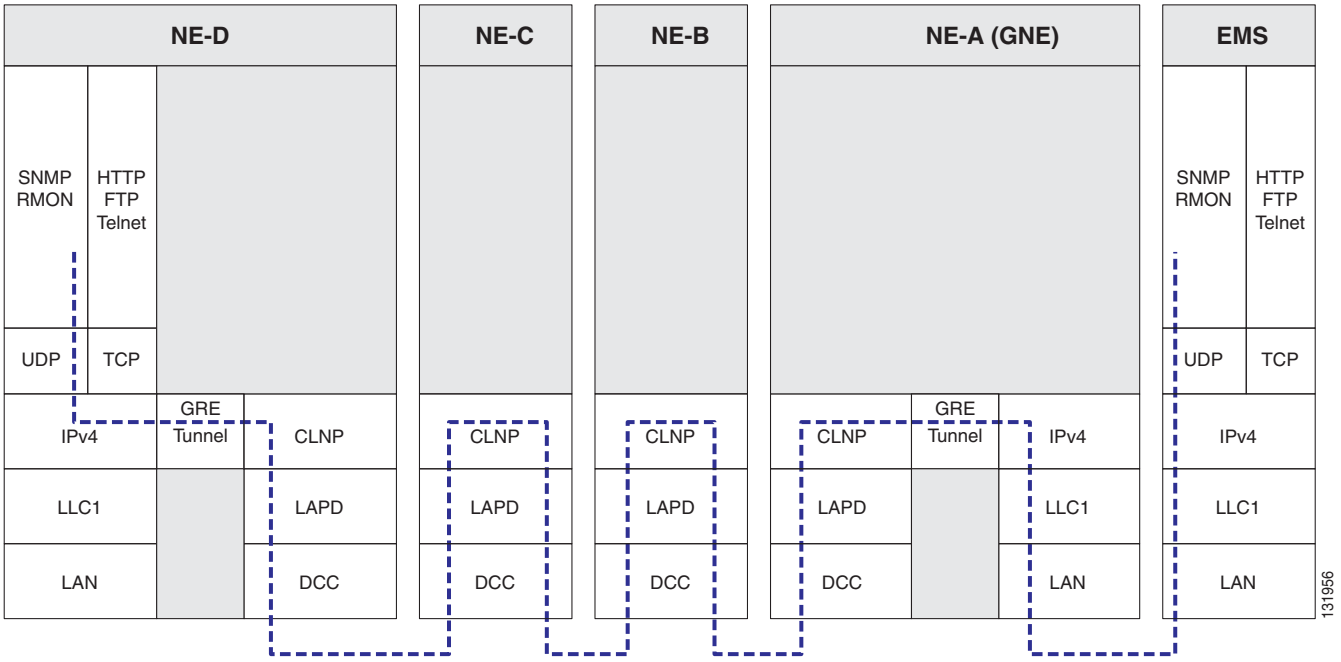
9.7.7 IP-over-CLNS Tunnels

IP-over-CLNS tunnels are used to encapsulate IP for transport across OSI NEs. The ONS 15327 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 9-20 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 9-20 IP-over-CLNS Tunnel Flow



9.7.7.1 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 Node" chapter in the *Cisco ONS 15327 Procedure 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 Cisco 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*.

9.7.7.2 IP Over CLNS Tunnel Scenario 1: ONS Node to Other Vendor GNE

Figure 9-21 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) SDCC and a GRE tunnel are created between the ONS NE 1 to the other vender GNE.

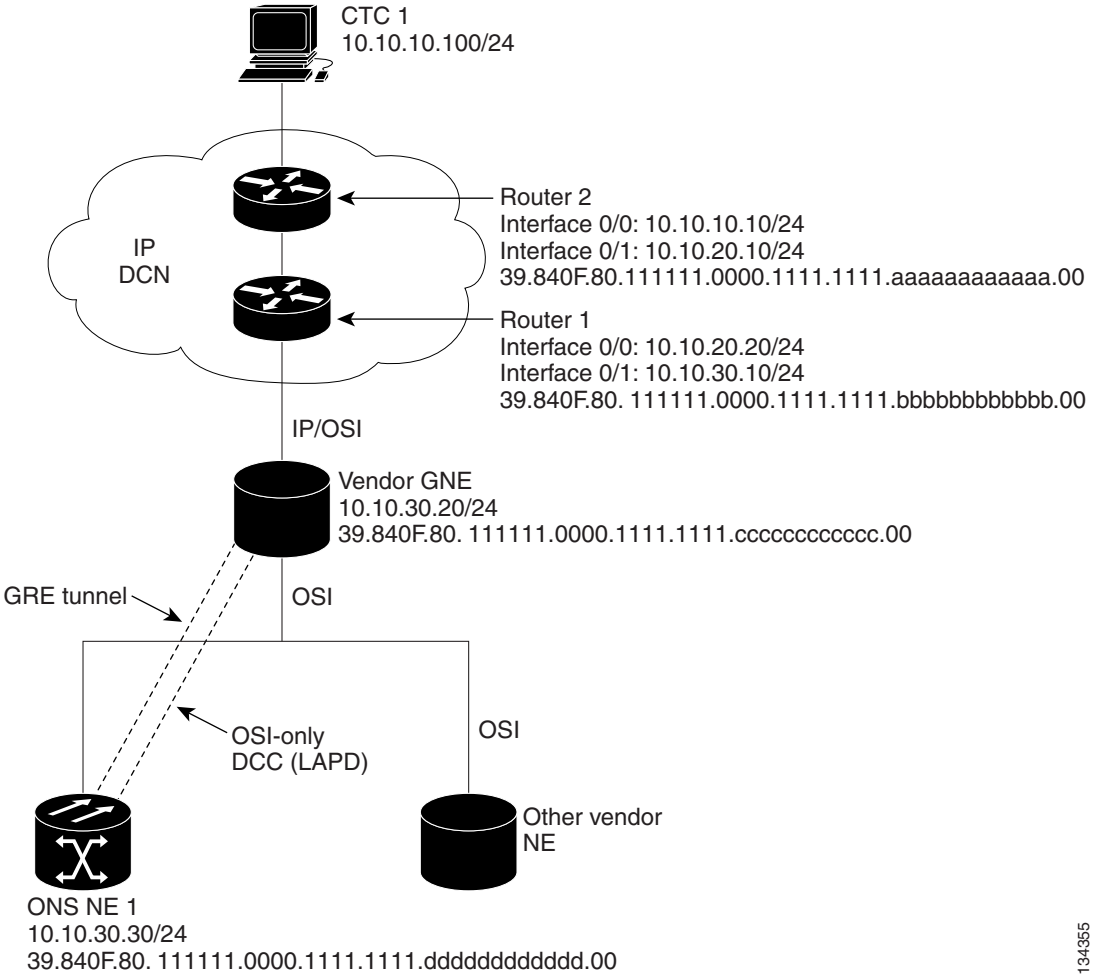
IP-over-CLNS tunnel on the ONS NE 1:

- 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.ccccccccccc.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.ddddddddddd.00 (ONS NE 1)
- Metric: 110
- Tunnel Type: GRE

Figure 9-21 IP Over CLNS Tunnel Scenario 1: ONS NE to Other Vender GNE



9.7.7.3 IP Over CLNS Tunnel Scenario 2: ONS Node to Router

Figure 9-22 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) SDCC 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.

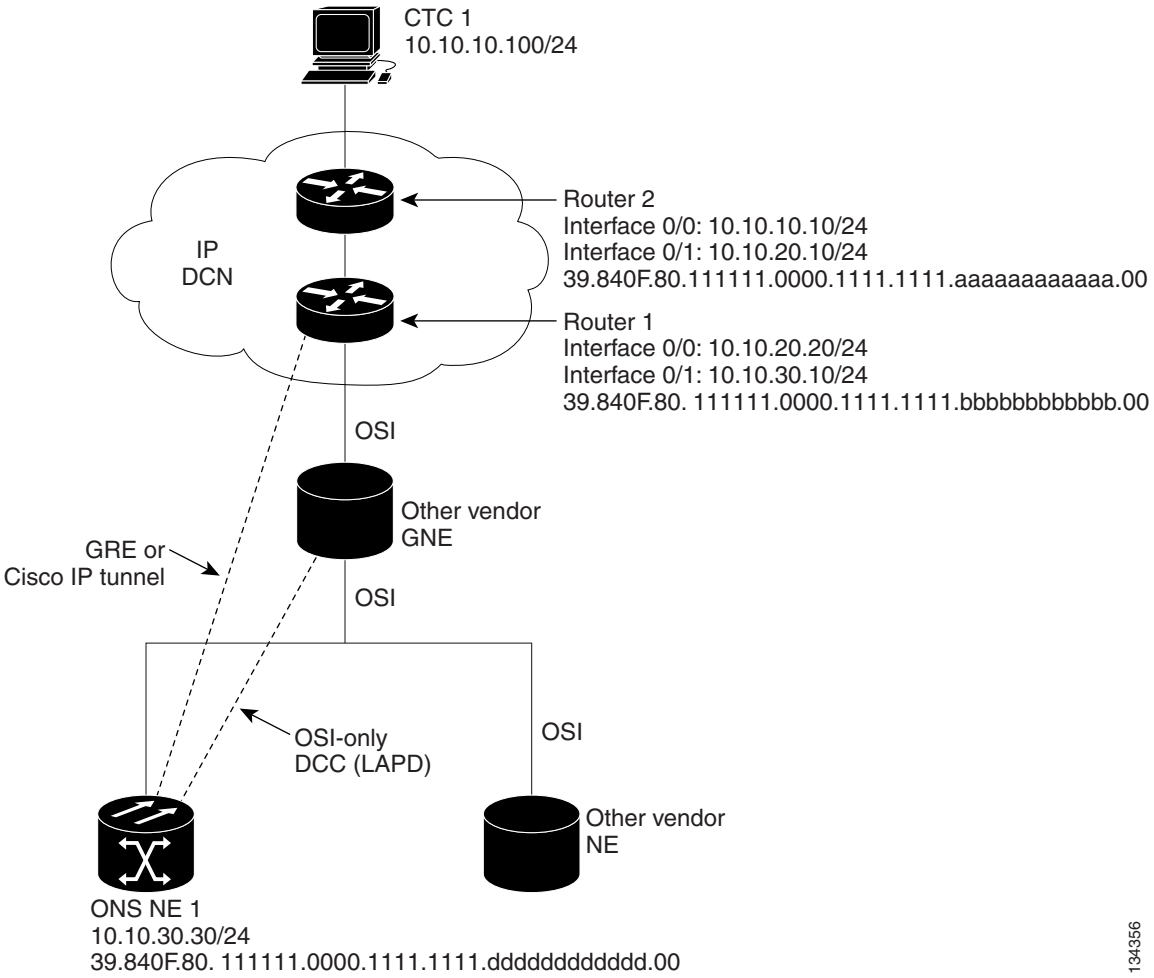
IP-over-CLNS tunnel on ONS NE 1:

- 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.ddddddddddd.00
interface Ethernet0/1
    clns router isis
router isis
    net 39.840F.80.1111.0000.1111.1111.bbbbbbbbbbbb.00
```

Figure 9-22 IP Over CLNS Tunnel Scenario 2: ONS Node to Router



9.7.7.4 IP Over CLNS Tunnel Scenario 3: ONS Node to Router Across an OSI DCN

Figure 9-23 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) SDCC 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.

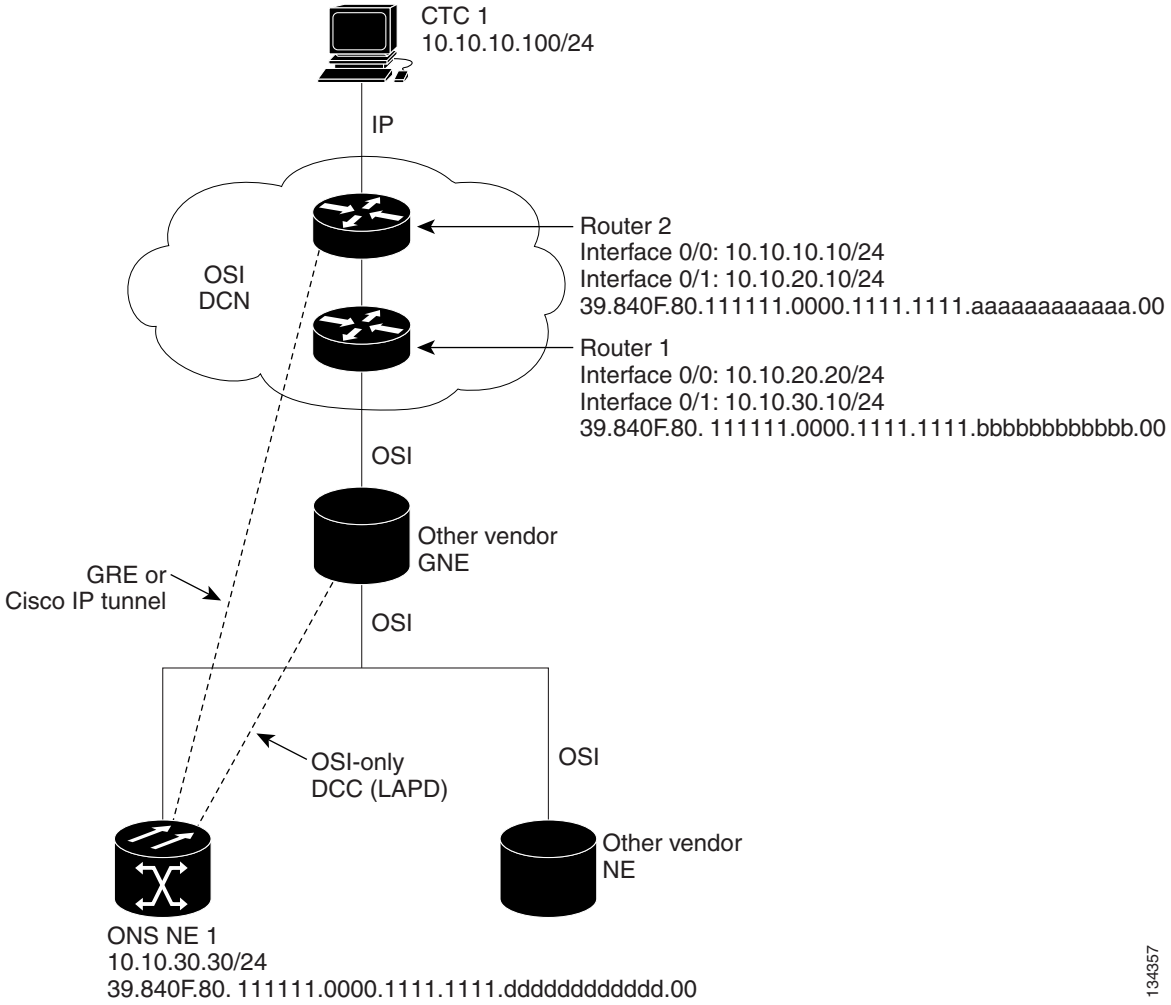
IP-over-CLNS tunnel on ONS NE 1:

- 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.ddddddddddd.00
interface Ethernet0/1
    clns router isis
router isis
    net 39.840F.80.1111.0000.1111.1111.aaaaaaaaaaa.00
```

Figure 9-23 IP Over CLNS Tunnel Scenario 3: ONS Node to Router Across an OSI DCN



9.7.8 Provisioning OSI in CTC

Table 9-15 shows the OSI actions that are performed from the node view Provisioning tab. Refer to the *Cisco ONS 15327 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. • Change OSI routing mode. • Change LSP buffers.
OSI > TARP > Config	Configure the TARP parameters: • PDU L1/L2 propagation and origination. • TARP data cache and loop detection buffer. • LAN storm suppression. • Type 4 PDU on startup. • 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. • Add, delete, and edit manual area addresses.
OSI > Routers > Subnets	Edit SDCC, LDCC, and LAN subnets that are provisioned for OSI.
OSI > Tunnels	Add, delete, and edit Cisco and IP-over-CLNS tunnels.
Comm Channels > SDCC	• Add OSI configuration to an SDCC. • Choose the data link layer protocol, PPP or LAP-D.
Comm Channels > LDCC	• Add OSI configuration to an SDCC.

Table 9-15 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. • Perform TID to NSAP resolutions. • Flush the TDC.

CHAPTER 10

Alarm Monitoring and Management

This chapter describes Cisco Transport Controller (CTC) alarm management. To troubleshoot specific alarms, refer to the *Cisco ONS 15327 Troubleshooting Guide*. Chapter topics include:

10.1 Overview

CTC detects and reports SONET alarms generated by the Cisco ONS 15327 and the larger SONET network. You can use CTC to monitor and manage alarms at the card, node, or network level. Default alarm severities conform to the Telcordia GR-253 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 15327 Troubleshooting Guide.*

Note ONS 15327 alarms can also be monitored and managed through Transaction Language One (TL1) or a network management system (NMS).

10.2 Viewing Alarms

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 with Telcordia GR-253. 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 the LOF and replaces it.

In Release 5.0, the Path Width column on the Alarms and Conditions tabs will expand upon alarmed object information contained in the TL1 access identifier (AID) string (such as “STS-4-1-3”) by giving the number of STSs contained in the alarmed path. For example, the Path Width will tell you whether a Critical alarm applies to a synchronous transport signal 1 (STS1) or an STS48c. The column reports the width as a 1, 3, 6, 12, 48, etc. as appropriate, understood to be “STS-*n*.”

Table 10-1 lists the column headings and the information recorded in each column.

Table 10-1 Alarms Column Descriptions

Column	Information Recorded
New	Indicates a new alarm. To change this status, click either the Synchronize button or the Delete Cleared Alarms button.
Date	Date and time of the alarm.
Node	Node where the alarm occurred (appears only in network view).
Object	TL1 access identifier (AID) for the alarmed object. For an STSmon or VTmon, this is the monitored STS or VT object, which is explained in Table 10-3 on page 10-3.
Eqpt Type	Card type in this slot.
Slot	Slot where the alarm occurred (appears only in network and node view).
Port	Port where the alarm is raised. For STSTerm and VTTerm, the port refers to the upstream card it is partnered with.
Path Width	Indicates how many STSs are contained in the alarmed path. This information complements the alarm object notation, which is explained in Table 10-3.
Sev	Severity level: CR (Critical), MJ (Major), MN (Major), NA (Not Alarmed), NR (Not Reported).
ST	Status: R (raised), C (clear).
SA	When checked, indicates a service-affecting alarm.
Cond	The error message/alarm name. These names are alphabetically defined in the “Alarm Troubleshooting” chapter of the *Cisco ONS 15327 Troubleshooting Guide.*
Description	Description of the alarm.
Num	Num (number) is the quantity of alarm messages received, and is incremented automatically as alarms occur to display the current total of received error messages.
Ref	Ref (reference) is a unique identification number assigned to each alarm to reference a specific alarm message that is displayed.

Table 10-2 lists the color codes for alarm and condition severities. In addition to the severities listed in the table, CTC alarm profiles list inherited (I) and unset (U) severities. These are only listed in the network view Provisioning > Alarm Profiles tab and are not currently implemented.

Table 10-2 Color Codes for Alarm and Condition Severities

Color	Description
Red	Raised Critical (CR) alarm
Orange	Raised Major (MJ) alarm
Yellow	Raised Minor (MN) alarm
Magenta	Raised Not Alarmed (NA) condition
Blue	Raised Not Reported (NR) condition
White	Cleared (C) alarm or condition

Note Major and Minor alarms may 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.

In network view, CTC identifies STS and VT alarm objects using a TL1-type AID, as shown in Table 10-3.

Table 10-3 STS and Alarm Object Identification

Object	STS or VT AID	Port No.
MON object	STS-<Slot>-<Port>-STS For example, STS-6-1-6 VT1-<Slot>-<Port>-<STS>-<VT Group>-<VT> For example, VT1-6-1-6-1-1	Port=1
TERM object	STS-<Upstream Slot>-<Port>-<STS> For example, STS-6-3-6 VT1-<Upstream Slot>-<Port>-<STS>-<VT Group>-<VT> For example, VT1-6-3-6-1-1	Port=1

10.2.1 Viewing Alarms With Each Node's Time Zone

By default, alarms and conditions are displayed with the time stamp of the CTC workstation where you are viewing them. You can set the node to report alarms (and conditions) using the time zone where the node is located by clicking Edit > Preferences, and then clicking the Display Events Using Each Node's Timezone check box.

10.2.2 Controlling Alarm Display

You can control the display of the alarms shown on the Alarms window. Table 10-4 shows the actions you can perform in the Alarms window.

Table 10-4 Alarm Display

Button/Check Box/Tool	Action
Filter button	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 display 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 button	Updates the alarm display. Although CTC displays alarms in real time, the Synchronize button allows you to verify the alarm display. This is particularly useful during provisioning or troubleshooting.

Table 10-4 Alarm Display (continued)

Button/Check Box/Tool	Action
Delete Cleared Alarms button	Deletes alarms that have been cleared.
AutoDelete Cleared Alarms check box	If checked, CTC automatically deletes cleared alarms.
Filter tool	Enables or disables alarm filtering in the card, node, or network view. When enabled or disabled, this state applies to other views for that node and for all other nodes in the network. For example, if the Filter tool is enabled in the node (default login) view Alarms window, the network view Alarms window and card view Alarms window also show the tool enabled. All other nodes in the network also show the tool enabled.

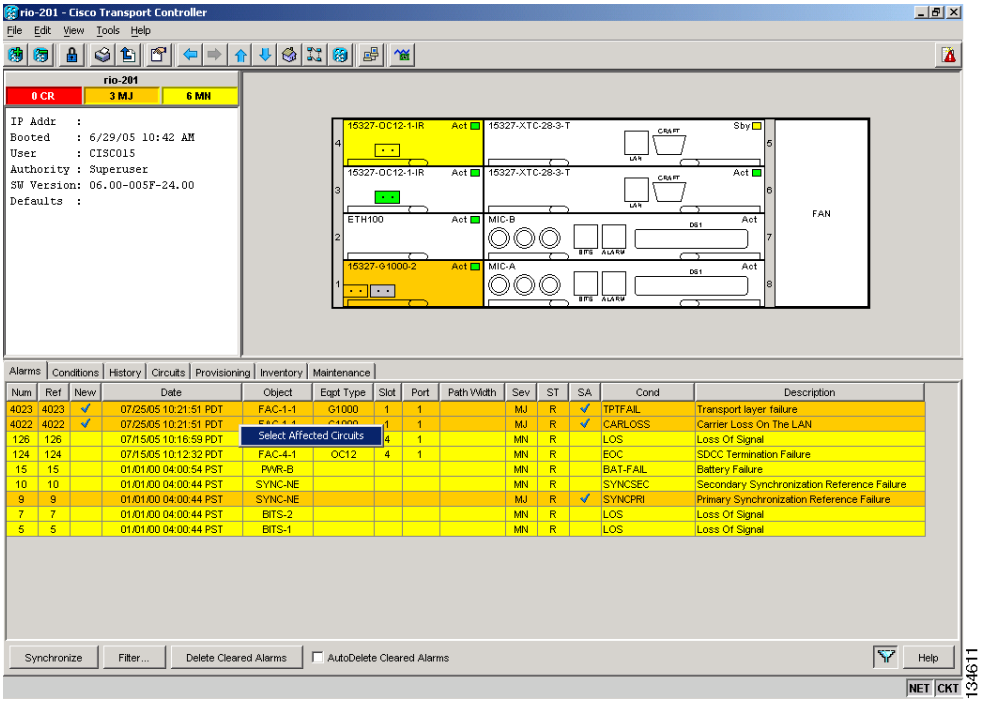
10.2.3 Filtering Alarms

The alarm display can be filtered to prevent display of alarms with certain severities or alarms that occurred between certain dates. You can set the filtering parameters by clicking the Filter button at the bottom-left of the Alarms window. You can turn the filter on or off by clicking the Filter tool 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 keeps the filter active the next time you log in.

10.2.4 Viewing Alarm-Affected Circuits

A user can view which ONS 15327 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 10-1). When the user selects the Select Affected Circuits option, the Circuits window appears to show the circuits that are affected by the alarm.

Figure 10-1 Select Affected Circuits Option



10.2.5 Conditions Tab

The Conditions window displays retrieved fault conditions. A condition is a fault or status detected by ONS 15327 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 15327.

The Conditions window shows all conditions that occur, including those that are superseded. 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 (even though LOS supersedes LOF). Having all conditions visible can be helpful when troubleshooting the ONS 15327. 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 by checking a check box in the window.

Fault conditions include reported alarms and Not Reported or Not Alarmed conditions. Refer to the trouble notifications information in the *Cisco ONS 15327 Troubleshooting Guide* for more information about alarm and condition classifications.

10.2.6 Controlling the Conditions Display

You can control the display of the conditions on the Conditions window. Table 10-5 shows the actions you can perform in the window.

Table 10-5 Conditions Display

Button	Action
Retrieve	Retrieves the current set of all existing fault conditions, as maintained by the alarm manager, from the ONS 15327.
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 button on the lower-right of the window that allows you to enable or disable the filter feature.

10.2.6.1 Retrieving and Displaying Conditions

The current set of all existing conditions maintained by the alarm manager can be seen when you click the Retrieve button. The set of conditions retrieved is relative to the view. For example, if you click the button while displaying the node view, node-specific conditions are displayed. If you click the button while displaying the network view, all conditions for the network (including ONS 15327 nodes and other connected nodes) are displayed, and the card view shows only card-specific conditions.

You can also set a node to display conditions using the time zone where the node is located, rather than the time zone of the PC where they are being viewed. See the "10.2.1 Viewing Alarms With Each Node's Time Zone" section on page 10-3 for more information.

10.2.6.2 Conditions Column Descriptions

Table 10-6 lists the Conditions window column headings and the information recorded in each column.

Table 10-6 Conditions Column Description

Column	Information Recorded
New	A new condition.
Date	Date and time of the condition.
Object	TL1 AID for the condition object. For an STSmon or VTmon, the object.
Eqpt Type	Card type in this slot.
Slot	Slot where the condition occurred (appears only in network and node view).
Port	Port where the condition occurred. For STSTerm and VTTerm, the port refers to the upstream card it is partnered with.
Sev[1]	Severity level: Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR).
SA	A service-affecting condition (when checked)
Cond	The error message/alarm name; these names are alphabetically defined in the *Cisco ONS 15327 Troubleshooting Guide*.

1. All alarms, their severities, and service-affecting status are also displayed in the Conditions tab unless you choose to filter the alarm from display using the Filter button.

10.2.6.3 Filtering Conditions

The condition display can be filtered to prevent display of conditions (including alarms) with certain severities or that occurred between certain dates. You can set the filtering parameters by clicking the Filter button at the bottom-left of the Conditions window. You can turn the filter on or off by clicking the Filter tool 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 keeps the filter active the next time your user ID is activated.

10.2.7 Viewing History

The History window displays historic alarm or condition data for the node or for your login session. You can chose to display only alarm history, only events, or both by checking check boxes in the History > Node window. You can view network-level alarm and condition history, such as for circuits, at that level. At the node level, you can see all port (facility), card, STS, and system-level history entries. For example, protection-switching events or performance-monitoring threshold crossings appear here. If you double-click a card, you can view all port, card, and STS alarm or condition history that directly affects the card.

The ONS 15327 can store up to 640 Critical alarm messages, 640 Major alarm messages, 640 Minor alarm messages, and 640 condition messages. When any of these limits is reached, the ONS 15327 discards the oldest events in that category.

Note In the Preference dialog box General tab, the Maximum History Entries value only applies to the Session window.

Different views of CTC display different kinds of history:

- The History > Session window is shown in network view, node view, and card view. It shows alarms and conditions that occurred during the current user CTC session.
- The History > Node window is only shown in node view. It shows the alarms and conditions that occurred on the node since CTC software was operated on the node.
- The History > Card window is only shown in card view. It shows the alarms and conditions that occurred on the card since CTC software was installed on the node.

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.

If you check the History window Alarms check box, you display the node history of alarms. If you check the Events check box, you display the node history of Not Alarmed and transient events (conditions). If you check both check boxes, you retrieve node history for both.

10.2.7.1 History Column Descriptions

Table 10-7 lists the History window column headings and the information recorded in each column.

Table 10-7 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 condition.
Object	TL1 AID for the condition object. For an STSmon or VTmon, the object.
Sev	Severity level: Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR).
Eqpt Type	Card type in this slot (only displays in network view and node view).
ST	Status: raised (R), cleared (C), or transient (T).
Description	Description of the condition.
Port	Port where the condition occurred. For STSTerm and VTTerm, the port refers to the upstream card it is partnered with.
Cond	Condition name.
Slot	Slot where the condition occurred (only displays in network view and node view).
SA	A service-affecting alarm (when checked).

10.2.7.2 Retrieving and Displaying Alarm and Condition History

You can retrieve and view the history of alarms and conditions, as well as transients (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).

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 > Node window, and the history of alarms, conditions, and transients that have occurred on the node during your login session in the History > Session window. In the card history window, after 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, but you cannot filter out Not Reported conditions or transients.

10.3 Alarm Severities

ONS 15327 alarm severities follow the Telcordia GR-253 standard, so a condition may be alarmed (at a severity of Critical [CR], Major [MJ], or Minor [MN]), Not Alarmed (NA), or Not Reported (NR). These severities are reported in the CTC software Alarms, Conditions, and History windows at all levels: network, shelf, and card.

ONS equipment provides a standard profile named Default that lists all alarms and conditions with severity settings based on Telcordia GR-253 and other standards, but users can create their own profiles with different settings for some or all conditions and apply these wherever desired. (See the "10.4 Alarm Profiles" section on page 10-9.) For example, in a custom alarm profile, the default severity of a carrier loss (CARLOSS) alarm on an Ethernet port could be changed from Major to Critical. The profile allows setting to Not Reported or Not Alarmed, as well as the three alarmed severities.

Critical and Major severities are only used for service-affecting alarms. If a condition is set as Critical or Major by profile, it will raise as Minor alarm in the following situations:

- In a protection group, if the alarm is on a standby entity (side not carrying traffic)
- If the alarmed entity has no traffic provisioned on it, so no service is lost.

Because of this possibility of being raised at two different levels, the alarm profile pane shows Critical as "CR / MN" and Major as "MJ / MN."

10.4 Alarm Profiles

The alarm profiles feature allows you to change default alarm severities by creating unique alarm profiles for individual ONS 15327 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, its cards, or its cards' 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 NE, and cannot be edited. The reserved Default profile contains Telcordia GR-253 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.

10.4.1 Creating and Modifying Alarm Profiles

Alarm profiles are created in the network view using the Provisioning > Alarm Profiles tabs. A default alarm severity following Telcordia GR-253 standards is preprovisioned for every alarm. After loading the default profile or another profile on the node, you can use the Clone feature to create custom profiles. After the new profile is created, the Alarm Profiles window shows the original profile—frequently Default—and the new profile. The Default alarm profile list contains alarm and condition severities that correspond when applicable to default values established in Telcordia GR-253.

Note All default or user-defined severity settings that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in non-service-affecting situations as defined in Telcordia GR-474.

Tip To see the full list of profiles including those available for loading or cloning, click the Available button. You must load a profile before you can clone it.

Note Up to ten profiles, including the two reserved profiles, Inherited and Default, can be stored in CTC.

Wherever it is applied, the Default alarm profile sets severities to standard Telcordia GR-253 settings. In the Inherited profile, alarms inherit, or copy, severity from the next-highest level. For example, a card with an Inherited alarm profile copies the severities used by the node housing the card. If you choose the Inherited profile from the network view, the severities at the lower levels (node and card) are copied from this selection.

You do not have to apply a single severity profile to the node-, card-, and port-level alarms. Different profiles can be applied at different levels. You could use the inherited or default profile on a node and on all cards and ports, but apply a custom profile that downgrades an alarm on one particular card. For example, you might choose to downgrade an OC-N unequipped path alarm (UNEQ-P) from Critical (CR) to Not Alarmed (NA) on an optical card because this alarm raises and then clears every time you create a circuit. UNEQ-P alarms for the card with the custom profile would not display on the Alarms tab (but they would still be recorded on the Conditions and History tabs).

When you modify severities in an alarm profile:

- All Critical (CR) or Major (MJ) default or user-defined severity settings are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.
- Default severities are used for all alarms and conditions until you create a new profile and apply it.

10.4.2 Alarm Profile Buttons

The Alarm Profiles window displays six buttons on the right side. Table 10-8 lists and describes each of the alarm profile buttons and their functions.

Table 10-8 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 (for example, 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 shows which profiles contain the alarm. Can be printed.

10.4.3 Alarm Profile Editing

Table 10-9 lists and describes the five profile-editing options available when you right-click an alarm item in the profile column (such as Default).

Table 10-9 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 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.

10.4.4 Alarm Severity Options

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
- Inherited (I)

Inherited and Use Default severity levels only appear in alarm profiles. They do not appear when you view alarms, history, or conditions.

10.4.5 Row Display Options

In the network view, the Alarm Profiles window displays two check boxes at the bottom of the window:

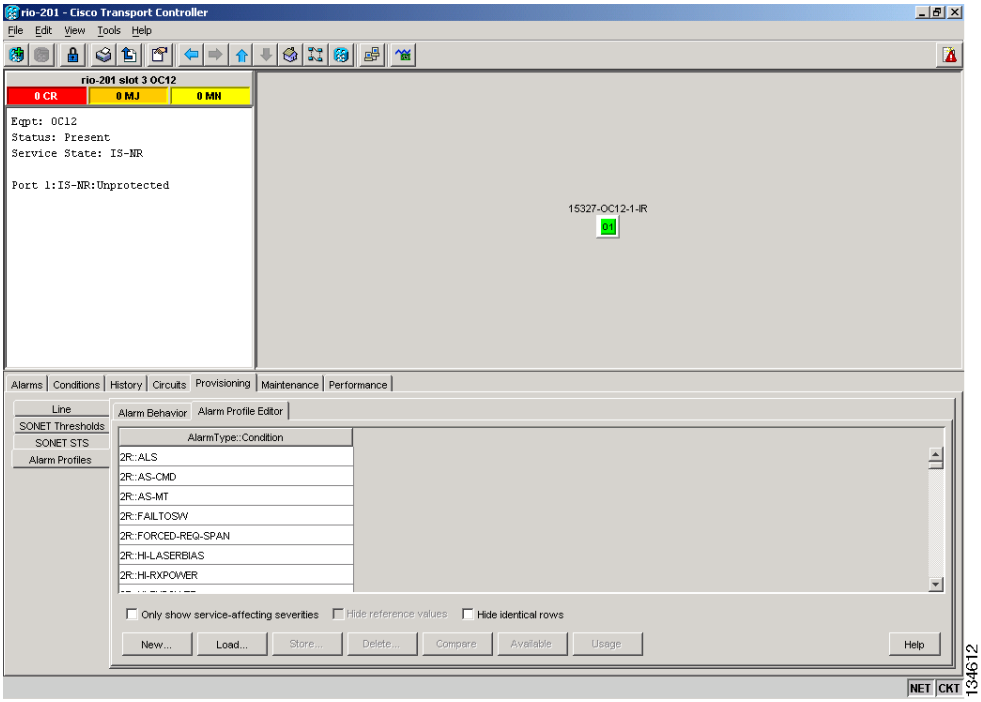
- Hide reference values—Highlights alarms with non-default severities by clearing alarm cells with default severities.
- Hide identical rows—Hides rows of alarms that contain the same severity for each profile.

10.4.6 Applying Alarm Profiles

In CTC node view, the Alarm Behavior window displays alarm profiles for the node. In card view, the Alarm Behavior window 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 or set alarm profiles for all ports on that card. Figure 10-2 shows the card view of an optical alarm profile.

Figure 10-2 Card View of an Optical Card Alarm Profile



10.5 Alarm Suppression

ONS 15327 nodes have an alarm suppression option that clears raised alarm messages for the node, chassis, one or more slots (cards), or one or more ports. After they are cleared, these alarms change appearance from their normal severity color to white and they can be cleared from the display by clicking Synchronize. Alarm suppression itself raises an alarm called AS-CMD that is shown in applicable Alarms windows. Node-level suppression is shown in the node view Alarms window, and card or port-level suppression is shown in all views. The AS-CMD alarm itself is not cleared by the suppress command. Each instance of this alarm indicates its object separately in the Object column.

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.

Suppression causes the entity alarm to behave like a Not Reported event. This means that the alarms, having been suppressed from view in the Alarms window, are now only shown in the Conditions window. The suppressed alarms are displayed with their usual visual characteristics (service-affecting status and color-coding) in the window. The alarms still appear in the History window.

Note 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.

10.6 External Alarms and Controls

External alarm physical connections are made on the mechanical interface card (MIC). However, the alarms are provisioned using the XTC card view for external sensors such as an open door and flood sensors, temperature sensors, and other environmental conditions. External control outputs on these two cards 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 in the XTC card view Provisioning> External Alarms tab and controls in the XTC card view Provisioning > External Controls tab. Up to six external alarm inputs and two external controls are available with the XTC card.

10.6.1 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); open means that the normal condition is no current flowing through the contact, and the alarm is generated when current does flow; closed means that normal condition is to have current flowing through the contact, and the alarm is generated with current stops flowing
- Virtual wire associated with the alarm
- CTC alarm log description (up to 63 characters)

Note If you provision an external alarm to raise upon an open contact before you physically connect to the ONS equipment, the alarm will raise until you create the physical connection.

Note When you provision an external alarm, the alarm object is ENV-IN-*nn*. The variable *nn* refers to the external alarm's number, regardless of the name you assign.

10.6.2 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 display
- 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.

Hardware Specifications

This appendix contains hardware and software specifications for the ONS 15327.

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.

A.1 Shelf Specifications

This section provides bandwidth specifications; slot assignments, card and topology lists; Cisco Transport Controller (CTC) specifications; the LAN, Transaction Language One (TL1), modem, alarm, and EIA interface specifications; timing, power, and environmental specifications; and shelf dimensions.

A.1.1 Bandwidth

- Total bandwidth: 240 Gbps
- Data plane bandwidth: 160 Gbps
- SONET plane bandwidth: 80 Gbps

A.1.2 Slot Assignments

- Total card slots: 8
- Traffic card slots (E10/100-4, G-1000-2, OC-3, OC-12, and OC-48): Slots 1 through 4
- Cross Connect, Timing and Control (XTC): Slots 5, 6
- Mechanical Interface Card (MIC): Slots 7, 8

A.1.3 Cards

- XTC-14
- XTC-28-3
- MIC A
- MIC B
- E10/100-4
- G1000-2
- OC3 IR 4 1310
- OC12 IR 1310
- OC12 LR 1550
- OC48-1-IR
- OC48 LR 1550

A.1.4 Configurations

- Two-fiber path protection
- Path protected mesh network (PPMN)
- Two-fiber bidirectional path-switched ring (BLSR)
- Add/drop multiplexer
- Point-to-point terminal mode

A.1.5 Cisco Transport Controller

- 10BaseT
- XTC access: RJ-45 connector

A.1.6 External LAN Interface

- 10BaseT Ethernet

A.1.7 TL1 Craft Interface

- Speed: 9600 bps
- XTC: EIA/TIA-232 DB-9 type connector

A.1.8 Modem Interface

- Hardware flow control

- XTC: EIA/TIA-232 DB-9 type connector

A.1.9 Alarm Interface

- Visual: Critical, Major, Minor, Remote
- Audible: Critical, Major, Minor, Remote
- Alarm contacts: 0.045mm, –48 V, 50 mA

A.1.10 Nonvolatile Memory

- 96 MB, flash memory

A.1.11 BITS Interface

- 2 DS-1 building integrated timing supply (BITS) inputs
- 2 derived DS-1 outputs

A.1.12 System Timing

- Stratum 3 per Telcordia GR-253-CORE
- Free running accuracy: +/–4.6 ppm
- Holdover stability: 3.7 x10^{-7}/day, including temperature (< 255 slips in first 24 hours)
- Reference: External BITS, line, internal

A.1.13 Power Specifications

- Input power: -48 VDC
- Power consumption: 260 W (maximum draw with cards)
- Power requirements: –42 to –56 VDC
- Power terminals: Removable screw-locking (#12-14 AWG)

A.1.14 Environmental Specifications

- Operating temperature: 0 to +55 degrees Celsius (32 to 131 degrees Fahrenheit); -40 to +65 degrees Celsius (-40 to +149 degrees Fahrenheit) with industrial temperature-rated cards
- Operating humidity: 5 to 95%, non-condensing

The FTA is required to fulfill environmental specifications.

A.1.15 Fan-Tray Assembly Specifications

- Operating Temperature: –40 to +149 degrees Celsius (–40 to +149 degrees Fahrenheit)
- Operating Humidity: 5 - 95%, non-condensing
- Power Consumption: 35 W maximum, 0.73A, 119 BTU/hr

A.1.16 Dimensions

- Height: 5.1 inches (13. cm)
- Width: 19 or 23 inches (41.8 or 50.6 cm) with mounting ears attached
- Depth: 11 inches (28 cm)
- Weight: 15 lb empty (with fan tray assembly); (27 lb maximum)

A.2 SFP Specifications

The ONS 15327 G1000-2 card uses industry standard small form-factor pluggable connectors (SFPs). The type of SFP plugged into the card appears in CTC and TL1. Cisco offers SFPs as separate orderable products.

Table A-1 lists the SFPs compatible with the G1000-2 card.

Table A-1 SFP Compatibility

Card	Compatible SFP (Cisco Product ID)	Cisco Top Assembly Number (TAN)
G1000-2	15327-SFP-LC-SX 15327-SFP-LC-LX	30-1301-01 30-1299-01

A.3 Card Specifications

This section provides specifications for the XTC, MIC, OC3 IR 4 1310, OC12 IR 1310, OC12 LR 1550, OC48 IR 1310, OC48 LR 1550, E10/100-4, and G1000-2 cards.

For compliance information, refer to the *Cisco Optical Transport Products Safety and Compliance Information* document.

A.3.1 XTC Card (XTC 28-3/XTC-14) Specifications

- CTC software interface: 10BaseT LAN
- TL1 craft interface
  - Speed: 9600 baud
  - Front panel access: EIA/TIA-232 DB9 type connector
- Synchronization
  - Stratum 3, per Telcordia GR-253-CORE

  - Free running access: 4.6 ppm accuracy
  - Holdover stability: 3.7 x10^{-7} ppm/day, including temperature (< 255 slips in first 24 hours)
  - Reference: External BITS, line, internal
- Environmental
  - Operating temperature: –40 to +149 degrees Fahrenheit (–40 to +65 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 56 W maximum, 1.17 A, 191 BTU/hr
- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 9.375 in. (238.1 mm)
  - Depth: 9.172 in. (233.0 mm)

A.3.2 MIC Specifications

- Environmental
  - Operating temperature: –40 to +149 degrees Fahrenheit (–40 to +65 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 4.8 W, 0.1 A, 16.4 BTU/hr
- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 9.375 in. (238.1 mm)
  - Depth: 9.172 in. (233.0 mm)

A.3.3 OC3 IR 4 1310 Card Specifications

- Line
  - Bit rate: 155.52 Mbps
  - Code: Scrambled nonreturn to zero (NRZ)
  - Fiber: 1310 nm single-mode
  - Loopback modes: Terminal and facility
  - Connector: LC
  - Compliance: Telcordia GR-253-CORE
- Transmitter
  - Maximum transmitter output power: –8 dBm
  - Minimum transmitter output power: –15 dBm
  - Center wavelength: 1274 nm to 1356 nm
  - Nominal wavelength: 1310 nm
  - Transmitter: Fabry Perot laser

- Receiver
  - Maximum receiver level: –8 dBm
  - Minimum receiver level: –28 dBm
  - Receiver: InGaAs/InP photo detector
  - Link loss budget: 13 dBm
- Environmental
  - Eye safety compliance: Class I
  - Operating temperature: –40 to +149 degrees Fahrenheit (–40 to +65 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 14 W, 0.29 A, 48 BTU/hr
- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 4.280 in. (108.7 mm)
  - Depth: 9.172 in. (233.0 mm)

A.3.4 OC12 IR 1310 Card Specifications

- Line
  - Bit rate: 622.08 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1310 nm single-mode
  - Loopback modes: Terminal and facility
  - Connector: SC
  - Compliance: Telcordia GR-253-CORE
- Transmitter
  - Maximum transmitter output power: –8 dBm
  - Minimum transmitter output power: –15 dBm
  - Center wavelength: 1274 nm to 1356 nm
  - Nominal wavelength: 1310 nm
  - Transmitter: Fabry Perot laser
- Receiver
  - Maximum receiver level: –7 dBm
  - Minimum receiver level: –29 dBm
  - Receiver: InGaAs/InP photo detector
  - Link loss budget: 14 dBm
- Environmental
  - Eye safety compliance: Class I
  - Operating temperature: –40 to +149 degrees Fahrenheit (–40 to +65 degrees Celsius)

  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 14 W, 0.29 A, 48 BTU/hr
- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 4.280 in. (108.7 mm)
  - Depth: 9.172 in. (233.0 mm)

A.3.5 OC12 LR 1550 Card Specifications

- Line
  - Bit rate: 622.08 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1550 nm single-mode
  - Loopback modes: Terminal and facility
  - Connector: SC
  - Compliance: Telcordia GR-253-CORE
- Transmitter
  - Maximum transmitter output power: +2 dBm
  - Minimum transmitter output power: –3 dBm
  - Center wavelength: 1480 nm to 1580 nm
  - Nominal wavelength: 1550 nm
  - Transmitter: DFB (distributed feedback) laser
- Receiver
  - Maximum receiver level: –7 dBm
  - Minimum receiver level: –29 dBm
  - Receiver: InGaAs/InP photo detector
  - Link loss budget: 26 dBm
- Environmental
  - Eye safety compliance: Class I
  - Operating temperature: –40 to +149 degrees Fahrenheit (–40 to +65 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 14 W, 0.29 A, 48 BTU/hr
- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 4.280 in. (108.7 mm)
  - Depth: 9.172 in. (233.0 mm)

A.3.6 OC48-1-IR Card Specifications

- Line
  - Bit rate: 2488.320 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1310-nm single-mode
  - Loopback modes: Terminal and facility
  - Connector: SC
  - Compliance: Telcordia GR-253-CORE
- Transmitter
  - Maximum transmitter output power: 0 dBm
  - Minimum transmitter output power: –5 dBm
  - Center wavelength: 1280 nm to 1350 nm
  - Nominal wavelength: 1310 nm
  - Transmitter: Fabry Perot laser
- Receiver
  - Maximum receiver level: 0 dBm
  - Minimum receiver level: –18 dBm
  - Receiver: InGaAs InP photo detector
  - Link loss budget: 13 dBm minimum
- Environmental
  - Eye safety compliance: Class I
  - Operating temperature: –40 to +149 degrees Fahrenheit (–40 to +65 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 25 W, 0.52 A, 85 BTU/hr
- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 4.280 in. (108.7 mm)
  - Depth: 9.172 in. (233.0 mm)

A.3.7 OC48 LR 1550 Card Specifications

- Line
  - Bit rate: 2488.320 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1550-nm single-mode
  - Loopback modes: Terminal and facility
  - Connector: SC

  - Compliance: Telcordia GR-253-CORE
- Transmitter
  - Maximum transmitter output power: +3dBm
  - Minimum transmitter output power: –2 dBm
  - Center wavelength: 1520 nm to 1580 nm
  - Nominal wavelength: 1550 nm
  - Transmitter: Fabry Perot laser
- Receiver
  - Maximum receiver level:–8 dBm
  - Minimum receiver level: –28 dBm
  - Receiver: InGaAs InP photo detector
  - Link loss budget: 26 dBm minimum, with 1 dB dispersion penalty
- Environmental
  - Eye safety compliance: Class I
  - Operating temperature: –40 to +149 degrees Fahrenheit (–40 to +65 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 25 W, 0.52 A, 85 BTU/hr
- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 4.280 in. (108.7 mm)
  - Depth: 9.172 in. (233.0 mm)

A.3.8 E10/100-4 Card Specifications

- Environmental
  - Operating temperature: 32 to 131 degrees Fahrenheit (0 to +55 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 45 W, 0.95 A, 154 BTU/hr
- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 4.280 in. (108.7 mm)
  - Depth: 9.172 in. (233.0 mm)

A.3.9 G1000-2 Card Specifications

- Environmental
  - Operating temperature:

    C-Temp (15327-E1000-2): 32 to 131 degrees Fahrenheit (0 to +55 degrees Celsius)

  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 53.50 W, 1.11 A, 182.67 BTU/hr.
- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 4.280 in. (108.7 mm)
  - Depth: 9.172 in. (233.0 mm)
  - Card weight: 2.1 lb (0.9 kg)

Administrative and Service States

This appendix describes administrative and service states for Cisco ONS 15327 cards, ports, and cross-connects. For circuit state information, see Chapter 7, "Circuits and Tunnels." Software Release 5.0 states are based on the generic state model defined in Telcordia GR-1093-CORE, Issue 2 and ITU-T X.731.

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 15327.

Table B-1 ONS 15327 Service State Primary States and Primary State Qualifiers

Primary State, Primary State Qualifier	Definition
IS-NR	(In-Service and Normal) The entity is fully operational and will perform as provisioned.
OOS-AU	(Out-of-Service and Autonomous) The entity is not operational because of an autonomous event.
OOS-AUMA	(Out-of-Service and Autonomous Management) The entity is not operational because of an autonomous event and has also been manually removed from service.
OOS-MA	(Out-of-Service and Management) The entity has been manually removed from service.

Table B-2 defines the SSTs supported by the ONS 15327.

Table B-2 ONS 15327 Secondary States

Secondary State	Definition
AINS	(Automatic In-Service) The entity is delayed before transitioning to the IS-NR service state. The transition to IS-NR depends on 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 Cisco Transport Controller (CTC) Conditions tab or by using the Transaction Language One (TL1) RTRV-COND command.
DSBLD	(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.
FLT	(Fault) The entity has a raised alarm or condition.
LPBK	(Loopback) The entity is in loopback mode.
MEA	(Mismatched Equipment) An improper card is installed. For example, an installed card is not compatible with the card preprovisioning or the slot. This SST applies only to cards.
MT	(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.
SWDL	(Software Download) The card is involved in a software and database download. This SST applies only to cards.
UAS	(Unassigned) The card is not provisioned in the database. This SST applies only to cards.
UEQ	(Unequipped) 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 15327. 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 15327 Administrative States

Administrative State (PST,SST)	Definition
IS	Puts the entity in service.
IS,AINS	Puts the entity in automatic in-service.

Table B-3 ONS 15327 Administrative States (continued)

Administrative State (PST,SST)	Definition
OOS,DSBLD	Removes the entity from service and disables it.
OOS,MT	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.

B.3.1 Card Service State Transitions

Table B-4 lists card service state transitions.

Table B-4 ONS 15327 Card Service State Transitions

Current Service State	Action	Next Service State
IS-NR	Change the administrative state to OOS,MT.	OOS-MA,MT
	Delete the card.	OOS-AUMA,UAS
	Pull the card.	OOS-AU,UEQ
	Reset the card.	OOS-AU,SWDL
	Alarm/condition is raised.	OOS-AU,FLT
OOS-AU,AINS and MEA	Pull the card.	OOS-AU,AINS & UEQ
	Delete the card.	OOS-AUMA,UAS if the card is valid OOS-AUMA,MEA & UAS if the card is invalid
OOS-AU,AINS & SWDL	Restart completed.	IS-NR
	Pull the card.	OOS-AU,AINS & UEQ
OOS-AU,AINS & UEQ	Insert a valid card.	OOS-AU,AINS & SWDL
	Insert an invalid card.	OOS-AU,AINS & MEA
	Delete the card.	OOS-AUMA,UAS & UEQ
OOS-AU,FLT	Pull the card.	OOS-AU,UEQ
	Delete the card.	OOS-AUMA,UAS
	Change the administrative state to OOS,MT.	OOS-AUMA,FLT & MT
	Reset the card.	OOS-AU,SWDL
	Alarm/condition is cleared.	IS-NR

Table B-4 ONS 15327 Card Service State Transitions (continued)

Current Service State	Action	Next Service State
OOS-AU,MEA	Pull the card.	OOS-AU,UEQ
	Delete the card.	OOS-AUMA,UAS if the card is valid OOS-AUMA,MEA & UAS if the card is invalid
	Change the administrative state to OOS,MT.	OOS-AUMA, MEA & MT
OOS-AU,SWDL	Restart completed.	IS-NR
	Pull the card.	OOS-AU,UEQ
OOS-AU,UEQ	Insert a valid card.	OOS-AU,SWDL
	Insert an invalid card.	OOS-AU,MEA
	Delete the card.	OOS-AUMA,UAS & UEQ
	Change the administrative state to OOS,MT.	OOS-AUMA,MT & UEQ
OOS-AUMA,FLT & MT	Pull the card.	OOS-AUMA,MT & UEQ
	Delete the card.	OOS-AUMA,UAS
	Change the administrative state to IS.	OOS-AU,FLT
	Reset the card.	OOS-AUMA,MT & SWDL
	Alarm/condition is cleared.	IS-NR
OOS-AUMA,MEA & MT	Change the administrative state to IS.	OOS-AU,MEA
	Pull the card.	OOS-AUMA,MT & UEQ
	Delete the card.	OOS-AUMA,UAS if the card is valid OOS-AUMA,MEA & UAS if the card is invalid
OOS-AUMA,MEA & UAS	Pull the card.	OOS-AUMA,UAS & UEQ
	Provision the card.	OOS-AU,MEA
OOS-AUMA,MT & SWDL	Restart completed.	OOS-MA,MT
	Pull the card.	OOS-AUMA,MT & UEQ
OOS-AUMA,MT & UEQ	Change the administrative state to IS.	OOS-AU,UEQ
	Insert a valid card.	OOS-AUMA,MT & SWDL
	Insert an invalid card.	OOS-AUMA,MEA & MT
	Delete the card.	OOS-AUMA,UAS & UEQ

Table B-4 ONS 15327 Card Service State Transitions (continued)

Current Service State	Action	Next Service State
OOS-AUMA,UAS	Pull the card.	OOS-AUMA,UAS & UEQ
	Provision an invalid card.	OOS-AU,MEA
	Provision a valid card.	OOS-AU,SWDL
OOS-AUMA,UAS & UEQ	Insert a valid card.	OOS-AU,SWDL
	Insert an invalid card.	OOS-AUMA,MEA & UAS
	Preprovision a card.	OOS-AU,AINS & UEQ
OOS-MA,MT	Change the administrative state to IS.	IS-NR
	Delete the card.	OOS-AUMA,UAS
	Pull the card.	OOS-AUMA,MT & UEQ
	Reset the card.	OOS-AUMA,MT & SWDL
	Alarm/condition is raised.	OOS-AUMA,FLT & MT

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 OOS-AU,AINS service state cannot transition autonomously into the IS-NR service state until the parent port is IS-NR.

Note Deleting a cross-connect removes it from the system. The deleted cross-connect does not transition to another service state.

Table B-5 ONS 15327 Port and Cross-Connect Service State Transitions

Current Service State	Action	Next Service State
IS-NR	Put the port or cross-connect in the OOS,MT administrative state.	OOS-MA,MT
	Put the port or cross-connect in the OOS,DSBLD administrative state.	OOS-MA,DSBLD
	Put the port or cross-connect in the IS,AINS administrative state.	OOS-AU,AINS
	Alarm/condition is raised.	OOS-AU,FLT

Table B-5 ONS 15327 Port and Cross-Connect Service State Transitions (continued)

Current Service State	Action	Next Service State
OOS-AU,AINS	Put the port or cross-connect in the IS administrative state.	IS-NR
	Put the port or cross-connect in the OOS,MT administrative state.	OOS-MA,MT
	Put the port or cross-connect in the OOS,DSBLD administrative state.	OOS-MA,DSBLD
	Alarm/condition is raised.	OOS-AU,AINS & FLT
OOS-AU,AINS & FLT	Alarm/condition is cleared.	OOS-AU,AINS
	Put the port or cross-connect in the IS administrative state.	OOS-AU,FLT
	Put the port or cross-connect in the OOS,DSBLD administrative state.	OOS-MA,DSBLD
	Put the port or cross-connect in the OOS,MT administrative state.	OOS-AUMA,FLT & MT
OOS-AU,FLT	Alarm/condition is cleared.	IS-NR
	Put the port or cross-connect in the IS,AINS administrative state.	OOS-AU,AINS & FLT
	Put the port or cross-connect in the OOS,DSBLD administrative state.	OOS-MA,DSBLD
	Put the port or cross-connect in the OOS,MT administrative state	OOS-AUMA,FLT & MT
OOS-AUMA,FLT & LPBK & MT	Release the loopback.	OOS-AUMA,FLT & MT
	Alarm/condition is cleared.	OOS-MA,LPBK & MT
OOS-AUMA,FLT & MT	Alarm/condition is cleared.	OOS-MA,MT
	Put the port or cross-connect in the IS administrative state.	OOS-AU,FLT
	Put the port or cross-connect in the IS,AINS administrative state.	OOS-AU,AINS & FLT
	Put the port or cross-connect in the OOS,DSBLD administrative state.	OOS-MA,DSBLD
	Put the port or cross-connect in a loopback.	OOS-AUMA,FLT & LPBK & MT

Table B-5 ONS 15327 Port and Cross-Connect Service State Transitions (continued)

Current Service State	Action	Next Service State
OOS-MA,DSBLD	Put the port or cross-connect in the IS administrative state.	IS-NR
	Put the port or cross-connect in the IS,AINS administrative state.	OOS-AU,AINS
	Put the port or cross-connect in the OOS,MT administrative state.	OOS-MA,MT
OOS-MA,LPBK & MT	Release the loopback. **Note** While in OOS-MA,LPBK & MT service state, both CTC and TL1 allow a cross-connect to be deleted, which also removes the loopback. This applies only to the cross-connect, not the ports.	OOS-MA,MT
	Alarm/condition is raised.	OOS-AUMA,FLT & LPBK & MT
OOS-MA,MT	Put the port or cross-connect in the IS administrative state.	IS-NR
	Put the port or cross-connect in the IS,AINS administrative state.	OOS-AU,AINS
	Put the port or cross-connect in the OOS,DSBLD administrative state.	OOS-MA,DSBLD
	Put the port or cross-connect in loopback.	OOS-MA,LPBK & MT

Network Element Defaults

This appendix describes the factory-configured (default) network element (NE) settings for the Cisco ONS 15327. It includes descriptions of card default settings and node default settings. To import, export, and edit the settings, refer to the "Maintain the Node" chapter of the *Cisco ONS 15327 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 changing the defaults), refer to the "Change Card Settings" chapter of the *Cisco ONS 15327 Procedure Guide*. To change node settings, refer to the "Change Node Settings" chapter of the *Cisco ONS 15327 Procedure Guide*.

This appendix contains the following sections:

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.

C.1 Network Element Defaults Description

The NE defaults are preinstalled on each Cisco ONS 15327 XTC card. They also ship as a file called 15327-defaults.txt on the Cisco Transport Controller (CTC) software CD in case you want to import the defaults onto existing Cross-Connect, Timing, and Control (XTC) cards. The NE defaults include card-level and node-level defaults.

Changes to card provisioning made manually using the "Change Card Settings" chapter in the *Cisco ONS 15327 Procedure Guide* override default settings. If you use the CTC Defaults editor (in the node view > Provisioning > Defaults tabs) or import a new defaults file, any changes to card or slot settings that result only affect cards that are installed or preprovisioned after the defaults have changed.

Changes 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, bidirectional line switched ring [BLSR] ring reversion time, BLSR ring revertive, BLSR span reversion time, BLSR span revertive), which apply to subsequent provisioning.

Note Changing some NE defaults can cause CTC disconnection or a reboot of the node in order for the default to take effect. Before you change a default, 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 card. Cisco provides user-configurable defaults for the Cisco ONS 15327 optical and electrical cards, including:

- Soak Time—(All cards) The length of time that elapses between an automaticInService (AINS) port receiving a valid signal and when it automatically changes to in-service status.
- Line Coding—(XTCDS1 cards) Defines the DS-1 transmission coding type that is used.
- Line Length—(XTCDS1 and XTCDS3 cards) Defines the distance (in feet) from the backplane connection to the next termination point.
- Line Type—(XTCDS1 cards) Defines the type of framing used.
- Port State—(All cards) Sets the port to one of the four available states (IS, OOS, OOS_MT, or IS_AINS), depending on whether you need ports in or out of service.
- SF BER Level—OC-N cards. Defines the signal fail (SF) bit error rate (BER).
- SD BER Level—OC-N cards. Defines the signal degrade (SD) BER.
- Enable Sync Messages—OC-N cards. Enables synchronization transport signal (STS) status messages (SSM) (S1 byte), which allow the node to choose the best timing source.
- PJ STS Mon—OC-N cards. Sets the synchronus timiSTS that will be used for pointer justification. If set to 0, no STS is monitored.
- STS IPPM Enabled—OC-N cards. Enables intermediate-path performance monitoring (IPPM) on a node for transparent monitoring of a channel that does not terminate on that node.
- Send Do Not Use—OC-N cards. Sends a do not use (DUS) message on the S1 byte when enabled.
- PM Threshold Settings—(All cards) Set the performance monitoring (PM) parameters for gathering performance data and detecting problems early.

Note When the card level defaults are changed, the new provisioning done after the defaults have changed is affected. Existing provisioning remains unaffected.

Note For more information about each individual card setting, refer to the “Change Card Settings” chapter of the *Cisco ONS 15327 Procedure Guide*.

Note For more information about the performance monitoring parameters, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

C.2.1 XTCDS-1 Card Default Settings

Table C-1 lists the XTCDS-1 card default settings.

Table C-1 XTCDS-1 Card Default Settings

Default Name	Default Value	Default Domain
XTCDS1.config.AINSSoakTime	08:00 (hours:mins)	00:00, 00:15, 00:30 .. 48:00
XTCDS1.config.LineCoding	AMI	B8ZS, AMI
XTCDS1.config.LineLength	0 - 131 ft	0 - 131 ft, 132 - 262 ft, 263 - 393 ft, 394 - 524 ft, 525 - 655 ft
XTCDS1.config.LineType	D4	ESF, D4, UNFRAMED
XTCDS1.config.SDBER	1E-7	1E-5, 1E-6, 1E-7, 1E-8, 1E-9
XTCDS1.config.SFBER	1E-4	1E-3, 1E-4, 1E-5
XTCDS1.config.State	IS,AINS	IS; OOS,DSBLD; OOS,MT; IS,AINS
XTCDS1.pmthresholds.line.farend.15min.ES	65 (seconds)	0–900
XTCDS1.pmthresholds.line.farend.1day.ES	648 (seconds)	0–86400
XTCDS1.pmthresholds.line.nearend.15min.CV	13340 (BPV count)	0–1388700
XTCDS1.pmthresholds.line.nearend.15min.ES	65 (seconds)	0–900
XTCDS1.pmthresholds.line.nearend.15min.LOSS	10 (seconds)	0–900
XTCDS1.pmthresholds.line.nearend.15min.SES	10 (seconds)	0–900
XTCDS1.pmthresholds.line.nearend.1day.CV	133400 (BPV count)	0–133315200
XTCDS1.pmthresholds.line.nearend.1day.ES	648 (seconds)	0–86400
XTCDS1.pmthresholds.line.nearend.1day.LOSS	10 (seconds)	0–86400
XTCDS1.pmthresholds.line.nearend.1day.SES	100 (seconds)	0–86400
XTCDS1.pmthresholds.path.farend.15min.CSS	25 (seconds)	0–900
XTCDS1.pmthresholds.path.farend.15min.CV	13296 (BIP count)	0–287100
XTCDS1.pmthresholds.path.farend.15min.ES	65 (seconds)	0–900
XTCDS1.pmthresholds.path.farend.15min.ESA	25 (seconds)	0–900
XTCDS1.pmthresholds.path.farend.15min.ESB	25 (seconds)	0–900
XTCDS1.pmthresholds.path.farend.15min.SEFS	25 (seconds)	0–900
XTCDS1.pmthresholds.path.farend.15min.SES	10 (seconds)	0–900
XTCDS1.pmthresholds.path.farend.15min.UAS	10 (seconds)	0–900
XTCDS1.pmthresholds.path.farend.1day.CSS	25 (seconds)	0–86400
XTCDS1.pmthresholds.path.farend.1day.CV	132960 (BIP count)	0–27561600
XTCDS1.pmthresholds.path.farend.1day.ES	648 (seconds)	0–86400
XTCDS1.pmthresholds.path.farend.1day.ESA	25 (seconds)	0–86400
XTCDS1.pmthresholds.path.farend.1day.ESB	25 (seconds)	0–86400
XTCDS1.pmthresholds.path.farend.1day.SEFS	25 (seconds)	0–86400

Table C-1 XTCDS-1 Card Default Settings (continued)

Default Name	Default Value	Default Domain
XTCDS1.pmthresholds.path.farend.1day.SES	100 (seconds)	0–86400
XTCDS1.pmthresholds.path.farend.1day.UAS	10 (seconds)	0–86400
XTCDS1.pmthresholds.path.nearend.15min.AISS	10 (seconds)	0–900
XTCDS1.pmthresholds.path.nearend.15min.CV	13296 (BIP count)	0–287100
XTCDS1.pmthresholds.path.nearend.15min.ES	65 (seconds)	0–900
XTCDS1.pmthresholds.path.nearend.15min.FC	10 (count)	0–72
XTCDS1.pmthresholds.path.nearend.15min.SAS	2 (seconds)	0–900
XTCDS1.pmthresholds.path.nearend.15min.SES	10 (seconds)	0–900
XTCDS1.pmthresholds.path.nearend.15min.UAS	10 (seconds)	0–900
XTCDS1.pmthresholds.path.nearend.1day.AISS	10 (seconds)	0–86400
XTCDS1.pmthresholds.path.nearend.1day.CV	132960 (BIP count)	0–27561600
XTCDS1.pmthresholds.path.nearend.1day.ES	648 (seconds)	0–86400
XTCDS1.pmthresholds.path.nearend.1day.FC	40 (count)	0–6912
XTCDS1.pmthresholds.path.nearend.1day.SAS	17 (seconds)	0–86400
XTCDS1.pmthresholds.path.nearend.1day.SES	100 (seconds)	0–86400
XTCDS1.pmthresholds.path.nearend.1day.UAS	10 (seconds)	0–86400
XTCDS1.pmthresholds.sts.farend.15min.CV	15 (B3 count)	0–2160000
XTCDS1.pmthresholds.sts.farend.15min.ES	12 (seconds)	0–900
XTCDS1.pmthresholds.sts.farend.15min.FC	10 (count)	0–72
XTCDS1.pmthresholds.sts.farend.15min.SES	3 (seconds)	0–900
XTCDS1.pmthresholds.sts.farend.15min.UAS	10 (seconds)	0–900
XTCDS1.pmthresholds.sts.farend.1day.CV	125 (B3 count)	0–207360000
XTCDS1.pmthresholds.sts.farend.1day.ES	100 (seconds)	0–86400
XTCDS1.pmthresholds.sts.farend.1day.FC	40 (count)	0–6912
XTCDS1.pmthresholds.sts.farend.1day.SES	7 (seconds)	0–86400
XTCDS1.pmthresholds.sts.farend.1day.UAS	10 (seconds)	0–86400
XTCDS1.pmthresholds.sts.nearend.15min.CV	15 (B3 count)	0–2160000
XTCDS1.pmthresholds.sts.nearend.15min.ES	12 (seconds)	0–900
XTCDS1.pmthresholds.sts.nearend.15min.FC	10 (count)	0–72
XTCDS1.pmthresholds.sts.nearend.15min.SES	3 (seconds)	0–900
XTCDS1.pmthresholds.sts.nearend.15min.UAS	10 (seconds)	0–900
XTCDS1.pmthresholds.sts.nearend.1day.CV	125 (B3 count)	0–207360000
XTCDS1.pmthresholds.sts.nearend.1day.ES	100 (seconds)	0–86400
XTCDS1.pmthresholds.sts.nearend.1day.FC	40 (count)	0–6912
XTCDS1.pmthresholds.sts.nearend.1day.SES	7 (seconds)	0–86400
XTCDS1.pmthresholds.sts.nearend.1day.UAS	10 (seconds)	0–86400

Table C-1 XTCDS-1 Card Default Settings (continued)

Default Name	Default Value	Default Domain
XTCDS1.pmthresholds.vt.farend.15min.CV	15 (BIP8 count)	0–2160000
XTCDS1.pmthresholds.vt.farend.15min.ES	12 (seconds)	0–900
XTCDS1.pmthresholds.vt.farend.15min.SES	3 (seconds)	0–900
XTCDS1.pmthresholds.vt.farend.15min.UAS	10 (seconds)	0–900
XTCDS1.pmthresholds.vt.farend.1day.CV	125 (BIP8 count)	0–207360000
XTCDS1.pmthresholds.vt.farend.1day.ES	100 (seconds)	0–86400
XTCDS1.pmthresholds.vt.farend.1day.SES	7 (seconds)	0–86400
XTCDS1.pmthresholds.vt.farend.1day.UAS	10 (seconds)	0–86400
XTCDS1.pmthresholds.vt.nearend.15min.CV	15 (BIP8 count)	0–2160000
XTCDS1.pmthresholds.vt.nearend.15min.ES	12 (seconds)	0–900
XTCDS1.pmthresholds.vt.nearend.15min.SES	3 (seconds)	0–900
XTCDS1.pmthresholds.vt.nearend.15min.UAS	10 (seconds)	0–900
XTCDS1.pmthresholds.vt.nearend.1day.CV	125 (BIP8 count)	0–207360000
XTCDS1.pmthresholds.vt.nearend.1day.ES	100 (seconds)	0–86400
XTCDS1.pmthresholds.vt.nearend.1day.SES	7 (seconds)	0–86400
XTCDS1.pmthresholds.vt.nearend.1day.UAS	10 (seconds)	0–86400

C.2.2 XTCDS-3 Card Default Settings

Table C-2 lists the XTCDS-3 card default settings.

Table C-2 XTCDS-3 Card Default Settings

Default Name	Default Value	Default Domain
XTCDS3.config.AINSSoakTime	08:00 (hours:mins)	00:00, 00:15, 00:30 .. 48:00
XTCDS3.config.LineLength	0 - 225 ft (feet)	0 - 225 ft, 226 - 450 ft
XTCDS3.config.SDBER	1E-7	1E-5, 1E-6, 1E-7, 1E-8, 1E-9
XTCDS3.config.SFBER	1E-4	1E-3, 1E-4, 1E-5
XTCDS3.config.State	IS,AINS	IS; OOS,DSBLD; OOS,MT; IS,AINS
XTCDS3.pmthresholds.line.nearend.15min.CV	387 (BPV count)	0–38700
XTCDS3.pmthresholds.line.nearend.15min.ES	25 (seconds)	0–900
XTCDS3.pmthresholds.line.nearend.15min.LOSS	10 (seconds)	0–900
XTCDS3.pmthresholds.line.nearend.15min.SES	4 (seconds)	0–900
XTCDS3.pmthresholds.line.nearend.1day.CV	3865 (BPV count)	0–3715200
XTCDS3.pmthresholds.line.nearend.1day.ES	250 (seconds)	0–900
XTCDS3.pmthresholds.line.nearend.1day.LOSS	10 (seconds)	0–900
XTCDS3.pmthresholds.line.nearend.1day.SES	40 (seconds)	0–900

Table C-2 XTCDS-3 Card Default Settings (continued)

Default Name	Default Value	Default Domain
XTCDS3.pmthresholds.sts.farend.15min.CV	15 (G1 count)	0–2160000
XTCDS3.pmthresholds.sts.farend.15min.ES	12 (seconds)	0–900
XTCDS3.pmthresholds.sts.farend.15min.FC	10 (count)	0–72
XTCDS3.pmthresholds.sts.farend.15min.SES	3 (seconds)	0–900
XTCDS3.pmthresholds.sts.farend.15min.UAS	10 (seconds)	0–900
XTCDS3.pmthresholds.sts.farend.1day.CV	125 (G1 count)	0–207360000
XTCDS3.pmthresholds.sts.farend.1day.ES	100 (seconds)	0–86400
XTCDS3.pmthresholds.sts.farend.1day.FC	40 (count)	0–6912
XTCDS3.pmthresholds.sts.farend.1day.SES	7 (seconds)	0–86400
XTCDS3.pmthresholds.sts.farend.1day.UAS	10 (seconds)	0–86400
XTCDS3.pmthresholds.sts.nearend.15min.CV	15 (B3 count)	0–2160000
XTCDS3.pmthresholds.sts.nearend.15min.ES	12 (seconds)	0–900
XTCDS3.pmthresholds.sts.nearend.15min.FC	10 (count)	0–72
XTCDS3.pmthresholds.sts.nearend.15min.SES	3 (seconds)	0–900
XTCDS3.pmthresholds.sts.nearend.15min.UAS	10 (seconds)	0–900
XTCDS3.pmthresholds.sts.nearend.1day.CV	125 (B3 count)	0–207360000
XTCDS3.pmthresholds.sts.nearend.1day.ES	100 (seconds)	0–86400
XTCDS3.pmthresholds.sts.nearend.1day.FC	40 (count)	0–6912
XTCDS3.pmthresholds.sts.nearend.1day.SES	7 (seconds)	0–86400
XTCDS3.pmthresholds.sts.nearend.1day.UAS	10 (seconds)	0–86400

C.2.3 OC-3 Card Default Settings

Table C-3 lists the OC-3 card default settings.

Table C-3 OC-3 Card Default Settings

Default Name	Default Value	Default Domain
OC3.config.line.AdminSSMIn	STU	PRS, STU, ST2, TNC, ST3E, ST3, SMC, ST4, DUS, RES
OC3.config.line.AINSSoakTime	08:00 (hours:mins)	00:00, 00:15, 00:30 .. 48:00
OC3.config.line.PJStsMon#	0 (STS #)	0–3
OC3.config.line.SDBER	1E-7	1E-5, 1E-6, 1E-7, 1E-8, 1E-9
OC3.config.line.Send<FF>DoNotUse	FALSE	• FALSE when SendDoNotUse is TRUE • FALSE, TRUE when SendDoNotUse is FALSE
OC3.config.line.SendDoNotUse	FALSE	FALSE, TRUE

Table C-3 OC-3 Card Default Settings (continued)

Default Name	Default Value	Default Domain
OC3.config.line.SFBER	1E-4	1E-3, 1E-4, 1E-5
OC3.config.line.State	IS,AINS	IS; OOS,DSBLD; OOS,MT; IS,AINS
OC3.config.line.SyncMsgIn	TRUE	FALSE, TRUE
OC3.config.sts.IPPMEnabled	FALSE	TRUE, FALSE
OC3.pmthresholds.line.farend.15min.CV	1312 (B2 count)	0–137700
OC3.pmthresholds.line.farend.15min.ES	87 (seconds)	0–900
OC3.pmthresholds.line.farend.15min.FC	10 (count)	0–72
OC3.pmthresholds.line.farend.15min.SES	1 (seconds)	0–900
OC3.pmthresholds.line.farend.15min.UAS	3 (seconds)	0–900
OC3.pmthresholds.line.farend.1day.CV	13120 (B2 count)	0–13219200
OC3.pmthresholds.line.farend.1day.ES	864 (seconds)	0–86400
OC3.pmthresholds.line.farend.1day.FC	40 (count)	0–6912
OC3.pmthresholds.line.farend.1day.SES	4 (seconds)	0–86400
OC3.pmthresholds.line.farend.1day.UAS	10 (seconds)	0–86400
OC3.pmthresholds.line.nearend.15min.CV	1312 (B2 count)	0–137700
OC3.pmthresholds.line.nearend.15min.ES	87 (seconds)	0–900
OC3.pmthresholds.line.nearend.15min.FC	10 (count)	0–72
OC3.pmthresholds.line.nearend.15min.PSC	1 (count)	0–600
OC3.pmthresholds.line.nearend.15min.PSD	300 (seconds)	0–900
OC3.pmthresholds.line.nearend.15min.SES	1 (seconds)	0–900
OC3.pmthresholds.line.nearend.15min.UAS	3 (seconds)	0–900
OC3.pmthresholds.line.nearend.1day.CV	13120 (B2 count)	0–13219200
OC3.pmthresholds.line.nearend.1day.ES	864 (seconds)	0–86400
OC3.pmthresholds.line.nearend.1day.FC	40 (count)	0–6912
OC3.pmthresholds.line.nearend.1day.PSC	5 (count)	0–57600
OC3.pmthresholds.line.nearend.1day.PSD	600 (seconds)	0–86400
OC3.pmthresholds.line.nearend.1day.SES	4 (seconds)	0–86400
OC3.pmthresholds.line.nearend.1day.UAS	10 (seconds)	0–86400
OC3.pmthresholds.section.nearend.15min.CV	10000 (B1 count)	0–138600
OC3.pmthresholds.section.nearend.15min.ES	500 (seconds)	0–900
OC3.pmthresholds.section.nearend.15min.SEFS	500 (seconds)	0–900
OC3.pmthresholds.section.nearend.15min.SES	500 (seconds)	0–900
OC3.pmthresholds.section.nearend.1day.CV	100000 (B1 count)	0–13305600
OC3.pmthresholds.section.nearend.1day.ES	5000 (seconds)	0–86400
OC3.pmthresholds.section.nearend.1day.SEFS	5000 (seconds)	0–86400

Table C-3 OC-3 Card Default Settings (continued)

Default Name	Default Value	Default Domain
OC3.pmthresholds.section.nearend.1day.SES	5000 (seconds)	0–86400
OC3.pmthresholds.sts1.nearend.15min.CV	15 (B3 count)	0–2160000
OC3.pmthresholds.sts1.nearend.15min.ES	12 (seconds)	0–900
OC3.pmthresholds.sts1.nearend.15min.FC	10 (count)	0–72
OC3.pmthresholds.sts1.nearend.15min.NPJC-PDET	60 (count)	0–7200000
OC3.pmthresholds.sts1.nearend.15min.NPJC-PGEN	60 (count)	0–7200000
OC3.pmthresholds.sts1.nearend.15min.PJCDIFF	60 (count)	0–14400000
OC3.pmthresholds.sts1.nearend.15min.PJCS-PDET	100 (seconds)	0–900
OC3.pmthresholds.sts1.nearend.15min.PJCS-PGEN	100 (seconds)	0–900
OC3.pmthresholds.sts1.nearend.15min.PPJC-PDET	60 (count)	0–7200000
OC3.pmthresholds.sts1.nearend.15min.PPJC-PGEN	60 (count)	0–7200000
OC3.pmthresholds.sts1.nearend.15min.SES	3 (seconds)	0–900
OC3.pmthresholds.sts1.nearend.15min.UAS	10 (seconds)	0–900
OC3.pmthresholds.sts1.nearend.1day.CV	125 (B3 count)	0–207360000
OC3.pmthresholds.sts1.nearend.1day.ES	100 (seconds)	0–86400
OC3.pmthresholds.sts1.nearend.1day.FC	40 (count)	0–6912
OC3.pmthresholds.sts1.nearend.1day.NPJC-PDET	5760 (count)	0–691200000
OC3.pmthresholds.sts1.nearend.1day.NPJC-PGEN	5760 (count)	0–691200000
OC3.pmthresholds.sts1.nearend.1day.PJCDIFF	5760 (count)	0–1382400000
OC3.pmthresholds.sts1.nearend.1day.PJCS-PDET	9600 (seconds)	0–86400
OC3.pmthresholds.sts1.nearend.1day.PJCS-PGEN	9600 (seconds)	0–86400
OC3.pmthresholds.sts1.nearend.1day.PPJC-PDET	5760 (count)	0–691200000
OC3.pmthresholds.sts1.nearend.1day.PPJC-PGEN	5760 (count)	0–691200000
OC3.pmthresholds.sts1.nearend.1day.SES	7 (seconds)	0–86400
OC3.pmthresholds.sts1.nearend.1day.UAS	10 (seconds)	0–86400
OC3.pmthresholds.sts3c.nearend.15min.CV	25 (B3 count)	0–2160000
OC3.pmthresholds.sts3c.nearend.15min.ES	20 (seconds)	0–900
OC3.pmthresholds.sts3c.nearend.15min.FC	10 (count)	0–72
OC3.pmthresholds.sts3c.nearend.15min.NPJC-PDET	60 (count)	0–7200000
OC3.pmthresholds.sts3c.nearend.15min.NPJC-PGEN	60 (count)	0–7200000
OC3.pmthresholds.sts3c.nearend.15min.PJCDIFF	60 (count)	0–14400000
OC3.pmthresholds.sts3c.nearend.15min.PJCS-PDET	100 (seconds)	0–900
OC3.pmthresholds.sts3c.nearend.15min.PJCS-PGEN	100 (seconds)	0–900
OC3.pmthresholds.sts3c.nearend.15min.PPJC-PDET	60 (count)	0–7200000
OC3.pmthresholds.sts3c.nearend.15min.PPJC-PGEN	60 (count)	0–7200000
OC3.pmthresholds.sts3c.nearend.15min.SES	3 (seconds)	0–900

Table C-3 OC-3 Card Default Settings (continued)

Default Name	Default Value	Default Domain
OC3.pmthresholds.sts3c.nearend.15min.UAS	10 (seconds)	0–900
OC3.pmthresholds.sts3c.nearend.1day.CV	250 (B3 count)	0–207360000
OC3.pmthresholds.sts3c.nearend.1day.ES	200 (seconds)	0–86400
OC3.pmthresholds.sts3c.nearend.1day.FC	40 (count)	0–6912
OC3.pmthresholds.sts3c.nearend.1day.NPJC-PDET	5760 (count)	0–691200000
OC3.pmthresholds.sts3c.nearend.1day.NPJC-PGEN	5760 (count)	0–691200000
OC3.pmthresholds.sts3c.nearend.1day.PJCDIFF	5760 (count)	0–1382400000
OC3.pmthresholds.sts3c.nearend.1day.PJCS-PDET	9600 (seconds)	0–86400
OC3.pmthresholds.sts3c.nearend.1day.PJCS-PGEN	9600 (seconds)	0–86400
OC3.pmthresholds.sts3c.nearend.1day.PPJC-PDET	5760 (count)	0–691200000
OC3.pmthresholds.sts3c.nearend.1day.PPJC-PGEN	5760 (count)	0–691200000
OC3.pmthresholds.sts3c.nearend.1day.SES	7 (seconds)	0–86400
OC3.pmthresholds.sts3c.nearend.1day.UAS	10 (seconds)	0–86400

C.2.4 OC-12 Card Default Settings

Table C-4 lists the OC-12 card default settings.

Table C-4 OC-12 Card Default Settings

Default Name	Default Value	Default Domain
OC12.config.line.AdminSSMIn	STU	PRS, STU, ST2, TNC, ST3E, ST3, SMC, ST4, DUS, RES
OC12.config.line.AINSSoakTime	08:00 (hours:mins)	00:00, 00:15, 00:30 .. 48:00
OC12.config.line.PJStsMon#	0 (STS #)	0–12
OC12.config.line.SDBER	1E-7	1E-5, 1E-6, 1E-7, 1E-8, 1E-9
OC12.config.line.Send<FF>DoNotUse	FALSE	• FALSE when SendDoNotUse is TRUE • FALSE, TRUE when SendDoNotUse is FALSE
OC12.config.line.SendDoNotUse	FALSE	FALSE, TRUE
OC12.config.line.SFBER	1E-4	1E-3, 1E-4, 1E-5
OC12.config.line.State	IS,AINS	IS; OOS,DSBLD; OOS,MT; IS,AINS
OC12.config.line.SyncMsgIn	TRUE	FALSE, TRUE
OC12.config.sts.IPPMEnabled	FALSE	TRUE, FALSE
OC12.pmthresholds.line.farend.15min.CV	5315 (B2 count)	0–552600
OC12.pmthresholds.line.farend.15min.ES	87 (seconds)	0–900

Table C-4 OC-12 Card Default Settings (continued)

Default Name	Default Value	Default Domain
OC12.pmthresholds.line.farend.15min.FC	10 (count)	0–72
OC12.pmthresholds.line.farend.15min.SES	1 (seconds)	0–900
OC12.pmthresholds.line.farend.15min.UAS	3 (seconds)	0–900
OC12.pmthresholds.line.farend.1day.CV	53150 (B2 count)	0–53049600
OC12.pmthresholds.line.farend.1day.ES	864 (seconds)	0–86400
OC12.pmthresholds.line.farend.1day.FC	40 (count)	0–6912
OC12.pmthresholds.line.farend.1day.SES	4 (seconds)	0–86400
OC12.pmthresholds.line.farend.1day.UAS	10 (seconds)	0–86400
OC12.pmthresholds.line.nearend.15min.CV	5315 (B2 count)	0–552600
OC12.pmthresholds.line.nearend.15min.ES	87 (seconds)	0–900
OC12.pmthresholds.line.nearend.15min.FC	10 (count)	0–72
OC12.pmthresholds.line.nearend.15min.PSC	1 (count)	0–600
OC12.pmthresholds.line.nearend.15min.PSC-W	1 (count)	0–600
OC12.pmthresholds.line.nearend.15min.PSD	300 (seconds)	0–900
OC12.pmthresholds.line.nearend.15min.PSD-W	300 (seconds)	0–900
OC12.pmthresholds.line.nearend.15min.SES	1 (seconds)	0–900
OC12.pmthresholds.line.nearend.15min.UAS	3 (seconds)	0–900
OC12.pmthresholds.line.nearend.1day.CV	53150 (B2 count)	0–53049600
OC12.pmthresholds.line.nearend.1day.ES	864 (seconds)	0–86400
OC12.pmthresholds.line.nearend.1day.FC	40 (count)	0–6912
OC12.pmthresholds.line.nearend.1day.PSC	5 (count)	0–57600
OC12.pmthresholds.line.nearend.1day.PSC-W	5 (count)	0–57600
OC12.pmthresholds.line.nearend.1day.PSD	600 (seconds)	0–86400
OC12.pmthresholds.line.nearend.1day.PSD-W	600 (seconds)	0–86400
OC12.pmthresholds.line.nearend.1day.SES	4 (seconds)	0–86400
OC12.pmthresholds.line.nearend.1day.UAS	10 (seconds)	0–86400
OC12.pmthresholds.section.nearend.15min.CV	10000 (B1 count)	0–553500
OC12.pmthresholds.section.nearend.15min.ES	500 (seconds)	0–900
OC12.pmthresholds.section.nearend.15min.SEFS	500 (seconds)	0–900
OC12.pmthresholds.section.nearend.15min.SES	500 (seconds)	0–900
OC12.pmthresholds.section.nearend.1day.CV	100000 (B1 count)	0–53136000
OC12.pmthresholds.section.nearend.1day.ES	5000 (seconds)	0–86400
OC12.pmthresholds.section.nearend.1day.SEFS	5000 (seconds)	0–86400
OC12.pmthresholds.section.nearend.1day.SES	5000 (seconds)	0–86400
OC12.pmthresholds.sts1.nearend.15min.CV	15 (B3 count)	0–2160000
OC12.pmthresholds.sts1.nearend.15min.ES	12 (seconds)	0–900

Table C-4 OC-12 Card Default Settings (continued)

Default Name	Default Value	Default Domain
OC12.pmthresholds.sts1.nearend.15min.FC	10 (count)	0–72
OC12.pmthresholds.sts1.nearend.15min.NPJC-PDET	60 (count)	0–7200000
OC12.pmthresholds.sts1.nearend.15min.NPJC-PGEN	60 (count)	0–7200000
OC12.pmthresholds.sts1.nearend.15min.PJCDIFF	60 (count)	0–14400000
OC12.pmthresholds.sts1.nearend.15min.PJCS-PDET	100 (seconds)	0–900
OC12.pmthresholds.sts1.nearend.15min.PJCS-PGEN	100 (seconds)	0–900
OC12.pmthresholds.sts1.nearend.15min.PPJC-PDET	60 (count)	0–7200000
OC12.pmthresholds.sts1.nearend.15min.PPJC-PGEN	60 (count)	0–7200000
OC12.pmthresholds.sts1.nearend.15min.SES	3 (seconds)	0–900
OC12.pmthresholds.sts1.nearend.15min.UAS	10 (seconds)	0–900
OC12.pmthresholds.sts1.nearend.1day.CV	125 (B3 count)	0–207360000
OC12.pmthresholds.sts1.nearend.1day.ES	100 (seconds)	0–86400
OC12.pmthresholds.sts1.nearend.1day.FC	40 (count)	0–6912
OC12.pmthresholds.sts1.nearend.1day.NPJC-PDET	5760 (count)	0–691200000
OC12.pmthresholds.sts1.nearend.1day.NPJC-PGEN	5760 (count)	0–691200000
OC12.pmthresholds.sts1.nearend.1day.PJCDIFF	5760 (count)	0–1382400000
OC12.pmthresholds.sts1.nearend.1day.PJCS-PDET	9600 (seconds)	0–86400
OC12.pmthresholds.sts1.nearend.1day.PJCS-PGEN	9600 (seconds)	0–86400
OC12.pmthresholds.sts1.nearend.1day.PPJC-PDET	5760 (count)	0–691200000
OC12.pmthresholds.sts1.nearend.1day.PPJC-PGEN	5760 (count)	0–691200000
OC12.pmthresholds.sts1.nearend.1day.SES	7 (seconds)	0–86400
OC12.pmthresholds.sts1.nearend.1day.UAS	10 (seconds)	0–86400
OC12.pmthresholds.sts12c.nearend.15min.CV	75 (B3 count)	0–2160000
OC12.pmthresholds.sts12c.nearend.15min.ES	60 (seconds)	0–900
OC12.pmthresholds.sts12c.nearend.15min.FC	10 (count)	0–72
OC12.pmthresholds.sts12c.nearend.15min.NPJC-PDET	60 (count)	0–7200000
OC12.pmthresholds.sts12c.nearend.15min.NPJC-PGEN	60 (count)	0–7200000
OC12.pmthresholds.sts12c.nearend.15min.PJCDIFF	60 (count)	0–14400000
OC12.pmthresholds.sts12c.nearend.15min.PJCS-PDET	100 (seconds)	0–900
OC12.pmthresholds.sts12c.nearend.15min.PJCS-PGEN	100 (seconds)	0–900
OC12.pmthresholds.sts12c.nearend.15min.PPJC-PDET	60 (count)	0–7200000
OC12.pmthresholds.sts12c.nearend.15min.PPJC-PGEN	60 (count)	0–7200000
OC12.pmthresholds.sts12c.nearend.15min.SES	3 (seconds)	0–900
OC12.pmthresholds.sts12c.nearend.15min.UAS	10 (seconds)	0–900
OC12.pmthresholds.sts12c.nearend.1day.CV	750 (B3 count)	0–207360000
OC12.pmthresholds.sts12c.nearend.1day.ES	600 (seconds)	0–86400

Table C-4 OC-12 Card Default Settings (continued)

Default Name	Default Value	Default Domain
OC12.pmthresholds.sts12c.nearend.1day.FC	40 (count)	0–6912
OC12.pmthresholds.sts12c.nearend.1day.NPJC-PDET	5760 (count)	0–691200000
OC12.pmthresholds.sts12c.nearend.1day.NPJC-PGEN	5760 (count)	0–691200000
OC12.pmthresholds.sts12c.nearend.1day.PJCDIFF	5760 (count)	0–1382400000
OC12.pmthresholds.sts12c.nearend.1day.PJCS-PDET	9600 (seconds)	0–86400
OC12.pmthresholds.sts12c.nearend.1day.PJCS-PGEN	9600 (seconds)	0–86400
OC12.pmthresholds.sts12c.nearend.1day.PPJC-PDET	5760 (count)	0–691200000
OC12.pmthresholds.sts12c.nearend.1day.PPJC-PGEN	5760 (count)	0–691200000
OC12.pmthresholds.sts12c.nearend.1day.SES	7 (seconds)	0–86400
OC12.pmthresholds.sts12c.nearend.1day.UAS	10 (seconds)	0–86400
OC12.pmthresholds.sts3c-9c.nearend.15min.CV	25 (B3 count)	0–2160000
OC12.pmthresholds.sts3c-9c.nearend.15min.ES	20 (seconds)	0–900
OC12.pmthresholds.sts3c-9c.nearend.15min.FC	10 (count)	0–72
OC12.pmthresholds.sts3c-9c.nearend.15min.NPJC-PDET	60 (count)	0–7200000
OC12.pmthresholds.sts3c-9c.nearend.15min.NPJC-PGEN	60 (count)	0–7200000
OC12.pmthresholds.sts3c-9c.nearend.15min.PJCDIFF	60 (count)	0–14400000
OC12.pmthresholds.sts3c-9c.nearend.15min.PJCS-PDET	100 (seconds)	0–900
OC12.pmthresholds.sts3c-9c.nearend.15min.PJCS-PGEN	100 (seconds)	0–900
OC12.pmthresholds.sts3c-9c.nearend.15min.PPJC-PDET	60 (count)	0–7200000
OC12.pmthresholds.sts3c-9c.nearend.15min.PPJC-PGEN	60 (count)	0–7200000
OC12.pmthresholds.sts3c-9c.nearend.15min.SES	3 (seconds)	0–900
OC12.pmthresholds.sts3c-9c.nearend.15min.UAS	10 (seconds)	0–900
OC12.pmthresholds.sts3c-9c.nearend.1day.CV	250 (B3 count)	0–207360000
OC12.pmthresholds.sts3c-9c.nearend.1day.ES	200 (seconds)	0–86400
OC12.pmthresholds.sts3c-9c.nearend.1day.FC	40 (count)	0–6912
OC12.pmthresholds.sts3c-9c.nearend.1day.NPJC-PDET	5760 (count)	0–691200000
OC12.pmthresholds.sts3c-9c.nearend.1day.NPJC-PGEN	5760 (count)	0–691200000
OC12.pmthresholds.sts3c-9c.nearend.1day.PJCDIFF	5760 (count)	0–1382400000
OC12.pmthresholds.sts3c-9c.nearend.1day.PJCS-PDET	9600 (seconds)	0–86400
OC12.pmthresholds.sts3c-9c.nearend.1day.PJCS-PGEN	9600 (seconds)	0–86400
OC12.pmthresholds.sts3c-9c.nearend.1day.PPJC-PDET	5760 (count)	0–691200000
OC12.pmthresholds.sts3c-9c.nearend.1day.PPJC-PGEN	5760 (count)	0–691200000
OC12.pmthresholds.sts3c-9c.nearend.1day.SES	7 (seconds)	0–86400
OC12.pmthresholds.sts3c-9c.nearend.1day.UAS	10 (seconds)	0–86400

C.2.5 OC-48 Card Default Settings

Table C-5 lists the OC-48 card default settings.

Table C-5 OC-48 Card Default Settings

Default Name	Default Value	Default Domain
OC48.config.line.AdminSSMIn	STU	PRS, STU, ST2, TNC, ST3E, ST3, SMC, ST4, DUS, RES
OC48.config.line.AINSSoakTime	08:00 (hours:mins)	00:00, 00:15, 00:30 .. 48:00
OC48.config.line.PJStsMon#	0 (STS #)	0–48
OC48.config.line.SDBER	1E-7	1E-5, 1E-6, 1E-7, 1E-8, 1E-9
OC48.config.line.Send<FF>DoNotUse	FALSE	• FALSE when SendDoNotUse is TRUE • FALSE, TRUE when SendDoNotUse is FALSE
OC48.config.line.SendDoNotUse	FALSE	FALSE, TRUE
OC48.config.line.SFBER	1E-4	1E-3, 1E-4, 1E-5
OC48.config.line.State	IS,AINS	IS; OOS,DSBLD; OOS,MT; IS,AINS
OC48.config.line.SyncMsgIn	TRUE	FALSE, TRUE
OC48.config.sts.IPPMEnabled	FALSE	TRUE, FALSE
OC48.pmthresholds.line.farend.15min.CV	21260 (B2 count)	0–2212200
OC48.pmthresholds.line.farend.15min.ES	87 (seconds)	0–900
OC48.pmthresholds.line.farend.15min.FC	10 (count)	0–72
OC48.pmthresholds.line.farend.15min.SES	1 (seconds)	0–900
OC48.pmthresholds.line.farend.15min.UAS	3 (seconds)	0–900
OC48.pmthresholds.line.farend.1day.CV	212600 (B2 count)	0–212371200
OC48.pmthresholds.line.farend.1day.ES	864 (seconds)	0–86400
OC48.pmthresholds.line.farend.1day.FC	40 (count)	0–6912
OC48.pmthresholds.line.farend.1day.SES	4 (seconds)	0–86400
OC48.pmthresholds.line.farend.1day.UAS	10 (seconds)	0–86400
OC48.pmthresholds.line.nearend.15min.CV	21260 (B2 count)	0–2212200
OC48.pmthresholds.line.nearend.15min.ES	87 (seconds)	0–900
OC48.pmthresholds.line.nearend.15min.FC	10 (count)	0–72
OC48.pmthresholds.line.nearend.15min.PSC	1 (count)	0–600
OC48.pmthresholds.line.nearend.15min.PSC-R	1 (count)	0–600
OC48.pmthresholds.line.nearend.15min.PSC-S	1 (count)	0–600
OC48.pmthresholds.line.nearend.15min.PSC-W	1 (count)	0–600
OC48.pmthresholds.line.nearend.15min.PSD	300 (seconds)	0–900
OC48.pmthresholds.line.nearend.15min.PSD-R	300 (seconds)	0–900
OC48.pmthresholds.line.nearend.15min.PSD-S	300 (seconds)	0–900

Table C-5 OC-48 Card Default Settings (continued)

Default Name	Default Value	Default Domain
OC48.pmthresholds.line.nearend.15min.PSD-W	300 (seconds)	0–900
OC48.pmthresholds.line.nearend.15min.SES	1 (seconds)	0–900
OC48.pmthresholds.line.nearend.15min.UAS	3 (seconds)	0–900
OC48.pmthresholds.line.nearend.1day.CV	212600 (B2 count)	0–212371200
OC48.pmthresholds.line.nearend.1day.ES	864 (seconds)	0–86400
OC48.pmthresholds.line.nearend.1day.FC	40 (count)	0–6912
OC48.pmthresholds.line.nearend.1day.PSC	5 (count)	0–57600
OC48.pmthresholds.line.nearend.1day.PSC-R	5 (count)	0–57600
OC48.pmthresholds.line.nearend.1day.PSC-S	5 (count)	0–57600
OC48.pmthresholds.line.nearend.1day.PSC-W	5 (count)	0–57600
OC48.pmthresholds.line.nearend.1day.PSD	600 (seconds)	0–86400
OC48.pmthresholds.line.nearend.1day.PSD-R	600 (seconds)	0–86400
OC48.pmthresholds.line.nearend.1day.PSD-S	600 (seconds)	0–86400
OC48.pmthresholds.line.nearend.1day.PSD-W	600 (seconds)	0–86400
OC48.pmthresholds.line.nearend.1day.SES	4 (seconds)	0–86400
OC48.pmthresholds.line.nearend.1day.UAS	10 (seconds)	0–86400
OC48.pmthresholds.section.nearend.15min.CV	10000 (B1 count)	0–2151900
OC48.pmthresholds.section.nearend.15min.ES	500 (seconds)	0–900
OC48.pmthresholds.section.nearend.15min.SEFS	500 (seconds)	0–900
OC48.pmthresholds.section.nearend.15min.SES	500 (seconds)	0–900
OC48.pmthresholds.section.nearend.1day.CV	100000 (B1 count)	0–206582400
OC48.pmthresholds.section.nearend.1day.ES	5000 (seconds)	0–86400
OC48.pmthresholds.section.nearend.1day.SEFS	5000 (seconds)	0–86400
OC48.pmthresholds.section.nearend.1day.SES	5000 (seconds)	0–86400
OC48.pmthresholds.sts1.nearend.15min.CV	15 (B3 count)	0–2160000
OC48.pmthresholds.sts1.nearend.15min.ES	12 (seconds)	0–900
OC48.pmthresholds.sts1.nearend.15min.FC	10 (count)	0–72
OC48.pmthresholds.sts1.nearend.15min.NPJC-PDET	60 (count)	0–7200000
OC48.pmthresholds.sts1.nearend.15min.NPJC-PGEN	60 (count)	0–7200000
OC48.pmthresholds.sts1.nearend.15min.PJCDIFF	60 (count)	0–14400000
OC48.pmthresholds.sts1.nearend.15min.PJCS-PDET	100 (seconds)	0–900
OC48.pmthresholds.sts1.nearend.15min.PJCS-PGEN	100 (seconds)	0–900
OC48.pmthresholds.sts1.nearend.15min.PPJC-PDET	60 (count)	0–7200000
OC48.pmthresholds.sts1.nearend.15min.PPJC-PGEN	60 (count)	0–7200000
OC48.pmthresholds.sts1.nearend.15min.SES	3 (seconds)	0–900
OC48.pmthresholds.sts1.nearend.15min.UAS	10 (seconds)	0–900

Table C-5 OC-48 Card Default Settings (continued)

Default Name	Default Value	Default Domain
OC48.pmthresholds.sts1.nearend.1day.CV	125 (B3 count)	0–207360000
OC48.pmthresholds.sts1.nearend.1day.ES	100 (seconds)	0–86400
OC48.pmthresholds.sts1.nearend.1day.FC	40 (count)	0–6912
OC48.pmthresholds.sts1.nearend.1day.NPJC-PDET	5760 (count)	0–691200000
OC48.pmthresholds.sts1.nearend.1day.NPJC-PGEN	5760 (count)	0–691200000
OC48.pmthresholds.sts1.nearend.1day.PJCDIFF	5760 (count)	0–1382400000
OC48.pmthresholds.sts1.nearend.1day.PJCS-PDET	9600 (seconds)	0–86400
OC48.pmthresholds.sts1.nearend.1day.PJCS-PGEN	9600 (seconds)	0–86400
OC48.pmthresholds.sts1.nearend.1day.PPJC-PDET	5760 (count)	0–691200000
OC48.pmthresholds.sts1.nearend.1day.PPJC-PGEN	5760 (count)	0–691200000
OC48.pmthresholds.sts1.nearend.1day.SES	7 (seconds)	0–86400
OC48.pmthresholds.sts1.nearend.1day.UAS	10 (seconds)	0–86400
OC48.pmthresholds.sts12c-48c.nearend.15min.CV	75 (B3 count)	0–2160000
OC48.pmthresholds.sts12c-48c.nearend.15min.ES	60 (seconds)	0–900
OC48.pmthresholds.sts12c-48c.nearend.15min.FC	10 (count)	0–72
OC48.pmthresholds.sts12c-48c.nearend.15min.NPJC-PDET	60 (count)	0–7200000
OC48.pmthresholds.sts12c-48c.nearend.15min.NPJC-PGEN	60 (count)	0–7200000
OC48.pmthresholds.sts12c-48c.nearend.15min.PJCDIFF	60 (count)	0–14400000
OC48.pmthresholds.sts12c-48c.nearend.15min.PJCS-PDET	100 (seconds)	0–900
OC48.pmthresholds.sts12c-48c.nearend.15min.PJCS-PGEN	100 (seconds)	0–900
OC48.pmthresholds.sts12c-48c.nearend.15min.PPJC-PDET	60 (count)	0–7200000
OC48.pmthresholds.sts12c-48c.nearend.15min.PPJC-PGEN	60 (count)	0–7200000
OC48.pmthresholds.sts12c-48c.nearend.15min.SES	3 (seconds)	0–900
OC48.pmthresholds.sts12c-48c.nearend.15min.UAS	10 (seconds)	0–900
OC48.pmthresholds.sts12c-48c.nearend.1day.CV	750 (B3 count)	0–207360000
OC48.pmthresholds.sts12c-48c.nearend.1day.ES	600 (seconds)	0–86400
OC48.pmthresholds.sts12c-48c.nearend.1day.FC	40 (count)	0–6912
OC48.pmthresholds.sts12c-48c.nearend.1day.NPJC-PDET	5760 (count)	0–691200000
OC48.pmthresholds.sts12c-48c.nearend.1day.NPJC-PGEN	5760 (count)	0–691200000
OC48.pmthresholds.sts12c-48c.nearend.1day.PJCDIFF	5760 (count)	0–1382400000
OC48.pmthresholds.sts12c-48c.nearend.1day.PJCS-PDET	9600 (seconds)	0–86400
OC48.pmthresholds.sts12c-48c.nearend.1day.PJCS-PGEN	9600 (seconds)	0–86400
OC48.pmthresholds.sts12c-48c.nearend.1day.PPJC-PDET	5760 (count)	0–691200000
OC48.pmthresholds.sts12c-48c.nearend.1day.PPJC-PGEN	5760 (count)	0–691200000
OC48.pmthresholds.sts12c-48c.nearend.1day.SES	7 (seconds)	0–86400
OC48.pmthresholds.sts12c-48c.nearend.1day.UAS	10 (seconds)	0–86400

Table C-5 OC-48 Card Default Settings (continued)

Default Name	Default Value	Default Domain
OC48.pmthresholds.sts3c-9c.nearend.15min.CV	25 (B3 count)	0–2160000
OC48.pmthresholds.sts3c-9c.nearend.15min.ES	20 (seconds)	0–900
OC48.pmthresholds.sts3c-9c.nearend.15min.FC	10 (count)	0–72
OC48.pmthresholds.sts3c-9c.nearend.15min.NPJC-PDET	60 (count)	0–7200000
OC48.pmthresholds.sts3c-9c.nearend.15min.NPJC-PGEN	60 (count)	0–7200000
OC48.pmthresholds.sts3c-9c.nearend.15min.PJCDIFF	60 (count)	0–14400000
OC48.pmthresholds.sts3c-9c.nearend.15min.PJCS-PDET	100 (seconds)	0–900
OC48.pmthresholds.sts3c-9c.nearend.15min.PJCS-PGEN	100 (seconds)	0–900
OC48.pmthresholds.sts3c-9c.nearend.15min.PPJC-PDET	60 (count)	0–7200000
OC48.pmthresholds.sts3c-9c.nearend.15min.PPJC-PGEN	60 (count)	0–7200000
OC48.pmthresholds.sts3c-9c.nearend.15min.SES	3 (seconds)	0–900
OC48.pmthresholds.sts3c-9c.nearend.15min.UAS	10 (seconds)	0–900
OC48.pmthresholds.sts3c-9c.nearend.1day.CV	250 (B3 count)	0–207360000
OC48.pmthresholds.sts3c-9c.nearend.1day.ES	200 (seconds)	0–86400
OC48.pmthresholds.sts3c-9c.nearend.1day.FC	40 (count)	0–6912
OC48.pmthresholds.sts3c-9c.nearend.1day.NPJC-PDET	5760 (count)	0–691200000
OC48.pmthresholds.sts3c-9c.nearend.1day.NPJC-PGEN	5760 (count)	0–691200000
OC48.pmthresholds.sts3c-9c.nearend.1day.PJCDIFF	5760 (count)	0–1382400000
OC48.pmthresholds.sts3c-9c.nearend.1day.PJCS-PDET	9600 (seconds)	0–86400
OC48.pmthresholds.sts3c-9c.nearend.1day.PJCS-PGEN	9600 (seconds)	0–86400
OC48.pmthresholds.sts3c-9c.nearend.1day.PPJC-PDET	5760 (count)	0–691200000
OC48.pmthresholds.sts3c-9c.nearend.1day.PPJC-PGEN	5760 (count)	0–691200000
OC48.pmthresholds.sts3c-9c.nearend.1day.SES	7 (seconds)	0–86400
OC48.pmthresholds.sts3c-9c.nearend.1day.UAS	10 (seconds)	0–86400

C.2.6 G-1000-2 Card Default Settings

Table C-6 lists the G-1000-2 card default settings.

Table C-6 G-1000 Card Default Settings

Default Name	Default Value	Default Domain
G1000.config.AINSSoakTime	08:00 (hours:mins)	00:00, 00:15, 00:30 .. 48:00
G1000.config.State	OOS,DSBLD	IS; OOS,DSBLD; OOS,MT; IS,AINS

C.3 Node Default Settings

Table C-7 on page C-18 lists the node-level default settings for the Cisco ONS 15327. Cisco provides the following user-configurable defaults for each Cisco ONS 15327 node:

- Create TL1-Like—Instructs the node to create only cross-connects, allowing the resulting circuits to be in an upgradable state.
- Insert AIS-V on SDP—Instructs the node to insert Virtual Tributary (VT) alarm indication signal (AIS-V) in each VT whenever the carrying STS crosses the signal degrade path BER threshold.
- SDP BER—Defines the node signal degrade path bit error rate.
- Path protection settings—Set the threshold level for signal degradation and failure for path protection circuits.
- Craft Access Only—Allows CTC connectivity to the node only through the craft access port.
- CTC IP Display Suppression—Prevents display of node IP addresses in CTC (applicable for all users except Superusers).
- Defaults Description—Names the current defaults file on the node.
- Enable Firewall—Enables or disables the use of a firewall for accessing the node.
- IIOP Listener Port—Sets the Internet Inter-Object Request Broker Protocol (IIOP) listener port number.
- Login Warning Message—Warns users at the login screen about the possible legal or contractual ramifications of accessing equipment, systems, or networks without authorization.
- NTP/SNTP Server—Sets the IP address of the Network Time Protocol (NTP) / Simple Network Time Protocol (SNTP) server to be used with the node.
- Time Zone—Sets the time zone where the node is located.
- Use DST—Enables or disables the use of Daylight Savings Time (DST).
- 1+1 protection settings—Determine whether or not 1+1 protected circuits have bidirectional switching, are revertive, and what the reversion time is.
- BLSR Protection settings—Determine whether bidirectional line switched ring (BLSR)-protected circuits are revertive and what the reversion time is at both the ring and span levels.
- Security Policy settings—Determine 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 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.
- BITS Timing settings—Determine the AIS threshold, coding, framing, State, State Out, and line build out (LBO) settings for BITS1 and BITS2 timing.
- General Timing settings—Determine the mode (External, Line, or Mixed), quality of RES, 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 15327 Procedure Guide*.

Table C-7 Node Default Settings

Default Name	Default Value	Default Domain
NODE.circuits.SendPDIP	FALSE	TRUE, FALSE
NODE.circuits.State	IS,AINS	IS; OOS,DSBLD; OOS,MT; IS,AINS
NODE.circuits.upsr.ReversionTime	5.0 (minutes)	0.5, 1.0, 1.5 .. 12.0
NODE.circuits.upsr.Revertive	FALSE	TRUE, FALSE
NODE.circuits.upsr.STS_SDBER	1E-6	1E-5, 1E-6, 1E-7, 1E-8, 1E-9
NODE.circuits.upsr.STS_SFBER	1E-4	1E-3, 1E-4, 1E-5
NODE.circuits.upsr.SwitchOnPDIP	FALSE	TRUE, FALSE
NODE.circuits.upsr.VT_SDBER	1E-6	1E-5, 1E-6, 1E-7, 1E-8, 1E-9
NODE.circuits.upsr.VT_SFBER	1E-4	1E-3, 1E-4, 1E-5
NODE.general.DefaultsDescription	Factory Defaults	Free form field
NODE.general.InsertAISVOnSDP	FALSE	TRUE, FALSE
NODE.general.NtpSntpServer	0.0.0.0	IP Address
NODE.general.SDPBER	1E-6	1E-5, 1E-6, 1E-7, 1E-8, 1E-9
NODE.general.TimeZone	(GMT-08:00) Pacific Time (US & Canada), Tijuana	(For applicable time zones, see Table C-8 on page C-22.)
NODE.general.UseDST	TRUE	TRUE, FALSE
NODE.network.general.CtcIpDisplaySuppression	FALSE	TRUE, FALSE
NODE.network.general.GatewaySettings	None	LeaveAsIs, None, ENE, GNE, ProxyOnlyNode
NODE.osi.greTunnel.ctc.OspfCost	110	110, 120, 130 .. 65530
NODE.osi.greTunnel.ctc.SubnetMask	24 (bits)	8, 9, 10 .. 32
NODE.osi.lapd.ctc.Mode	AITS	AITS, UITS
NODE.osi.lapd.ctc.MTU	512	512, 513, 514 .. 1500
NODE.osi.lapd.ctc.Role	Network	Network, User
NODE.osi.lapd.ctc.T200	200 (ms)	200, 300, 400 .. 20000
NODE.osi.lapd.ctc.T203	10000 (ms)	4000, 4100, 4200 .. 120000

Table C-7 Node Default Settings (continued)

Default Name	Default Value	Default Domain
NODE.osi.mainSetup.L1LSPBufferSize	512 (bytes)	512–1500
NODE.osi.mainSetup.NodeRoutingMode	End System	End System, Intermediate System Level 1
NODE.osi.subnet.ctc.DISPriority	63	1, 2, 3 .. 127
NODE.osi.subnet.ctc.ESH	10 (sec)	10, 20, 30 .. 1000
NODE.osi.subnet.ctc.IIH	3 (sec)	1, 2, 3 .. 600
NODE.osi.subnet.ctc.ISH	10 (sec)	10, 20, 30 .. 1000
NODE.osi.subnet.ctc.LANISISCost	20	1, 2, 3 .. 63
NODE.osi.subnet.ctc.SDCCISISCost	60	1, 2, 3 .. 63
NODE.osi.tarp.L1DataCache	TRUE	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 (sec)	0–1440
NODE.osi.tarp.PDUsL1Propagation	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.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.blsr.RingReversionTime	5.0 (minutes)	0.5, 1.0, 1.5 .. 12.0
NODE.protection.blsr.RingRevertive	TRUE	TRUE, FALSE
NODE.protection.blsr.SpanReversionTime	5.0 (minutes)	0.5, 1.0, 1.5 .. 12.0
NODE.protection.blsr.SpanRevertive	TRUE	TRUE, FALSE
NODE.security.emsAccess.AccessState	NonSecure	NonSecure, Secure
NODE.security.emsAccess.IIOPListenerPort (May reboot node)	57790 (port #)	0–65535
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

Table C-7 Node Default Settings (continued)

Default Name	Default Value	Default Domain
NODE.security.idleUserTimeout.Superuser	00:15 (hours:mins)	00:00, 00:01, 00:02 .. 16:39
NODE.security.lanAccess.LANAccess (Might disconnect CTC from node)	Front Only	No LAN Access, Front Only
NODE.security.lanAccess.RestoreTimeout	5 (minutes)	0–60
NODE.security.legalDisclaimer.LoginWarningMessage	<html> WARNING This system is restricted to authorized users for business purposes. Unauthorized <p>access is a violation of the law. This service may be monitored for administrative <p>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 DisableInactiveUser is TRUE • 45 (and N/A) when DisableInactiveUser is FALSE
NODE.security.other.PMClearingPrivilege	Provisioning	Provisioning, Superuser
NODE.security.other.SingleSessionPerUser	FALSE	TRUE, FALSE
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

Table C-7 Node Default Settings (continued)

Default Name	Default Value	Default Domain
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.radiusServer.EnableNodeAsFinalAuthenticatorWhenAuthenticationEnabled	TRUE	FALSE, TRUE
NODE.security.serialCraftAccess.EnableCraftPort	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
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.shelf.security.radiusServer.ctc.AccountingPort	1813 (port)	0–32767
NODE.shelf.security.radiusServer.ctc.AuthenticationPort	1812 (port)	0–32767
NODE.timing.bits-1.AdminSSMIn	STU	PRS, STU, ST2, TNC, ST3E, ST3, SMC, ST4, DUS, RES
NODE.timing.bits-1.AISThreshold	SMC	PRS, STU, ST2, TNC, ST3E, ST3, SMC, ST4, DUS, RES
NODE.timing.bits-1.Coding	B8ZS	B8ZS, AMI
NODE.timing.bits-1.CodingOut	B8ZS	B8ZS, AMI
NODE.timing.bits-1.Framing	ESF	ESF, D4
NODE.timing.bits-1.FramingOut	ESF	ESF, D4
NODE.timing.bits-1.LBO	0-133	0-133, 134-266, 267-399, 400-533, 534-655
NODE.timing.bits-1.State	IS	IS, OOS,DSBLD
NODE.timing.bits-1.StateOut	IS	IS, OOS,DSBLD
NODE.timing.bits-2.AdminSSMIn	STU	PRS, STU, ST2, TNC, ST3E, ST3, SMC, ST4, DUS, RES
NODE.timing.bits-2.AISThreshold	SMC	PRS, STU, ST2, TNC, ST3E, ST3, SMC, ST4, DUS, RES

Table C-7 Node Default Settings (continued)

Default Name	Default Value	Default Domain
NODE.timing.bits-2.Coding	B8ZS	B8ZS, AMI
NODE.timing.bits-2.CodingOut	B8ZS	B8ZS, AMI
NODE.timing.bits-2.Framing	ESF	ESF, D4
NODE.timing.bits-2.FramingOut	ESF	ESF, D4
NODE.timing.bits-2.LBO	0-133	0-133, 134-266, 267-399, 400-533, 534-655
NODE.timing.bits-2.State	IS	IS, OOS,DSBLD
NODE.timing.bits-2.StateOut	IS	IS, OOS,DSBLD
NODE.timing.general.Mode	External	External, Line, Mixed
NODE.timing.general.QualityOfRES	RES=DUS	• PRS<RES, STU<RES<PRS, ST2<RES<STU, ST3<RES<ST2, SMC<RES<ST3, ST4<RES<SMC, RES<ST4, RES=DUS when SSMMessageSet is Generation 1 • PRS<RES, STU<RES<PRS, ST2<RES<STU, TNC<RES<ST2, ST3E<RES<TNC, ST3<RES<ST3E, SMC<RES<ST3, ST4<RES<SMC, RES<ST4, RES=DUS when SSMMessageSet is Generation 2
NODE.timing.general.ReversionTime	5.0 (minutes)	0.5, 1.0, 1.5 .. 12.0
NODE.timing.general.Revertive	FALSE	TRUE, FALSE
NODE.timing.general.SSMMessageSet	Generation 1	Generation 1, Generation 2

C.3.1 Time Zones

Table C-8 lists the time zones that apply for node time zone defaults. Time zones are expressed in terms of their relative relationships to Greenwich Mean Time (GMT).

Table C-8 Time Zones

Time Zone (GMT +/- Hours)	Location(s)
GMT-11:00	Midway Islands, Samoa
GMT-10:00	Hawaiian Islands, Tahiti

Table C-8 Time Zones (continued)

Time Zone (GMT +/- Hours)	Location(s)
GMT-09:00	Anchorage - Alaska
GMT-08:00	Pacific Time (US & Canada), Tijuana
GMT-07:00	Mountain Time (US & Canada)
GMT-07:00	Phoenix - Arizona
GMT-06:00	Central Time (US & Canada)
GMT-06:00	Mexico City
GMT-06:00	Costa Rica, Managua, San Salvador
GMT-06:00	Saskatchewan, Manitoba
GMT-05:00	Bogota, Lima, Quito
GMT-05:00	Eastern Time (US & Canada)
GMT-05:00	Havana
GMT-05:00	Indiana (US)
GMT-04:00	Asuncion
GMT-04:00	Caracas, La Paz, San Juan
GMT-04:00	Atlantic Time (Canada), Halifax, Saint John, Charlottetown
GMT-04:00	Santiago
GMT-04:00	Thule (Qaanaaq)
GMT-03:30	St. John's - Newfoundland
GMT-03:00	Brasilia, Rio de Janeiro, Sao Paulo
GMT-03:00	Buenos Aires, Georgetown
GMT-03:00	Godthab (Nuuk) - Greenland
GMT-02:00	Mid-Atlantic
GMT-01:00	Azores, Scoresbysund
GMT-01:00	Praia - Cape Verde
GMT 00:00	Casablanca, Reykjavik, Monrovia
GMT	Greenwich Mean Time
GMT 00:00	Dublin, Edinburgh, London, Lisbon
GMT+01:00	Amsterdam, Berlin, Rome, Stockholm, Paris
GMT+01:00	Belgrade, Bratislava, Budapest, Ljubljana, Prague
GMT+01:00	Brussels, Copenhagen, Madrid, Vienna
GMT+01:00	Sarajevo, Skopje, Sofija, Vilnius, Warsaw, Zagreb
GMT+01:00	West Central Africa, Algiers, Lagos, Luanda
GMT+01:00	Windhoek (Namibia)
GMT+02:00	Al Jizah, Alexandria, Cairo
GMT+02:00	Amman
GMT+02:00	Athens, Bucharest, Istanbul

Table C-8 Time Zones (continued)

Time Zone (GMT +/- Hours)	Location(s)
GMT+02:00	Beirut
GMT+02:00	Cape Town, Harare, Johannesburg, Pretoria
GMT+02:00	Jerusalem
GMT+02:00	Kaliningrad, Minsk
GMT+03:00	Aden, Antananarivo, Khartoum, Nairobi
GMT+03:00	Baghdad
GMT+03:00	Kuwait, Riyadh
GMT+03:00	Moscow, St. Petersburg, Novgorod
GMT+03:30	Tehran
GMT+04:00	Abu Dhabi, Mauritius, Muscat
GMT+04:00	Aqtau, T'bilisi
GMT+04:00	Baku
GMT+04:00	Yerevan, Samara
GMT+04:30	Kabul
GMT+05:00	Chelyabinsk, Prem, Yekaterinburg, Ufa
GMT+05:00	Islamabad, Karachi, Tashkent
GMT+05:30	Calcutta, Mumbai, New Delhi, Chennai
GMT+05:45	Kathmandu
GMT+06:00	Almaty
GMT+06:00	Colombo, Dhaka, Astana
GMT+06:00	Novosibirsk, Omsk
GMT+06:30	Cocos, Rangoon
GMT+07:00	Bangkok, Hanoi, Jakarta
GMT+07:00	Krasnoyarsk, Norilsk, Novokuznetsk
GMT+08:00	Irkutsk, Ulaan Bataar
GMT+08:00	Beijing, Shanghai, Hong Kong, Urumqi
GMT+08:00	Perth
GMT+08:00	Singapore, Manila, Taipei, Kuala Lumpur
GMT+09:00	Chita, Yakutsk
GMT+09:00	Osaka, Sapporo, Tokyo
GMT+09:00	Palau, Pyongyang, Seoul
GMT+09:30	Adelaide, Broken Hill
GMT+09:30	Darwin
GMT+10:00	Brisbane, Port Moresby, Guam
GMT+10:00	Canberra, Melbourne, Sydney
GMT+10:00	Hobart

Table C-8 Time Zones (continued)

Time Zone (GMT +/- Hours)	Location(s)
GMT+10:00	Khabarovsk, Vladivostok
GMT+10:30	Lord Howe Island
GMT+11:00	Honiara, Magadan, Soloman Islands
GMT+11:00	Noumea - New Caledonia
GMT+11:30	Kingston - Norfolk Island
GMT+12:00	Andyra, Kamchatka
GMT+12:00	Auckland, Wellington
GMT+12:00	Marshall Islands, Eniwetok
GMT+12:00	Suva - Fiji
GMT+12:45	Chatham Island
GMT+13:00	Nuku'alofa - Tonga
GMT+13:00	Rawaki, Phoenix Islands
GMT+14:00	Line Islands, Kiritimati - Kiribati

C.4 CTC Default Settings

Table C-9 lists the CTC-level default settings for the Cisco ONS 15327. Cisco provides the following user-configurable defaults for CTC.

- Create circuits with the Route Automatically check box selected by default.
- Create TL1-like circuits—Instructs the node to create only cross-connects, allowing the resulting circuits to be in an upgradable state.
- Choose a default network map (which country).

Table C-9 CTC Default Settings

Default Name	Default Value	Default Domain
CTC.circuits.AutoRoute	TRUE	TRUE, FALSE
CTC.circuits.CreateLikeTL1	FALSE	TRUE, FALSE
CTC.network.Map	United States	-none-, Germany, Japan, Netherlands, South Korea, United Kingdom, United States

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X