Cisco ONS 15310-CL Reference Manual

Product and Documentation Release 6.0
September 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-7816902=
Text Part Number: 78-16902-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

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

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

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

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

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

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

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

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

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco ONS 15310-CL Reference Manual, Release 6.0

CONTENTS

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.

This section provides the following information:

Revision History

Date	Notes
March 2007	Revision History Table added for the first time
September 2007	Updated About this Manual chapter
April 2008	Updated alarm information in External Alarms and Controls section in Alarm Monitoring and Management chapter.
September 2008	Added a note in Card Default Settings and Node Default Settings section of Appendix C, Network Element Defaults.

Document Objectives

The *Cisco ONS 15310-CL Reference Manual* provides hardware and software reference information for Cisco ONS 15310 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 15310-CL 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 15310-CL-CTX card, CE-100T-8 card, ML100T-8 card, filler card, and SFP modules.
Chapter 3, “Port Protection”	Includes electrical and optical card protection methods.
Chapter 4, “Cisco Transport Controller Operation”	Includes information about CTC installation, the CTC window, computer requirements, software versions, and database reset and revert.
Chapter 5, “Security”	Includes information for user set up, privileges, seurity policies, audit trail, and RADIUS authentication.
Chapter 6, “Timing”	Includes node and network timing information.

Table 1 Cisco ONS 15310-CL Reference Manual Chapters (continued)

Title	Summary
Chapter 7, "Circuits and Tunnels"	Includes STS and VT, unidirectional, VCAT, 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 15310-CL; including 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 IP networking with the ONS 15310-CL.
Chapter 10, "Alarm Monitoring and Management"	Includes CTC alarm management information.
Appendix A, "Specifications"	Includes shelf assembly and card specifications.
Appendix B, "Administrative and Service States"	Describes card, port, and cross-connect service states.
Appendix C, "Network Element Defaults"	Lists card, node, and CTC-level network element (NE) defaults.

Related Documentation

Use the *Cisco ONS 15310-CL Reference Manual* in conjunction with the following referenced publications:

- *Cisco ONS 15310-CL Procedure Guide*
  Provides installation, turn up, test, and maintenance procedures.
- *Cisco ONS 15310-CL 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, AIDs, conditions and modifiers for the Cisco ONS 15454, ONS 15327, ONS 15600 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.
- *Cisco ONS 15310-CL Ethernet Card Software Feature and Configuration Guide*
  Provides the software features and operation of the ML-100T-8 and CE-100T-8 Ethernet cards for the Cisco ONS 15310-CL.
- *Release Notes for the Cisco ONS 15310-CL 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.
{ 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

Upozornenie

DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY

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

USCHOVAJTE SI TENTO NÁVOD

Obtaining Optical Networking Information

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

Where to Find Safety and Warning Information

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

Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15310 product documentation, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated periodically and may be more current than printed documentation.

Obtaining Documentation and Submitting a Service Request

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

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

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

Shelf Assembly Hardware

This chapter provides a description of Cisco ONS 15310-CL shelf hardware. Instructions for installing equipment are provided in the *Cisco ONS 15310-CL Procedure Guide*.

Chapter topics include:

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

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

1.1 Installation Overview

You can mount the ONS 15310-CL in a 19- or 23-inch (482.6 or 584.2 mm) rack or it can be placed on a flat surface using the installed rubber feet.

The shelf assembly weighs 11.5 pounds (5.22 kg) without a card installed and 12.5 pounds (5.67 kg) fully loaded. An ONS 15310-CL is installed in a rack using reversible mounting brackets on each side of the shelf.

The ONS 15310-CL is powered using –48 VDC or 100/240 VAC power. AC power terminals are accessible on the front panel and the DC power connection is accessed from the rear of the shelf assembly. The CRIT, MAJ, MIN, and REM alarm LEDs visible on the front of the node indicate whether a Critical, Major, Minor, or Remote alarm is present anywhere on the ONS 15310-CL assembly. These

LEDs help you to determine quickly if any alarms are present on the assembly. You can access the ONS 15310-CL Ethernet card, small form-factor pluggables (SFPs), cables, and ports through the front of the shelf assembly only.

When installed in an equipment rack, the ONS 15310-CL assembly is typically connected to a fuse and alarm panel that provides centralized alarm connection points and distributed power for the ONS 15310-CL. 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 15310-CL” and “shelf assembly” are used interchangeably. In the installation context, these terms have the same meaning. Otherwise, shelf assembly refers to the physical steel enclosure that holds cards and connects power, and ONS 15310-CL refers to the entire system, both hardware and software.

Install the ONS 15310-CL in compliance with your local and national electrical codes:

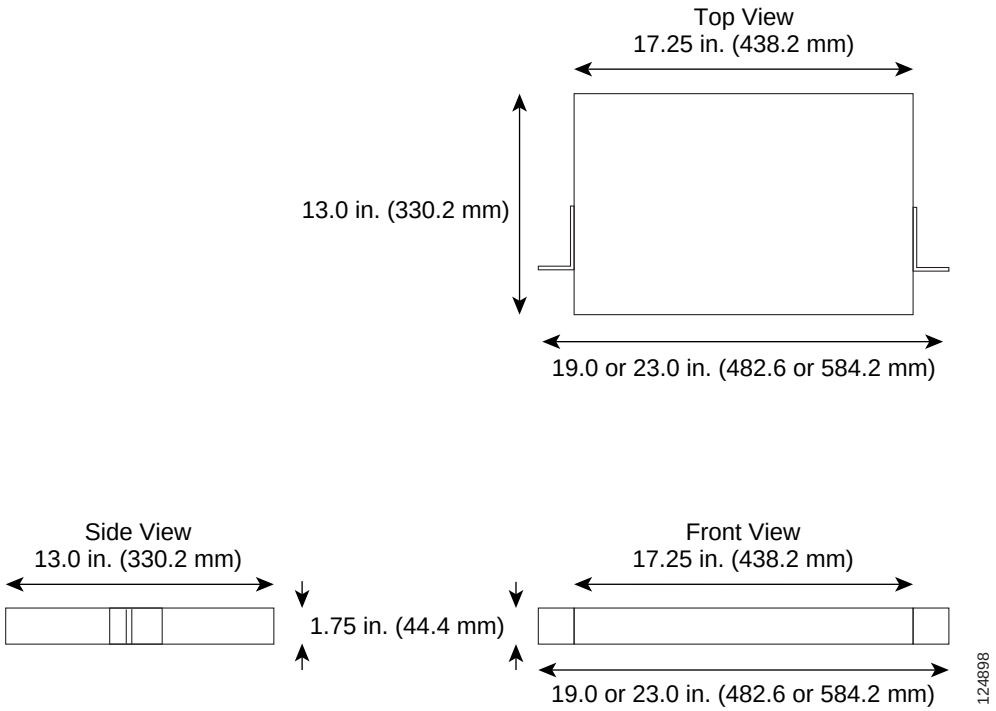
- United States: National Fire Protection Association (NFPA) 70; United States National Electrical Code
- Canada: Canadian Electrical Code, Part I, CSA C22.1
- Other countries: If local and national electrical codes, are not available, refer to IEC 364, Part 1 through Part 7

1.2 Rack Installation

The ONS 15310-CL is easily mounted in a 19- or 23-inch (482.6 or 584.2 mm) equipment rack. The shelf assembly can be mounted so that it projects five inches from the front of the rack. It mounts in both EIA-standard and Telcordia-standard racks. The shelf assembly is a total of 17.25 inches (438.2 mm) wide.

The ONS 15310-CL measures 1.75 inches high, 19 or 23 inches wide (depending on which brackets are installed), and 15 inches deep (44.4 x 482.6 or 584.2 x 381 mm). Figure 1-1 shows the dimensions of the ONS 15310-CL shelf assembly.

Figure 1-1 ONS 15310-CL Shelf Assembly Dimensions



1.2.1 Mounting Bracket

Caution Use only the fastening hardware provided with the ONS 15310-CL to prevent loosening, deterioration, and electromechanical corrosion of the hardware and joined material.

Caution When mounting the ONS 15310-CL in a frame with a non-conductive coating (such as paint, lacquer, or enamel) use either the thread-forming screws provided with the ONS 15310-CL shipping kit or remove the coating from the threads to ensure electrical continuity.

The shelf assembly comes with two mounting brackets, one for use with a 19-inch (482.6 mm) or 23-inch (584.2 mm) rack. Figure 1-2 shows the mounting bracket orientation for a 19-inch rack.

Figure 1-2 Mounting Brackets (23-Inch Orientation)

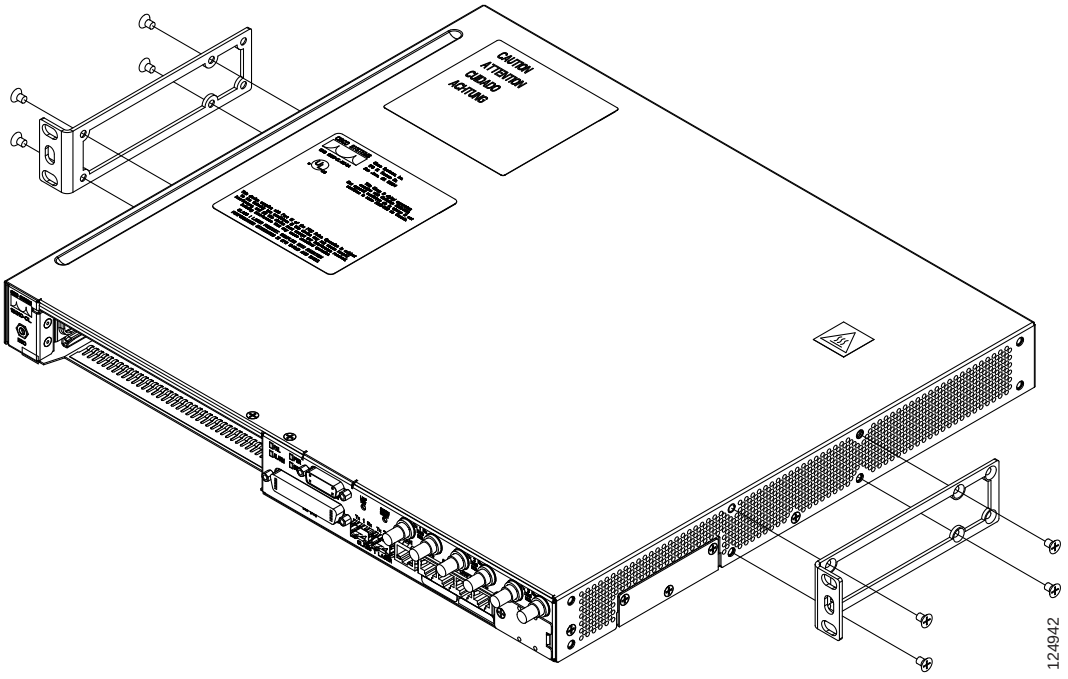
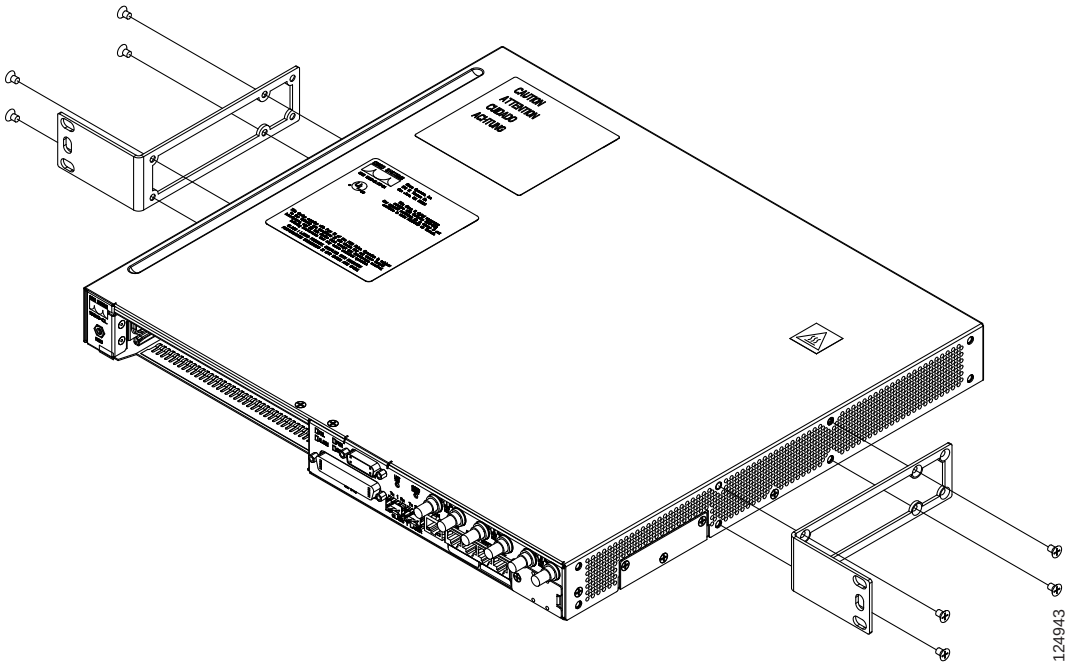


Figure 1-3 shows the mounting bracket orientations for a 23-inch rack. The brackets are installed in the same mounting holes for both rack sizes.

Figure 1-3 Mounting Brackets (19-Inch Orientation)



1.2.2 Mounting a Single Node

Mounting the ONS 15310-CL in a rack requires a minimum of 1.75 inches of vertical rack space (plus 1 inch [25.4 mm] for air flow). To ensure that the mounting is secure, use two #12-24 mounting screws for each side of the shelf assembly.

1.2.3 Mounting Multiple Nodes

Most standard seven-foot (2.1 m) racks can hold numerous ONS 15310-CL nodes and a fuse and alarm panel.

1.3 Power and Ground Description

This section describes how to connect the ONS 15310-CL shelf assembly to the power supply. For detailed procedures, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL Procedure Guide*. Terminate the chassis ground on the rear of the shelf assembly to either the office ground or rack ground before you install the power. Use the grounding lug to attach the #6 AWG 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 the 15310-CL-CTX card is reset, you must reset the ONS 15310-CL 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 15310-CL. Plug the wristband cable into the ESD jack located to the left of the expansion slot.

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 15310-CL can be ordered with either AC or DC power capability. The DC power option provides redundant –48 VDC power terminals on the rear of the chassis. The terminals are labeled A and B and are located at each end of the shelf assembly. The ONS 15310-CL AC power connector is located at the bottom right on the front of the chassis. The power cables are provided with the ship kit.

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 #14 AWG power cables and a #6 AWG ground cable and, to ensure circuit overcurrent protection, use a conductor with low impedance. However, the conductor must have the capability to safely conduct any fault current that might be imposed. Do not use aluminum conductors.

1.4 Cable Description and Installation

This section describes fiber-optic, DS-3/EC-1 (coaxial), DS-1 (96-pin LFH), UDC, and twisted-pair cables.

1.4.1 Cabling Types

The following types of cables are used with the ONS 15310-CL:

- Optical cables: The OC-3/12 signals operate over fiber spans via small form-factor pluggable (SFP) optics, including intermediate-reach (IR), and long-reach (LR) SFPs. Specification references can be found for the interface in ITU G.957 and GR-253. See "1.4.2 Fiber Cable Installation" section on page 1-6 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: Coaxial cables connect to the electrical ports using MiniBNC cable connectors. Coaxial cables carry DS-3/EC-1 traffic to and from the ONS 15310-CL. The ONS 15310-CL supports up to three transmit and three receive coaxial connectors on each shelf assembly.

Note Cisco recommends you use Cisco-orderable MiniBNC cables to ensure interoperability between the cables and Trompeter MiniBNC connectors on the ONS 15310-CL.

- LFH cables: A 96-pin LFH cable provides access to a maximum of 21 DS-1s. See the "1.4.4 DS-1 Cable Installation" section on page 1-7 for more information about the DS-1 cables and connectors.
- RJ-45 cables: RJ-45 cables connect to the alarm, LAN, CRAFT, UDC, and timing (BITS) ports. Shielded Twisted-pair (STP) #22 or #24 AWG wire is required for the CRAFT, and UDC ports. Unshielded Twisted-pair is sufficient for the alarm, LAN, and timing ports.

1.4.2 Fiber Cable Installation

To install fiber-optic cables on the ONS 15310-CL, a fiber cable with an LC connector must be connected to the SFPs installed in the SFP port on the ONS 15310-CL. The left side connector on the SFP 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.

Caution You must provide some type of strain relief for the cables, using either the tie-bars specifically designed for the ONS 15310-CL or a site-specific solution.

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

1.4.3 Coaxial Cable Installation

For DS-3/EC-1 traffic the ONS 15310-CL uses coaxial cables and connectors. Cisco recommends connecting a 735A coaxial cable to a patch panel. Use a compatible straight male BNC connector to connect the cable to the DS-3/EC-1 ports. The DS-3/EC-1 cables should be terminated with MiniBNC connectors on the ONS 15310-CL side and BNC connectors on the client side.

The electromagnetic compatibility (EMC) performance of the node depends on good-quality DS-3/EC-1 coaxial cables, such as Shuner Type G 03233 D, or the equivalent.

1.4.4 DS-1 Cable Installation

The ONS 15310-CL uses 96-pin LFH connector cabling for DS-1 connections.

1.4.5 Alarm Cable Installation

The alarm cables attach to the front of the 15310-CL using 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.

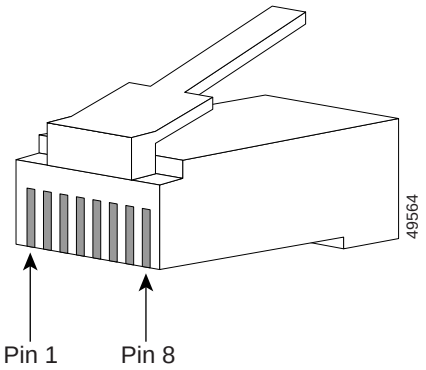
The pins on the ALARM port correspond to the three external alarm inputs and the two external alarm outputs (controls) that you can define using Cisco Transport Controller (CTC). Table 1-1 lists the input alarm pinouts and the corresponding alarm function numbers assigned to each port.

Table 1-1 Alarm Pin Assignments

RJ-45 Pin Number	Function
1	Alarm Contact 1+
2	Alarm Contact 1–
3	Alarm Contact 2+
4	Alarm Contact 2–
5	Alarm Input 1
6	Alarm Input 2
7	Alarm Input 3
8	Alarm Input Common

Figure 1-4 shows RJ-45 pin numbering.

Figure 1-4 Pins 1 and 8 on the RJ-45 Connector



For more information about external alarms and controls, see the "10.6 External Alarms and Controls" section on page 10-13.

1.4.6 BITS Cable Installation

The building integrated timing supply (BITS) cables attach to the ONS 15310-CL using BITS clock cable and twisted-pair #22 or #24 unshielded 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.

The 15310-CL has one BITS input and one BITS output. The BITS inputs and outputs have corresponding pins on the RJ-45 BITS ports. When connecting BITS cable to the ONS 15310-CL, see Table 1-2 for the BITS cable pin assignments.

For more information about connecting BITS timing to the ONS 15310-CL, refer to Chapter 6, "Timing.".

Table 1-2 BITS Cable Pin Assignments

RJ-45 Pin Number	Function
1	BITS Output+
2	BITS Output–
3	BITS Input+
4	—
5	—
6	BITS Input–
7	—
8	—

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

1.4.7 UDC Cable Installation

The 64K/RS-232 user data channel (UDC) interface provides E1, E2, F1, and F2 byte input and output. When connecting UDC cable to the ONS 15310-CL, see Table 1-3 for the UDC cable pin assignments. Shielded Twisted-pair (STP) #22 or #24 AWG wire is required for the UDC ports.

Table 1-3 UDC Cable Pin Assignments

Pin Number	Function (RS-232 Mode)	Function (64K Mode)
1	NC	TX+
2	DTR	TX–
3	TXD	RX+
4	GND	GND
5	GND	GND
6	RXC	RX–
7	NC	NC
8	NC	NC

1.5 Fans

The ONS 15310-CL has five fans permanently mounted to the inside of the chassis. The fans are not removable.

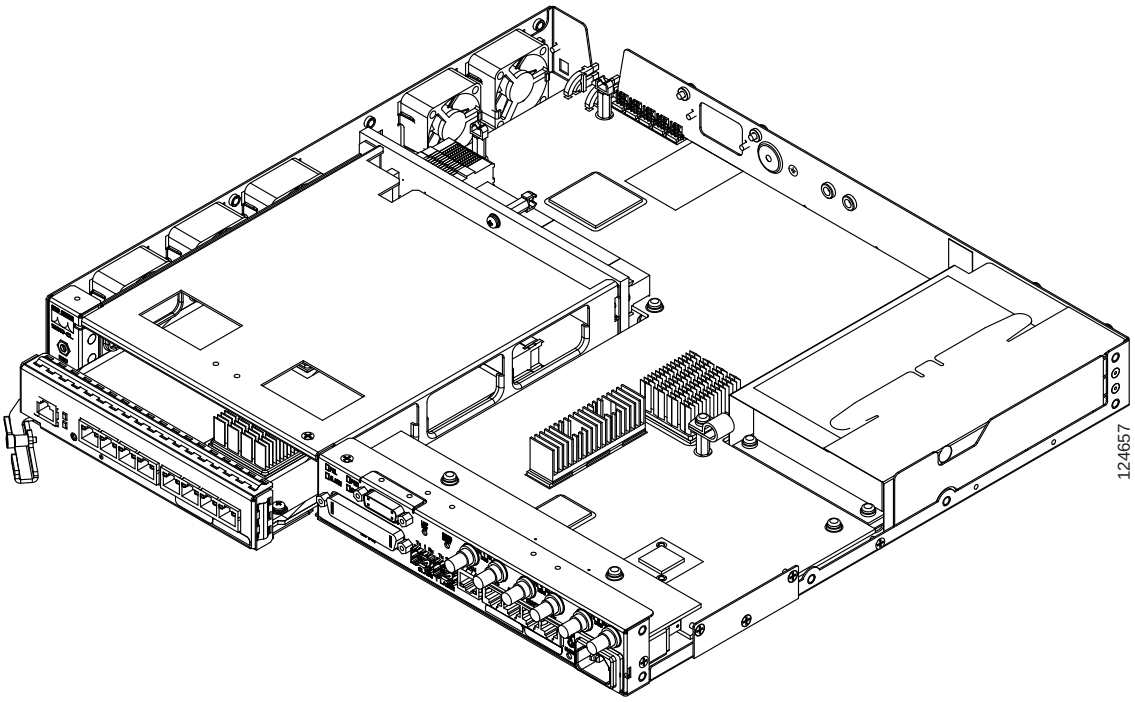
1.6 Cards and Slots

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

The ONS 15310-CL provides one expansion slot that can accommodate one of two Ethernet cards, the CE-100T-8 card or the ML-100T-8 card. These 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. Refer to Chapter 2, “Card Reference” for more information about ONS 15310-CL cards.

Figure 1-5 shows card installation for the ONS 15310-CL.

Figure 1-5 Installing an Ethernet Card



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

Table 1-4 lists the number of ports, line rates, connector options, and connector locations for ONS 15310-CL electrical, Ethernet, and optical interfaces.

Table 1-4 Port Line Rates, Connector Types, and Locations

Interface	Ports	Line Rate per Port	Connector Type	Connector Location
DS-1	21	1.544 Mbps	96-pin LFH	Front of the 15310-CL
DS-3	3	44.736 Mbps	75-ohm MiniBNC	Front of the 15310-CL
EC-1	3	51.84 Mbps	75-ohm MiniBNC	Front of the 15310-CL
OC-3/OC-12	2	155.52 Mbps (STS-3) 622.08 Mbps (STS-12)	LC	Front of the 15310-CL
CE-100T-8	8	10/100 Mbps	RJ-45	CE-100T-8 card faceplate (expansion slot)
ML-100T-8	8	10/1000 Mbps	RJ-45	ML-100T-8 card faceplate (expansion slot)

CHAPTER 2

Card Reference

This chapter describes the Cisco ONS 15310-CL cards. It includes descriptions, hardware specifications, and block diagrams for each card. For installation and turn-up procedures, refer to the *Cisco ONS 15310-CL Procedure Guide*.

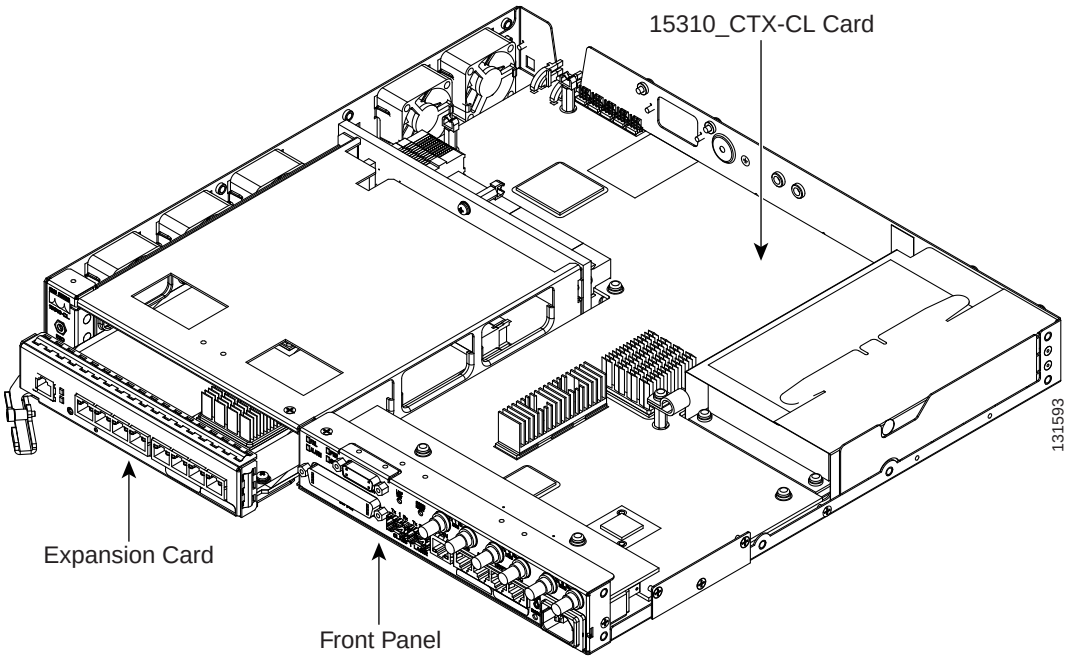
Chapter topics include:

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 15310-CL uses a common control card (the 15310-CL-CTX), an interconnect card, a connector expansion card, and a single expansion card (either the CE-100T-8 or ML100T-8). This overview provides a summary of the 15310-CL-CTX, CE-100T-8, and ML100T-8 cards. Figure 2-1 shows the ONS 15310-CL with an expansion card being inserted.

Figure 2-1 ONS 15310-CL with Expansion Card Being Inserted



2.1.1 Card Summary

Table 2-1 ONS 15310-CL Cards and Descriptions

Card	Description	For Additional Information...
15310-CL-CTX	The 15310-CL-CTX card serves as the common control and central element for ONS 15310-CL switching.	See the "2.2 15310-CL-CTX Card Description" section on page 2-3.
CE-100T-8 Card	The CE-100T-8 card provides eight RJ-45 10/100-Mbps Ethernet ports.	See the "2.3 CE-100T-8 Card" section on page 2-7.
ML100T-8 Card	The ML100T-8 Ethernet card provides eight ports of 10/100 Ethernet-encapsulated traffic into SONET/SDH STS-3/STM-1 payloads.	See the "2.4 ML100T-8 Card" section on page 2-10.
Filler Card	The filler card is used to fill unused traffic card slots in the ONS 15310-CL shelf. The Cisco Transport Controller (CTC) GUI detects the filler card.	See the "2.5 Filler Card" section on page 2-13
SFP Modules	The small form-factor pluggables (SFPs) are integrated fiber-optic transceivers that provide high-speed serial links from a port or slot to the network.	See the "2.6 SFP Modules" section on page 2-13

2.1.2 Card Compatibility

This section lists ONS 15310-CL cards and their compatible software versions. Table 2-2 lists Cisco Transport Controller (CTC) software release compatibility for each card. In the table, "Yes" means that the cards are compatible with the listed software versions. Table cells with dashes mean that the cards are not compatible with the listed software versions.

Table 2-2 ONS 15310-CL Software Release Compatibility Per Card

Card	R5.0	R6.0
15310-CL-CTX	Yes	Yes
CE-100T-8 Card	Yes	Yes
ML100T-8 Card	Yes	Yes
Filler Card	Yes	Yes
SFP Modules	Yes	Yes

2.2 15310-CL-CTX Card Description

This section describes the features and functions of the ONS 15310-CL Common Control, Timing, Cross-Connect Customer-Located (15310-CL-CTX) card.

The 15310-CL-CTX card is an internal, nonremovable card residing in the ONS 15310-CL platform. It operates in a nonredundant configuration and performs system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection/resolution, SONET data communications channel (DCC) termination, system fault detection, and cross-connect maintenance and management for the ONS 15310-CL. The cards also provides the circuitry for the DS-1, DS-3/EC-1, and OC-3/OC-12 interfaces and ensures that the system maintains timing with SMC stability.

The 15310-CL-CTX card connects to an expansion card (CE-100T-8 or ML100T-8) through a mechanical interconnect card within the ONS 15310-CL chassis that is similar to a backplane in appearance. The ONS 15310-CL provides a front chassis opening that accepts either a blank card, a CE-100T-8 plug-in card, or an ML100T-8 plug-in card. When a card is plugged in, it connects to the 15310-CL-CTX card through the interconnect card.

The 15310-CL-CTX has three sets of ports:

- Wideband electrical ports (WBE)
- Broadband electrical ports (BBE)
- Pluggable port module (PPM) ports

Note PPM is a generic term for SFPs. See the "2.6 SFP Modules" section on page 2-13.

There are 21 WBE ports. They are automatically provisioned as DS-1 ports and cannot be deleted or changed. These ports are available at the LFH 96-pin connector on the ONS 15310-CL front panel.

There are three BBE ports. The BBE ports are automatically provisioned as DS-3 ports through the use of network element (NE) defaults. They can also be configured as EC-1 ports. Port creation and deletion is supported for the BBE ports. BBE port provisioning, configuration, creation, and deletion is accomplished through CTC. These ports are located on the ONS 15310-CL front panel.

There are two PPM (SFP) slots. Each slot can contain a one-port PPM. ONS 15310-CL PPMs can be single-rate (OC-3 or OC-12) or multirate (OC-3 and OC-12). Single-rate PPMs are autoprovisioned when they are installed, but multirate PPMs must be provisioned. This behavior can be controlled by NE defaults.

Note To provision, edit, or delete PPM ports, refer to the "Change Port Settings" chapter in the *Cisco ONS 15310-CL Procedure Guide*.

The 15310-CL-CTX card does not have a faceplate because it is located inside the chassis; however, the 15310-CL-CTX LED indicators and connectors are located on the ONS 15310-CL front panel (Figure 2-2).

Figure 2-2 ONS 15310-CL Front Panel

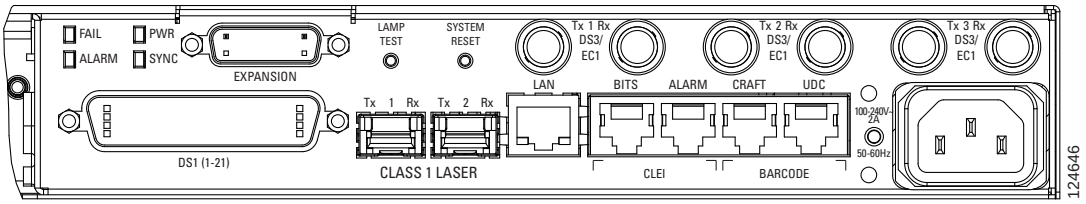
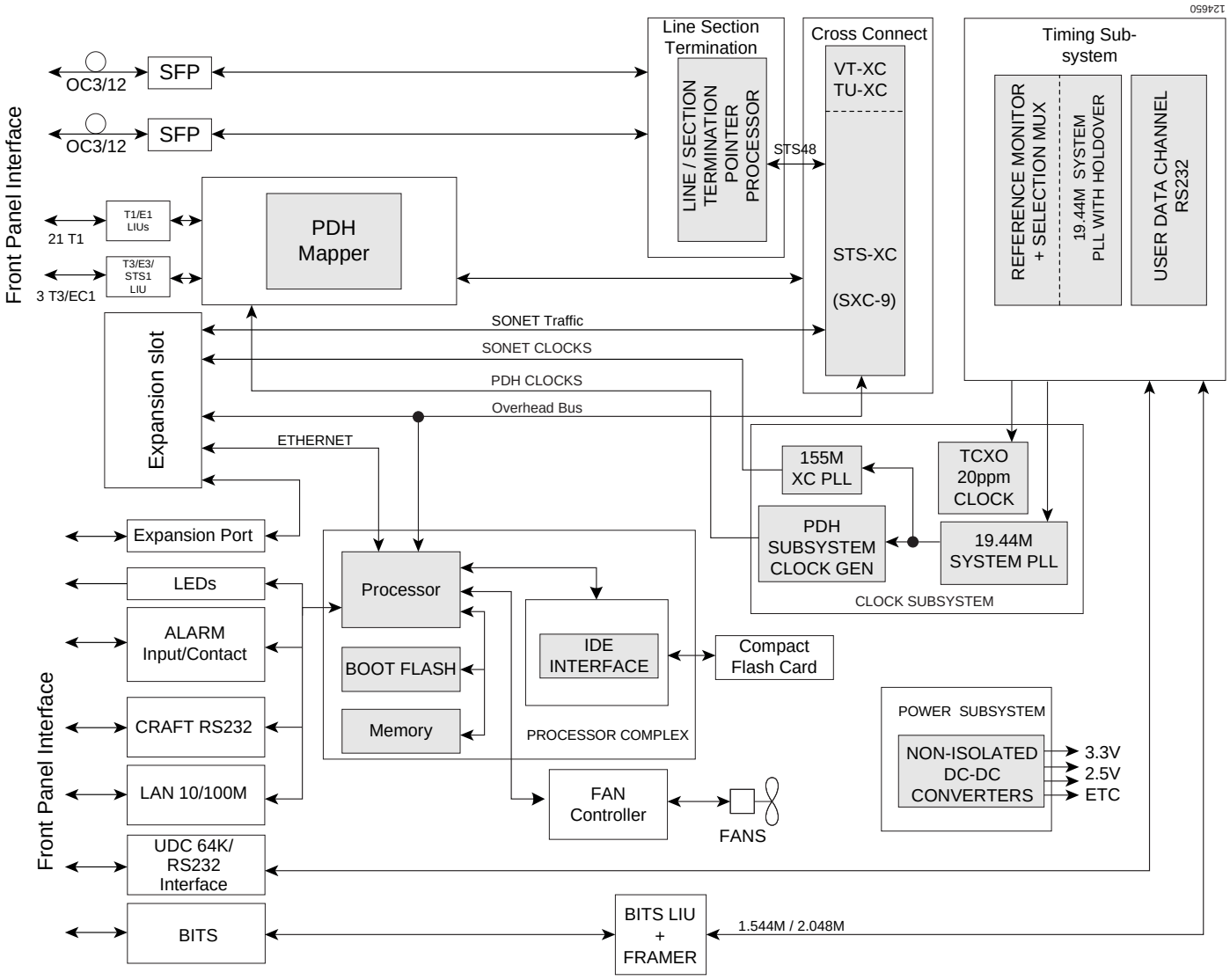


Figure 2-3 shows the 15310-CL-CTX card functional block diagram.

Figure 2-3 15310-CL-CTX Block Diagram



2.2.1 Features

The 15310-CL-CTX card has the following features:

- Support for a maximum of 21 bidirectional DS-1 and three D-3/EC-1 ports
- Support for two SFP/LC optical interfaces for OC-3/OC-12
- 10/100BaseT LAN interface for CTC software
- 57.6-K maximum baud rate EIA/TIA-232 craft interface for Transaction Language One (TL1)
- Configurable alarm inputs and outputs (three input alarms and two alarm output contacts)

- One building integrated timing supply (BITS) input and one BITS output
- User data channel (UDC) connector for synchronous 64-Kbps or asynchronous EIA/TIA-232 communication
- Free-running SMC clock accurate to 20 ppm
- Timing reference to external BITS, optical links, or DS-1/EC-1 ports
- Retime any DS-1/EC-1 port, or use the ports as a timing source
- Nonblocking high-order STS1 cross-connect
- STS-48 worth of low-order cross-connect
- STS-24 worth of low-order VT1.5 cross-connect

2.2.2 Synchronization and Timing

This synchronization and timing subsystem is responsible for monitoring and selecting reference clocks in the node. A free-running SMC clock, accurate to 20 ppm, is available for internal synchronization in the event that no synchronization timing source is available. The 15310-CL-CTX card is normally synchronized from the optical link.

2.2.3 System Cross-Connect

This subsystem is responsible for the setup and maintenance of cross-connections within the system. It supports STS-Nc, STS-1, and VT1.5 cross-connect capability in SONET mode.

2.2.4 Optical Interface

The optical subsystem provides two SFP optical transceivers for two OC-3/OC-12 SONET-compliant interfaces.

2.2.5 Communication and Control

This subsystem is responsible for overall control of the system, such as system initialization, provisioning, alarm reporting, maintenance, diagnostics, intercard communication, DCC termination, and system fault detection.

2.2.6 Electrical Interface (BBE and WBE)

This subsystem supports Telcordia GR-499 compliant, 1.544-Mbps (DS-1) and 44.736-Mbps (DS-3/EC-1) interfaces. Performance monitoring is provided by means of this interface to allow validation of signal quality.

Any outgoing DS-1 signal can be retimed to eliminate accumulated jitter and wander at the point of egress from a synchronous network. Any incoming DS-1 signal from the transport element can also be used as timing source.

2.2.7 15310-CL-CTX Card-Level Indicators

The 15310-CL-CTX card is responsible for operating the LED indicators on the ONS 15310-CL front panel. The panel has four card-level LEDs, described in Table 2-3.

Table 2-3 15310-CL-CTX Card-Level Indicators

Card-Level LEDs	Description
FAIL LED (Red)	The red FAIL LED indicates that the card processor is not ready or that a catastrophic software failure occurred on the 15310-CL-CTX card. As part of the boot sequence, the FAIL LED turns on and flashes until the software deems the card operational.
ALARM LED (Red/Amber)	The ALARM LED is red for Critical and Major alarm conditions. It is amber for Minor alarm conditions.
PWR LED (Green/Amber)	The PWR LED is green if AC power is connected and operating or if both DC power sources are connected and operating. The LED is amber if only one DC power source is connected and operating.
SYNC LED (Green/Amber/Red)	The SYNC LED is green if the 15310-CL-CTX card detects both a primary and secondary clock reference. It is amber if the card detects only a single clock reference. The LED is RED if the card detects no clock reference.

2.3 CE-100T-8 Card

This section describes the features and functions of the ONS 15310-CL 10/100 Ethernet (CE-100T-8) card.

The CE-100T-8 card maps 8-port 10/100-Mbps Ethernet-encapsulated traffic into SONET payloads, making use of low-order (VT1.5) virtual concatenation (VCAT), high-order (STS-1, STS-3c) VCAT, generic framing procedure (GFP), and Point-to-Point Protocol/high-level data link control (PPP/HDLC) framing protocols. It also supports the link capacity adjustment scheme (LCAS), which allows hitless dynamic adjustment of SONET link bandwidth. The CE-100T-8 card provides eight RJ-45 10/100-Mbps Ethernet ports on the faceplate of the card. An inactive RJ-45 console port is also on the faceplate.

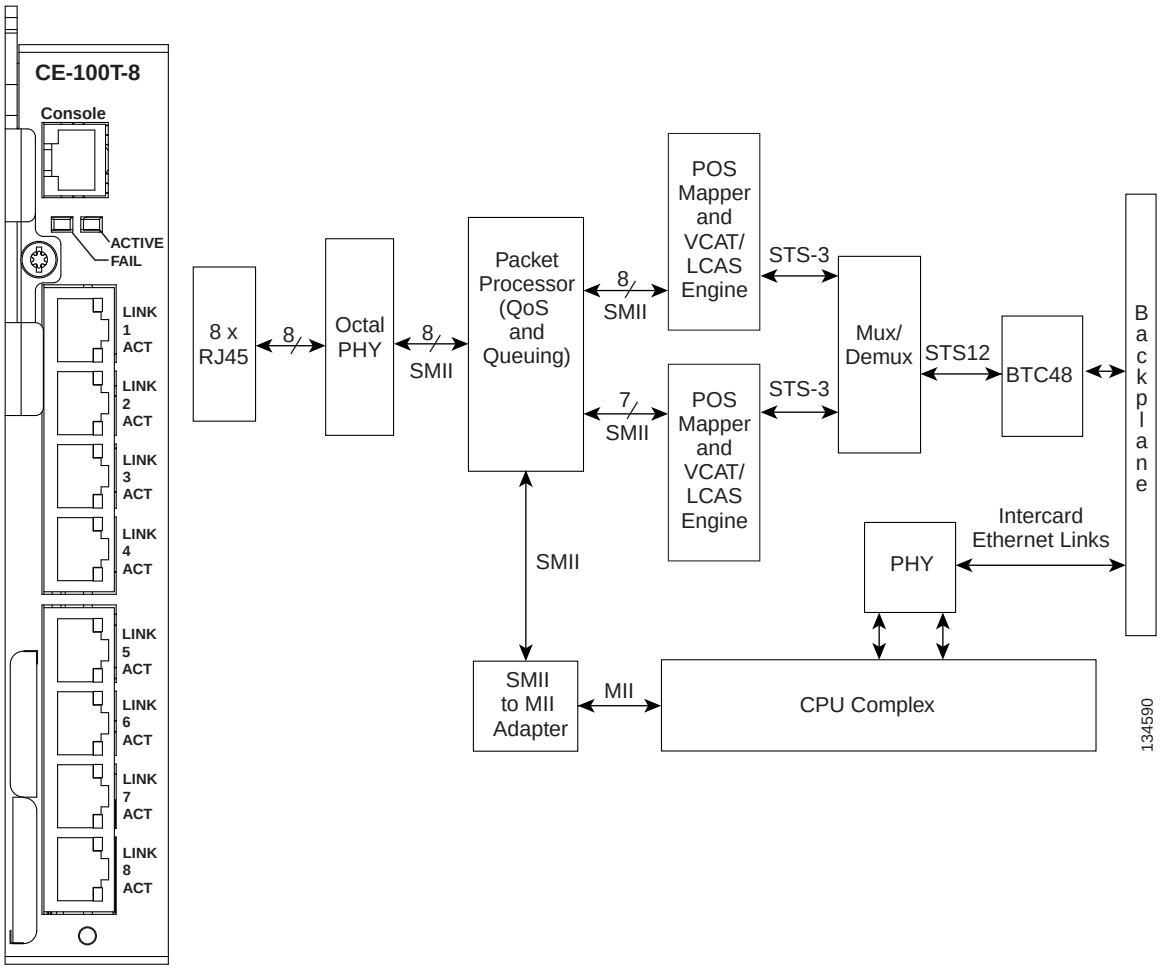
The circuit types supported are:

- STS-1 and STS-3c CCAT
- STS-1-Nv VCAT (N = 1-3)
- STS-1-Nv LCAS (N = 1-3)
- STS-1-2v software LCAS (SW-LCAS) (compatible with ML-Series cards only)
- VT1.5-Nv VCAT (N = 1-64)
- VT1.5-Nv LCAS (N = 1-64)

Each 10/100 Ethernet port can be mapped to a SONET channel in increments of VT1.5 or STS-1 granularity. There are eight backend packet-over-SONET (POS) ports (VCAT groups [VCGs]) available on the ML100T-8 card. Additionally, the CE-100T-8 card supports packet processing, classification, quality of service (QoS)-based queuing, and traffic scheduling.

Figure 2-4 shows the CE-100T-8 card faceplate and block diagram.

Figure 2-4 CE-100T-8 Faceplate and Block Diagram



The following paragraphs describe the general functions of the CE-100T-8 card and relate it to the block diagram.

In the ingress direction (Ethernet-to-SONET), an octal PHY, which performs all of the physical layer interface functions for 10/100-Mbps Ethernet, sends the frame to the Packet Processor for queuing in the respective packet buffer memory. The Packet Processor performs packet processing, packet switching, and classification. The Ethernet frames are then passed over SMII channels to the POS Mappers, where Ethernet traffic is terminated and is encapsulated using the PPP/HDLC or GFP framing protocols. The encapsulation method is selected on a per-port basis. The encapsulated Ethernet frames are then mapped into a configurable number of VCAT low-order and high-order payloads, such as VT1.5 synchronous payload envelope (SPE), STS-1 SPE, or a contiguous concatenated (CCAT) payload such as STS-3c SPE. Up to 64 VT1.5 SPEs or three STS-1 SPEs can be virtually concatenated.

The SPE from each POS Mapper (up to STS-3) carrying encapsulated Ethernet frames are passed onto the multiplexer/demultiplexer (Mux/Demux) next, where the STS-3 frames from both POS Mappers are multiplexed to form an STS-12 frame for transport over the SONET network by means of the Bridging Transmission Convergence (BTC-48) ASIC.

Note Although the STS-3 frames are multiplexed into an STS-12 frame, the frame carries at most an STS-6 payload, leaving half of the STS-12 bandwidth free.

In the egress direction (SONET-to-Ethernet), the Mux/Demux extracts the first and second STS-3 SPEs from the STS-12 frame it receives from the BTC-48 before sending them to the POS Mappers. The STS-3 SONET SPE carrying GFP or PPP/HDLC encapsulated Ethernet frames are then extracted and buffered in the external memory of the POS Mappers. This memory is used for providing alignment and differential delay compensation for the received low/high order virtual concatenated payloads. When alignment and delay compensation are complete, the Ethernet frames are decapsulated with one of the framing protocols (GFP or PPP/HDLC). Decapsulated Ethernet frames are then passed onto the Packet Processor for quality-of-service (QoS) queuing and traffic scheduling. The Network Processor switches the frame to one of the corresponding PHY channels and then onto the Ethernet port for transmission to the external clients.

With regard to QoS, users can use the VLAN class-of-service (CoS) threshold (value 0 to 7, default 7) of incoming Ethernet packets and the IP type-of-service (ToS) threshold (value 0 to 255, default 255) of incoming Ethernet packets for priority queuing. These thresholds are provisionable through CTC, TL1, and Cisco Transport Manager (CTM). CoS takes precedence over ToS unless the CoS threshold is set to the default of 7. This threshold value does not prioritize any packets based on CoS, so ToS is used. The value configured is a threshold and any value greater than that value is set as a priority. For example, if a CoS of 5 is set as the threshold, only CoS values of 6 and 7 would be set to priority.

2.3.1 CE-100T-8 Card-Level Indicators

The CE-100T-8 card faceplate has two card-level LED indicators, described in Table 2-4.

Table 2-4 CE-100T-8 Card-Level Indicators

Card-Level LEDs	Description
SF LED (Red)	The red FAIL LED indicates that the card processor is not ready or that a catastrophic software failure occurred on the CE-100T-8 card. As part of the boot sequence, the FAIL LED blinks until the software deems the card operational, then it turns off.
ACT LED (Green)	The ACT LED provides the operational status of the CE-100T-8. When the ACT LED is green, it indicates that the CE-100T-8 card is active and the software is operational; otherwise, it is off.

2.3.2 CE-100T-8 Port-Level Indicators

The CE-100T-8 card has two LEDs embedded into each of the eight Ethernet-port RJ-45 connectors. The LEDs are described in Table 2-5.

Table 2-5 CE-100T-8 Port-Level Indicators

Port-Level Indicators	Description
ACT LED (Amber)	A steady amber LED indicates a link is detected, but there is an issue inhibiting traffic. A blinking amber LED means traffic is flowing.
LINK LED (Green)	A steady green LED indicates that a link is detected, but there is no traffic. A blinking green LED flashes at a rate proportional to the level of traffic being received and transmitted over the port.
Both ACT and LINK LED OFF	Unlit green and amber LEDs indicate no traffic.

2.4 ML100T-8 Card

This section describes the features and functions of the ONS 15310-CL Multilayer 10/100 Ethernet (ML100T-8) card.

2.4.1 ML100T-8 Card Description

The ML100T-8 card maps eight ports of 10/100 Ethernet encapsulated traffic into SONET STS-3 payloads. The card is compatible with high-order STS-1 VCAT and the GFP and PPP/HDLC framing protocols. It also supports LCAS, which allows hitless dynamic adjustment of SONET/SDH link bandwidth. Each 10/100 Ethernet port can be mapped to a SONET channel in increments of STS-1 granularity.

The ML100T-8 card provides a switched operating mode, with eight subscriber interfaces and two virtual POS (VCG) interfaces mapped through the cross-connect for transport with other services between NEs.

The circuit types supported are:

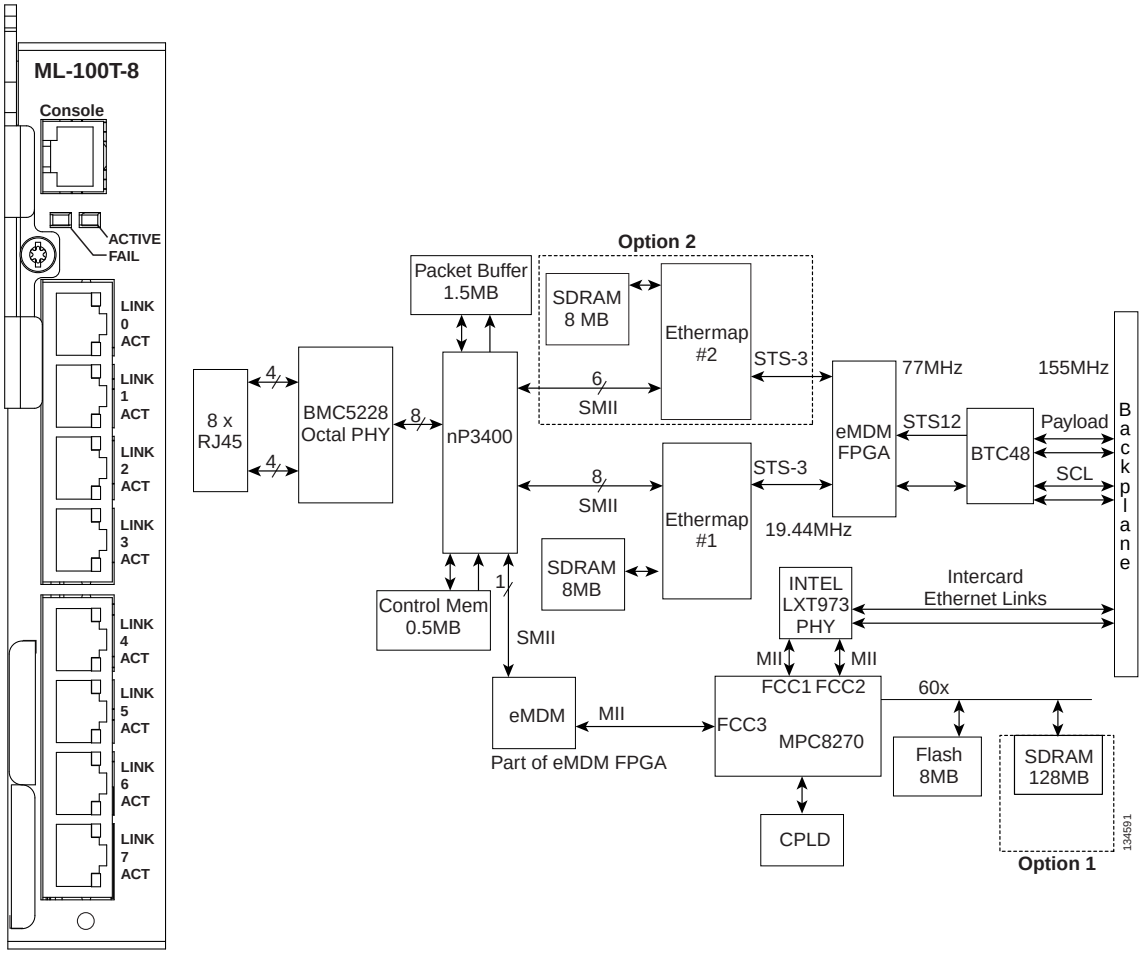
- STS-1
- STS-1-Nv VCAT (N=1–2)
- STS-1-Nv LCAS (N=1–2)
- STS-1-2v SW-LCAS

Additionally, the ML100T-8 card supports packet processing, classification, QoS-based queuing, traffic scheduling, and packet multiplexing services for Layer2/3. The ML100T-8 card facilitates more efficient transport of Ethernet and IP over the SONET/SDH infrastructure with multilayer intelligence.

The ML100T-8 contains an RJ-45 console port that is active by default. It is used to receive keyboard input as well as output error and warning messages.

Figure 2-5 shows the ML100T-8 card faceplate and block diagram.

Figure 2-5 ML100T-8 Card Faceplate and Block Diagram



The following paragraphs describe the general functions of the ML100T-8 card and relate to the block diagram.

In the ingress direction (Ethernet-to-SONET), Ethernet frames first enter from a physical Ethernet port to one of the corresponding channels of the octal PHY, which performs all of the physical layer interface functions for 10/100 Ethernet. The PHY sends the Ethernet frame to the Packet Processor by means of the SMII interfaces for queuing in the respective packet buffer memory. The Packet Processor performs packet processing, packet switching, and classification. The Ethernet frames are then passed on to the POS Mappers through the SMII interfaces. The POS Mappers terminate the 10/100-Mbps Ethernet traffic. The Ethernet frames are extracted and buffered in POS Mapper external memory. Ethernet frames are encapsulated using one of the framing protocols (PPP/HDLC or GFP), selected on a per-port basis. The encapsulated Ethernet frames are mapped into a configurable number of STS-1 or VCAT high-order payloads (STS-1-1v or STS-1-2v). The SPE from each POS Mapper (up to STS-3) carrying encapsulated Ethernet frames are next passed onto the Mux/Demux, where the STS-3 frames from both POS Mappers are multiplexed to form an STS-12 frame for transport over the SONET network by means of the BTC-48 ASIC.

Note Although the STS-3 frames are multiplexed into an STS-12 frame, the frame carries at most an STS-6 payload, leaving half of the STS-12 bandwidth free.

In the egress direction (SONET-to-Ethernet), the Mux/Demux extracts the first and second STS-3 SPEs from the STS-12 frame it receives from the BTC-48 before sending it to the POS Mapper. The STS-3 SONET SPEs carrying GFP or PPP/HDLC encapsulated Ethernet frames are then extracted and buffered in the POS Mapper external memory. This memory is used for providing alignment and differential delay compensation for the received high-order VCAT payloads. After alignment and delay compensation have been done, the Ethernet frames are decapsulated with one of the framing protocols (GFP or PPP/HDLC). Decapsulated Ethernet frames are then passed onto the Network Processor for QoS queuing, traffic scheduling, packet switching, and multiplexing. The Network Processor switches the frame to one of the corresponding PHY channels and then onto the Ethernet port for transmission to the external clients.

2.4.2 ML100T-8 Card-Level Indicators

The ML100T-8 card faceplate has two card-level LED indicators, described in Table 2-6.

Table 2-6 ML100T-8 Card-Level Indicators

Card-Level LEDs	Description
SF LED (Red)	The red FAIL LED indicates that the card processor is not ready or that a catastrophic software failure occurred on the CE-100T-8 card. As part of the boot sequence, the FAIL LED blinks until the software deems the card operational, then it turns off.
ACT LED (Green)	The ACT LED provides the operational status of the ML100T-8. When the ACT LED is green, it indicates that the ML100T-8 card is active and the software is operational; otherwise, it is off.

2.4.3 ML100T-8 Port-Level Indicators

The ML100T-8 card has two LEDs embedded into each of the eight Ethernet port RJ-45 connectors. The LEDs are described in Table 2-7.

Table 2-7 ML100T-8 Port-Level Indicators

Port-Level Indicators	Description
ACT LED (Amber)	A steady amber LED indicates a link is detected, but there is an issue inhibiting traffic. A blinking amber LED means traffic is flowing.
LINK LED (Green)	A steady green LED indicates that a link is detected, but there is no traffic. A blinking green LED flashes at a rate proportional to the level of traffic being received and transmitted over the port.
Both ACT and LINK LED OFF	Unlit LEDs indicate no traffic.

2.5 Filler Card

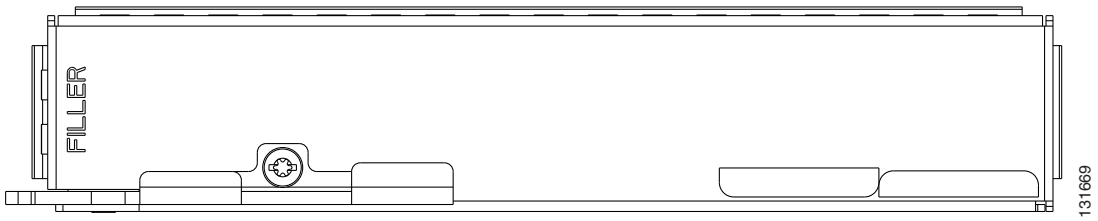
If an expansion card (CE-100T-8 or ML100T-8) is not plugged in, a filler card must be inserted in the expansion slot. The filler card serves three functions: it prevents exposure to hazardous voltages and currents inside the ONS 15310-CL chassis, it eliminates electromagnetic interference (EMI) that might disrupt other equipment, and it directs the flow of cooling air through the chassis.

Caution Do not operate the ONS 15310-CL system unless a card is plugged into the expansion slot.

The blank card is a printed circuit board (PCB) with a blank faceplate and two connectors that, when the card is installed, plug into receptacles at the back of the slot. CTC, the ONS 15310-CL graphical user interface (GUI), detects when a filler car d is plugged in and displays it in node view.

Figure 2-6 shows the filler card faceplate.

Figure 2-6 Filler Card



2.6 SFP Modules

This section describes the SFPs that can be used with the 15310-CL-CTX card. The 15310-CL-CTX card does not have a faceplate because it is located inside the chassis; therefore, the two SFP slots are located on the ONS 15310-CL faceplate, just to the left of the LAN connector (see Figure 2-2 on page 2-4). The CE-100T-8 and ML100T-8 cards do not use SFPs.

2.6.1 Compatibility by Card

Table 2-8 lists the SFPs compatible with the 15310-CL-CTX card.

Caution Only use SFPs certified for use in Cisco Optical Networking Systems (ONSs). The qualified Cisco SFP top assembly numbers (TANs) are provided in Table 2-8.

Table 2-8 SFP Card Compatibility

Card	Compatible SFP (Cisco Product ID)	Cisco Top Assembly Number (TAN)
15310-CL-CTX (ONS 15310-CL SONET)	ONS-SI-155-L1 ONS-SI-155-L2 ONS-SI-155-I1 ONS-SI-622-L1 ONS-SI-622-L2 ONS-SI-622-I1	10-1957-01 10-1937-01 10-1938-01 10-1958-01 10-1936-01 10-1956-01

2.6.2 SFP Description

SFPs are integrated fiber-optic transceivers that provide high-speed serial links from a port or slot to the network. Various latching mechanisms can be utilized on the SFPs. There is no correlation between the type of latch to the model type (such as SX or LX/LH) or technology type (such as Gigabit Ethernet). See the label on the SFP for the technology type and model. One type of latch available is a mylar tab, shown in Figure 2-7. A second type of latch is an actuator/button (Figure 2-8), and a third type is a bail clasp (Figure 2-9).

SFP dimensions are:

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

SFP temperature ranges are:

- COM—Commercial operating temperature range –5 to 70 degrees C (23 to 158 degrees F)
- EXT—Extended operating temperature range –5 to 85 degrees C (23 to 185 degrees F)
- IND—Industrial operating temperature range –40 to 85 degrees C (–40 to 85 degrees F)

Figure 2-7 Mylar Tab SFP

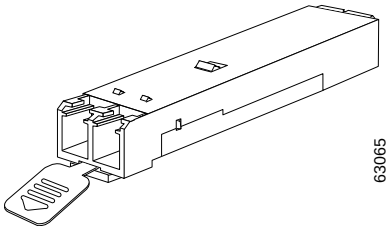


Figure 2-8 Actuator/Button SFP

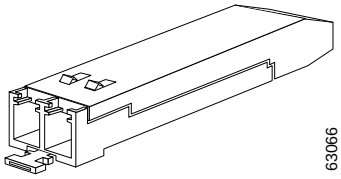
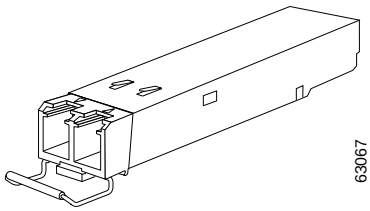


Figure 2-9 Bail Clasp SFP



2.6.3 PPM Provisioning

SFPs are known as pluggable-port modules (PPMs) in the ONS 15310-CL graphical user interface (GUI), CTC. SFPs for the 15310-CL-CTX card can be provisioned for different line rates in CTC. See the "2.2 15310-CL-CTX Card Description" section on page 2-3 for more information. For procedures for provisioning PPMs, refer to the *Cisco ONS 15310-CL Procedure Guide*.

Port Protection

This chapter explains the Cisco ONS 15310-CL port protection configurations. To provision port protection, refer to the *Cisco ONS 15310-CL Procedure Guide*. Chapter topics include:

3.1 Introduction

The Cisco ONS 15310-CL has a single common control card (15310-CTX-CL), so no redundant common control protection is available. The only card protection available is 1+1 optical protection through the two optical ports. The 15310-CL does not provide electrical interface protection (1:1 and 1:N).

The optical ports on the 15310-CTX-CL are provided via small form factor pluggables (SFPs), which are termed PPMs (pluggable port modules) in Cisco Transport Controller (CTC), the ONS 15310-CL software interface.

3.2 Optical Port Protection

When you set up 1+1 optical protection for the ONS 15310-CL, the working optical port on one ONS 152310-CL node is paired with a working optical port on other ONS 15310-CL nodes in a 1+1 protection group. Similarly, the protect optical port on one ONS 152310-CL node is paired with protect optical ports on other ONS 15310-CL nodes in a 1+1 protection group. The data rate and port type of the protect port must match that of the working port. Because the ONS 15310-CL has only two optical ports, they must always be in the same protection group. The rates of the two ports must be the same, either OC-3 or OC-12.

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 port to the protect port, the signal stays switched until it is manually switched back. Revertive 1+1 protection automatically switches the signal back to the working port when the working port comes back online.

To provision 1+1 protection, refer to the “Turn Up Node” chapter in the *Cisco ONS 15310-CL Procedure Guide*.

3.3 Unprotected Ports

An unprotected port is not included in a protection scheme; therefore, a port failure or a signal error results in lost data. Because no bandwidth lies in reserve for protection, unprotected schemes maximize the available ONS 15310-CL bandwidth. Unprotected is the default protection type.

3.4 Automatic Protection Switching

Unidirectional switching allows traffic on the transmit and receive fibers to switch independently.

With nonrevertive 1+1 protection, automatic protection switching (APS) switches a signal after a failure from the working port to the protect port and the signal stays switched to the protect port until it is manually switched back. Revertive switching automatically switches the signal back to the working port when the working port comes back online. 1+1 protection is unidirectional and nonrevertive by default; revertive switching is easily provisioned using CTC.

Traffic over a 1+1 APS link is errorless during a soft reboot or a software upgrade for ONS 15310-CL nodes regardless of whether the 1+1 APS protection is active.

3.5 External Switching Commands

The external switching commands on the ONS 15310-CL are Manual, Force, and Lock out. A Manual switch will switch traffic if the path has an error rate less than the signal degrade. A Force switch will switch traffic even if the path has signal degrade (SD) or signal fail (SF) conditions. A Force switch has a higher priority than a Manual switch. In 1+1 mode, however, if there is an SF condition on the protect line, the SF condition has a higher priority than Force, and Force cannot override the SF condition to make a switch to the protect line. Lockouts can only be applied to a protect port (in 1+1 configurations) and prevent traffic from switching to the protect port under any circumstance. Lockouts have the highest priority. In a 1+1 configuration you can also apply a lock on to the working port. A working port with a lock on applied cannot switch traffic to the protect port in the protection group (pair).

Cisco Transport Controller Operation

This chapter describes Cisco Transport Controller (CTC), the Cisco ONS 15310-CL software interface. For CTC set up and login information, refer to the *Cisco ONS 15310-CL Procedure Guide*.

Chapter topics include:

4.1 CTC Software Delivery Methods

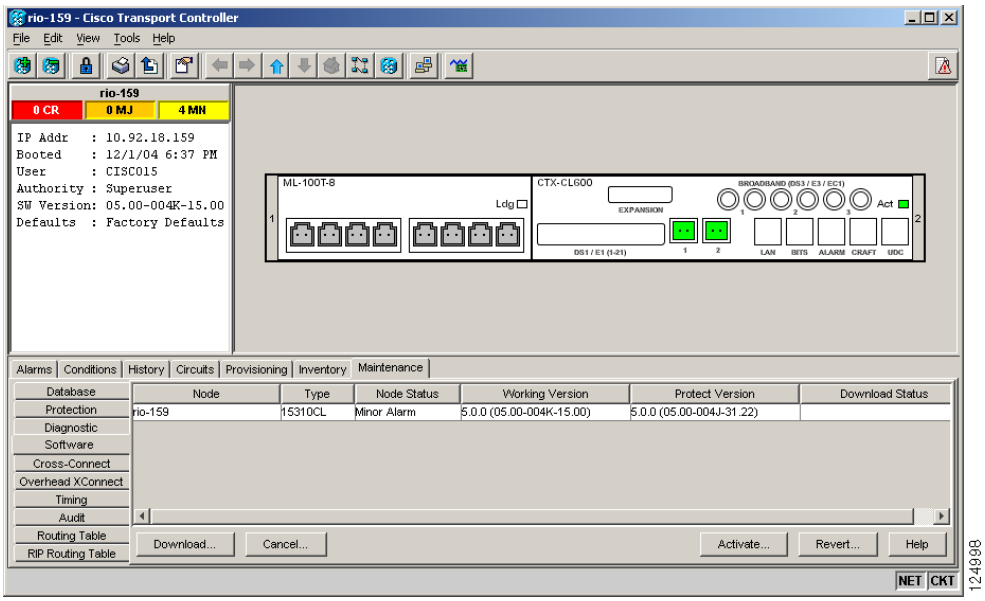
ONS 15310-CL provisioning and administration is performed using CTC software. CTC is a Java application that is installed in two locations; CTC is stored on the 15310-CL-CTX card, and it is downloaded to your workstation the first time you log into the ONS 15310-CL with a new software release.

4.1.1 CTC Software Installed on the 15310-CL-CTX Card

CTC software is preloaded on the 15310-CL-CTX cards; therefore, you do not need to install software.

You can view the software versions that are installed on an ONS 15310-CL by selecting the Maintenance > Software tabs in node view (Figure 4-1). 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



4.1.2 CTC Software Installed on the PC or UNIX Workstation

CTC software Java Archive (JAR) files are installed on your computer using one of the following methods:

- The JAR files are downloaded from the 15310-CL-CTX card and installed on your computer automatically the first time you connect to an ONS 15310-CL. Downloading the CTC software files at login ensures that your computer has the same CTC software version as the ONS 15310-CL you are accessing. The CTC JAR files are stored in the temporary directory designated by your computer operating system.

  You can use the Delete CTC Cache button to remove files. If the files are deleted, they are downloaded the next time you connect to an ONS 15310-CL. Downloading the CTC JAR files may take 1-2 minutes, or 45-50 minutes, depending on the bandwidth of the connection between your workstation and the ONS 15310-CL. JAR files downloaded from a modem or a data communication channel (DCC) network link will require more time than JAR files downloaded over a LAN connection.

- You can install the ONS 15310-CL JAR files on your computer using the CTC setup wizard provided on the CTC software or documentation CDs. Installing the JAR files with the setup wizard eliminates the need to wait for the files to download the first time you log into the ONS 15310-CL. In addition, you can manage ONS 15310-CL nodes that are added to networks with ONS nodes running older software releases. After you install the ONS 15310-CL JAR files, you can log into an ONS 15454 running the earlier software release and manage the ONS 15310-CL nodes. However, if you use the Delete CTC Cache function, you must reinstall the JAR files from the CD.

4.2 CTC Installation Overview

To connect to an ONS 15310-CL using CTC, enter the ONS 15310-CL IP address in the URL field of Netscape Navigator or Microsoft Internet Explorer. After connecting to an ONS 15310-CL, the following events occur automatically:

1. The CTC launcher applet downloads from the 15310-CL-CTX card to your computer.
2. The launcher determines whether your computer has a CTC release matching the release on the 15310-CL-CTX card.
3. If the computer does not have CTC installed, or if the installed release is older than the 15310-CL-CTX card version, the launcher downloads the CTC program files from the 15310-CL-CTX card.
4. The launcher starts CTC. The CTC session is separate from the web browser session, so the web browser is no longer needed.
5. You should always log into nodes having the latest software release unless run the CTC setup wizard and install the ONS 15310-CL Java Archive (JAR) client software files on your computer. If the JAR files are installed on your computer, you can log into ONS 15454s running Release 4.1 or 4.6 to manage ONS 15310-CL nodes that are connected by DCCs to the ONS 15454s.

Each ONS 15310-CL can handle up to five concurrent CTC sessions. CTC performance can vary, depending upon the volume of activity in each session, network bandwidth, and 15310-CL-CTX card load.

Note You can also use TL1 commands to communicate with the Cisco ONS 15310-CL through VT100 terminals and VT100 emulation software, or you can Telnet to an ONS 15310-CL 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 15310-CL, 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 15310-CL software CD and the ONS 15310-CL documentation CD. Table 4-1 lists the requirements for PCs and UNIX workstations. In addition to the JRE, the Java plug-in is included on the ONS 15310-CL software CD and the ONS 15310-CL documentation CD.

Table 4-1 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.

Table 4-1 CTC Computer Requirements (continued)

Area	Requirements	Notes
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 • 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 15310 software and documentation CDs. JRE 1.4.2 provides enhancements to CTC performance, especially for large networks with numerous circuits.
Web browser	• PC: Netscape 7.x, Internet Explorer 6.x • UNIX Workstation: Netscape 7.x	For the PC, use JRE 1.4.2 with any supported web browser. For UNIX, use JRE 1.4.2 with Netscape 7.x. Internet Explorer 6.x is available at the following site: http://www.microsoft.com
Cable	User-supplied Cat-5 straight-through cable with RJ-45 connectors on each end to connect the computer to the ONS 15310-CL directly or though a LAN	—

4.4 ONS 15310-CL Connection

You can connect to the ONS 15310-CL in multiple ways. You can connect your PC directly to the ONS 15310-CL (local craft connection) using the CRAFT port on the front of the ONS 15310-CL, or by connecting your PC to a hub or switch that is connected to the LAN port on the front of the ONS 15310-CL. You can connect to the ONS 15310-CL through a LAN or modem, and you can establish TL1 connections from a PC or TL1 terminal. Table 4-2 lists the ONS 15310-CL connection methods and requirements.

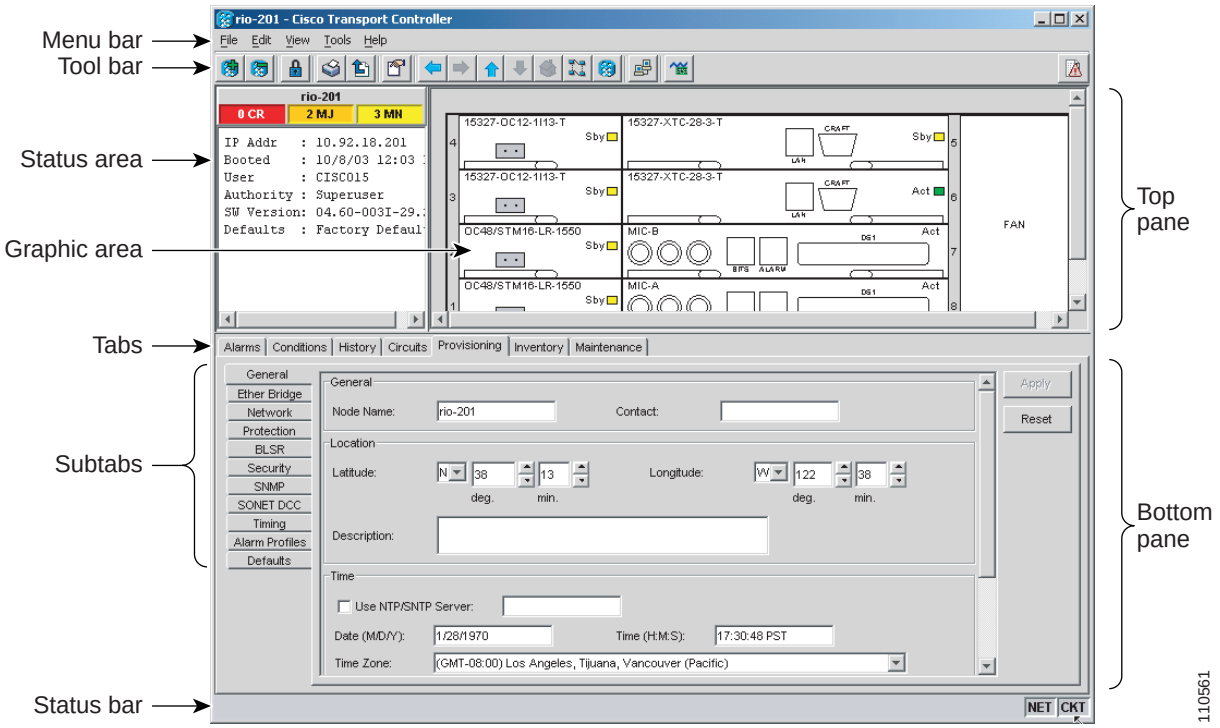
Table 4-2 ONS 15310-CL Connection Methods

Method	Description	Requirements
Local craft	Refers to onsite network connections between the CTC computer and the ONS 15310 using one of the following: • The RJ-45 (LAN) port on the front of the ONS 15310-CL • A hub or switch to which the ONS 15310-CL 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 15310-CL through a corporate or network operations center (NOC) LAN.	• The ONS 15310-CL must be provisioned for LAN connectivity, including IP address, subnet mask, default gateway. • The ONS 15310-CL must be physically connected to the corporate LAN. • The CTC computer must be connected to the corporate LAN that has connectivity to the ONS 15310-CL.
TL1	Refers to a connection to the ONS 15310-CL 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 Reference Guide*.	—
Remote	Refers to a connection made to the ONS 15310-CL using a modem.	• A modem must be connected to the ONS 15310-CL. • The modem must be provisioned for ONS 15310-CL. 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 15310-CL. Figure 4-2 shows an example of the CTC window. The window includes a menu bar, 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 15310-CL information and perform ONS 15310-CL provisioning and maintenance. From this window you can display three ONS 15310-CL views: network, node, and card.

Figure 4-2 Node View (Default Login View) Example



4.5.1 Node View

Node view, shown in Figure 4-2, is the first view that appears after you log into an ONS 15310-CL. 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 15310-CL 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 15310-CL shelf assembly. The colors of the cards in the graphic reflect the real-time status of the physical card and slot (Table 4-3).

Table 4-3 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.

Table 4-3 Node View Card and Slot Colors (continued)

Card and Slot Color	Status
Orange	Slot is provisioned; a Major alarm condition exists.
Red	Slot is provisioned; a Critical alarm exists.

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

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

Port Color	Service State	Description
Cyan (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 (see Figure 4-3 on page 4-8 and Figure 4-4 on page 4-8). 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.
Cyan (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 4-5 lists the card statuses.

Table 4-5 Node View Card Statuses

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

4.5.1.2 Node View Card Shortcuts

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

4.5.1.3 Node View Tabs

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

Table 4-6 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

Table 4-6 Node View Tabs and Subtabs (continued)

Tab	Description	Subtabs
Provisioning	Provisions the ONS 15310-CL node.	General, Network, OSI, Protection, Security, SNMP, Comm Channels, Timing, Alarm Profiles, Defaults
Inventory	Provides inventory information (part number, serial number, Common Language Equipment Identification [CLEI] codes) for cards installed in the node. Allows you to delete and reset cards, and to change card service state. For more information on card service states, see Appendix B, "Administrative and Service States."	—
Maintenance	Performs maintenance tasks for the node.	Database, OSI, Protection, Software, Cross-Connect, Overhead XConnect, Diagnostic, Timing, Audit, RIP Routing Table, Routing Table,

4.5.2 Network View

Network view allows you to view and manage ONS 15310-CL nodes that have DCC connections to the node that you logged into and any login node groups you have selected. Nodes with DCC connections to the login node will not display if you selected Disable Network Discovery on the Login dialog box.

The graphic area displays a background image with colored ONS 15310-CL icons. A Superuser can set up the logical network view feature, which enables each user to see the same network view. The icon colors indicate the node status (Table 4-7).

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).

There are four possible combinations for the appearance of DCCs: green/solid, green/dashed, gray/solid, and gray/dashed. DCC appearance corresponds to the following states: active/routable, active/nonroutable, failed/routable, or failed/nonroutable. Circuit provisioning uses active/routable links. Selecting a node or span in the graphic area displays information about the node and span in the status area.

The color of a node in network view indicates the node alarm status. Table 4-7 lists the node colors shown in network view.

Table 4-7 Node Colors Indicating Status 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 4-8 lists the tabs and subtabs available in the network view.

Table 4-8 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, 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 15310-CL 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 either the card status (active or standby), card service state if the card is present, or port service state (Table 4-4 on page 4-7). The information that appears and the actions you can perform depend on the card.

Figure 4-5 CTC Card View Showing an ML100T-8 Card

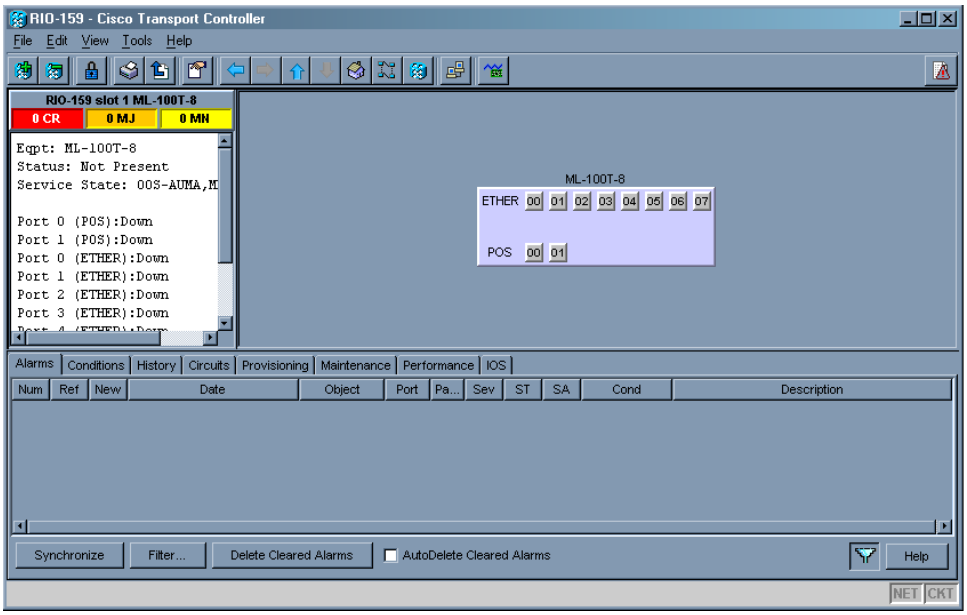


Table 4-9 shows the tabs and subtabs available in card view. The subtabs, fields, and information shown under each tab depend on the card type selected.

Table 4-9 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 completes rolls.	Circuits, Rolls

Table 4-9 Card View Tabs and Subtabs (continued)

Tab	Description	Subtabs
Provisioning	Provisions an ONS 15310-CL-CTX card.	15310-CL-CTX cards: Wideband Ports, Broadband Ports, Pluggable Port Modules, DS1 (subtabs include Line, Line Thresholds, Elect Path Thresholds, and SONET Thresholds); DS3 (subtabs include Line, Line Thresholds, Elect Path Thresholds, and SONET Thresholds); EC1 (subtabs include Line, SONET Thresholds, and SONET STS); Optical (subtabs include Line, SONET Thresholds, and SONET STS); External Alarms; External Controls, and Alarm Profiles. OC-N ports: Line, SONET Thresholds, SONET STS, and Alarm Profiles Ethernet cards (subtabs depend on the card type): Ether Ports, POS Ports, Ether VLAN, Ether Card, Ether Thresholds, Alarm Profiles
Maintenance	Performs maintenance tasks for the card.	15310-CL-CTX card: DS1 (subtabs include Loopback, Protection, Path Trace AINS Soak); DS3 (subtabs include Loopback, Protection, Path Trace AINS Soak); EC1(subtabs include Loopback, Protection, Path Trace AINS Soak); Optical (subtabs include Loopback, ALS, Protection, Path Trace AINS Soak); External Alarms; External Controls; and Virtual Wires OC-N ports: Loopback, Info, Protection, AINS Soak, Path Trace (options depend on the card type) Ethernet cards: Path Trace, Loopback, Bandwidth
Performance	Performs performance monitoring for the card.	15310-CL-CTX card: DS1, DS3, EC1, Optical Ethernet cards (subtabs depend on the card type): Ether Ports, POS Ports

4.5.4 Print and Export CTC Data

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

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

- Entire frame—Prints or exports the entire CTC window including the graphical view of the card, node, or network. This option is available for all windows.
- Tabbed view—Prints or exports the lower half of the CTC window containing tabs and data. The printout includes the selected tab (on top) and the data shown in the tab window. For example, if you print the History window tabbed view, you print only history items appearing in the window. This option is available for all windows.

- Table Contents—Prints CTC data in table format without graphical representations of shelves, cards, or tabs. This option does not apply to all windows; refer to the print task in the *Cisco ONS 15310-CL Procedure Guide* for specifics.
- 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.

4.6 15310-CL-CTX Card Reset

You can reset the ONS 15310-CL card by using the hard-reset or soft-reset commands in CTC. A soft reset reboots the 15310-CL-CTX card and reloads the operating system and the application software. A hard reset temporarily removes power from the 15310-CL-CTX card and clears all buffer memory. Before you hard-reset a card, the card must be put in standby mode by completing a soft-reset.

From the node view, select a card and right-click to open a menu with the hard-reset and soft-reset commands. Soft resets do not impact traffic, however hard resets are service affecting. A card must be in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state before you can perform a hard reset.

4.7 CE-100T-8 and ML100T-8 Card Reset

You can reset the CE-100T-8 and ML100T-8 cards by using the hard-reset or soft-reset commands in CTC. A soft reset reboots the card and reloads the operating system and the application software. A hard reset temporarily removes power from the card and clears all buffer memory.

From the node view, select a card and right-click to open a menu with the hard-reset and soft-reset commands. A card must be in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state before you can perform a hard reset.

4.8 15310-CL-CTX Card Database

You can store a back-up version of the database on the workstation running CTC. This operation should be part of a regular ONS 15310-CL maintenance program performed at approximately weekly intervals, and should also be completed when preparing an ONS 15310-CL for a pending natural disaster, such as a flood.

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 15310-CL-CTX copies the current working database and saves it in a reserved location in the 15310-CL-CTX 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) do not reinstate 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 6.0.1 to 6.0.0), because maintenance releases use the same database.

Security

This chapter provides information about Cisco ONS 15310-CL user security. To provision security, refer to the *Cisco ONS 15310-CL Procedure Guide*.

Chapter topics include:

5.1 Users IDs and Security Levels

The CISCO15 user ID is provided with the ONS 15310-CL for initial login, but Cisco Transport Controller (CTC) does not display this user ID when you log in. Use this ID to set up other ONS 15310-CL user IDs. (For instructions, see the "Turn Up Node" chapter in the *Cisco ONS 15310-CL Procedure Guide*.)

An ONS 15310-CL node can support up to 500 user IDs. Each CTC or Transaction Language 1 (TL1) user ID 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 15310-CL maintenance options.
- Provisioning—Users can access provisioning and maintenance options.
- Superuser—Users can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users.

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 ID and prevent concurrent logins for all users.

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

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 15310-CL 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	—	Create/Edit/Delete	—	—	X	X
		Filter/Search	X	X	X	X

Table 5-1 ONS 15310-CL Security Levels—Node View (continued)

CTC Tab	Subtab	[Subtab]: Actions	Retrieve	Maintenance	Provisioning	Superuser
Provisioning	General	Edit	—	—	Partial[1]	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	X
		TARP: Config	—	—	X	X
		TARP: Static TDC	—	—	X	X
		TARP: MAT	—	—	X	X
		Routers: Setup	—	—	X	X
		Routers: Subnets	—	—	X	X
		Tunnels	—	—	X	X
	Protection	Create/Delete/Edit	—	—	X	X
		View	X	X	X	X
	Security	Users: Create/Delete/Clear Security Intrusion	—	—	—	X
		Users: Change	Same user	Same user	Same user	All users
		Active Logins: Logout	—	—	—	X
		RADIUS Server	—	—	—	X
		Policy/Access/Legal Disclaimer: Edit	—	—	—	X
	SNMP	Trap Destinations/Selected Destination: Create/Delete/Edit	—	—	X	X
		View	X	X	X	X
	Comm Channels	SDCC/LDCC/PPC: Create/Edit/Delete	—	—	X	X
	Timing	General/BITS Facilities: Edit	—	—	X	X
	Alarm Profiles	Alarm Behavior: Edit	—	—	X	X
		Alarm Profiles Editor: Store/Delete[2]	—	—	X	X
		Alarm Profiles Editor: New/Load/Compare/Available/ Usage	X	X	X	X
	Defaults	Edit/Import	—	—	—	X
		Export	X	X	X	X

Table 5-1 ONS 15310-CL Security Levels—Node View (continued)

CTC Tab	Subtab	[Subtab]: Actions	Retrieve	Maintenance	Provisioning	Superuser
Inventory	—	Delete	—	—	X	X
		Hard Reset/Soft Reset	—	X	X	X
Maintenance	Database	Backup	—	X	X	X
		Restore	—	—	—	X
	OSI	IS-IS RIB	—	—	—	X
		ES-IS RIB	—	—	—	X
		TDC	—	—	—	X
	Software	Download/Cancel	—	X	X	X
		Activate/Revert	—	—	—	X
	Cross-Connect	Resource Usage: Delete	—	—	X	X
		Resource Usage: Refresh	X	X	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
	RIP Routing Table	Retrieve	X	X	X	X
	Routing Table	Retrieve	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 15310-CL 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
History	—	Filter	X	X	X	X
Circuits	—	Create/Edit/Delete	—	—	X	X
		Filter/Search	X	X	X	X

Table 5-2 ONS 15310-CL Security Levels—Network View (continued)

CTC Tab	Subtab	[Subtab]: Actions	Retrieve	Maintenance	Provisioning	Superuser
Provisioning	Security	Users: Create/Delete/Clear Security Intrusion Alarm	—	—	—	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	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/Edit/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 the Superuser security privilege can provision security policies on the ONS 15310-CL. These security policies include idle user timeouts, password changes, password aging, and user lockout parameters. In addition, a Superuser can access the ONS 15310-CL through the LAN port on the front of the node.

5.2.2.1 Idle User Timeout

Each ONS 15310-CL 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. 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 “Change Node Settings” chapter in the *Cisco ONS 15310-CL Procedure Guide* for instructions.

Table 5-3 ONS 15310-CL Default User Idle Times

Security Level	Idle Time
Superuser	15 minutes
Provisioning	30 minutes
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 in via CTC or TL1 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 their passwords and how frequently passwords can be reused.
- Login attempts and locking out users—Superusers can specify the maximum number of times that a user can unsuccessfully attempt to log in before being locked out of CTC. Superusers can also provision the length of time before the lockout is removed.
- Disabling users— Superusers can provision the length of time before inactive user IDs 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 15310-CL using the 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 channels that are not secure. Port 22 is the default port and cannot be changed.

5.3 Audit Trail

The ONS 15310-CL maintains a Telcordia GR-839-CORE-compliant audit trail log that resides on the 15310-CL-CTX card. 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 audit trail log shows who has accessed the node and what operations were performed during a given period of time. The log includes authorized Cisco support logins and logouts using the operating system command line interface (CLI), CTC, and TL1; the log also includes FTP actions, circuit creation/deletion, and user/system generated actions.

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

To view the audit trail log, refer to the *Cisco ONS 15310-CL 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, or upgrades.

Note 15310-CL does not support a real time clock with battery backup. Hence, when you reset 15310-CL-CTX card, the audit log is reset to 1970 until you set the date and time again.

5.3.1 Audit Trail Log Entries

Audit trail records capture various types of activities. Individual audit entries contain a varying subset of the activities in the following list:

- 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—The service used to connect to the node (for example, telnet, console, or SNMP)
- Category—Type of change: Hardware, Software, Configuration
- Status—Status of the user action: Read, Initial, Successful, Timeout, Failed
- Time—Time of change
- Message Type—Denotes if the event is Success/Failure type
- Message Details—A description of the change

5.3.2 Audit Trail Capacities

The ONS 15310-CL 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.

When the log server reaches the 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 you off-load the file, this event will not occur a second time regardless of the amount of entries that are overwritten by incoming data. To export the audit trail log, refer to the *Cisco ONS 15310-CL 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 a customer site, while the clients reside in the dial-up access servers and can be distributed throughout the network.

An ONS 15310 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 RADIUS client and 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 monitoring an unsecured network could determine a user's password. Refer to the *Cisco ONS 15310-CL Procedure Guide* to implement 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 from 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 5-4.

Table 5-4 Shared Secret Character Groups

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

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

Timing

This chapter provides information about Cisco ONS 15310-CL SONET timing. To provision timing, refer to the *Cisco ONS 15310-CL Procedure Guide*.

Chapter topics include:

6.1 Timing Parameters

Node Timing parameters must be set for each ONS 15310-CL. Each ONS 15310-CL independently accepts its timing reference from one of three sources:

- The building integrated timing supply (BITS) port on the ONS 15310-CL.
- An OC-N port on the ONS 15310-CL. The port is connected to a node that receives timing through a BITS source.
- The internal ST3 clock on the CTX card.

You can set ONS 15310-CL timing to one of three modes: external, line, or mixed. If timing is coming from the BITS port, set ONS 15310-CL timing to external. If the timing comes from an OC-N and DS1 port, set the timing to line. Typical ONS 15310-CL 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 CTX 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 DS1 port and OC-N trunk (span) port.

You can set three timing references for each ONS 15310-CL. 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 15310-CL CTX 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 15310-CL node becomes isolated, timing is maintained at the ST3 level.

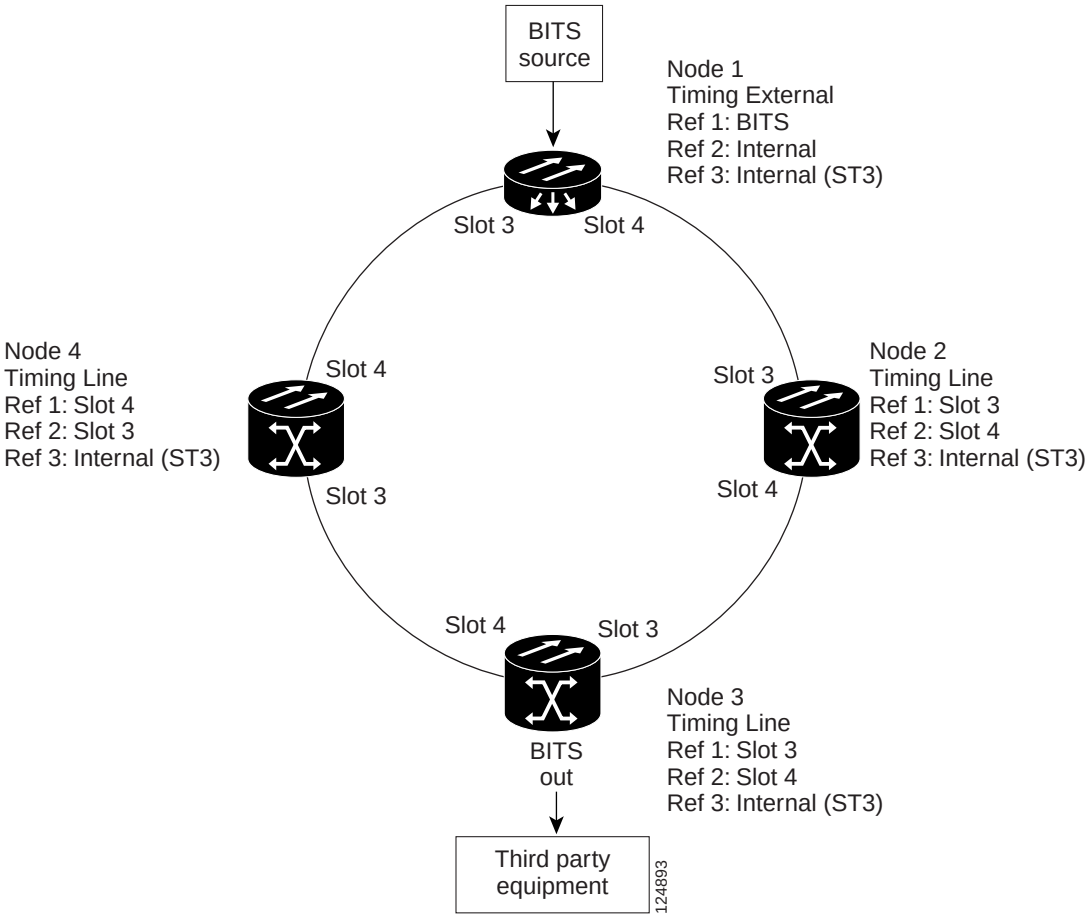
The CTC Maintenance > Timing > Report tabs show current timing information for an ONS 15310-CL, including the timing mode, clock state and status, switch type, and reference data.

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 15310-CL network timing setup. Node 1 is set to external timing. One reference is set to BITS, the two references are set to internal. The BITS output pins on the CTX cards of Node 3 provide timing to outside equipment, such as a digital access line multiplexer.

Figure 6-1 ONS 15310-CL 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 15310-CL, 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

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

This chapter explains Cisco ONS 15310-CL 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 15310-CL Procedure Guide*.

Chapter topics include:

7.1 Overview

You can create circuits across and within ONS 15310-CL nodes and assign different attributes to circuits. For example, you can:

- Create one-way, two-way (bidirectional), or broadcast circuits.
- Assign user-defined names to circuits.
- Assign different circuit sizes.

- Automatically or manually route circuits.
- Automatically create multiple circuits with autoranging. VT tunnels do not use autoranging.
- Provide full protection to the circuit path.
- Provide only protected sources and destinations for circuits.
- Define a secondary circuit source or destination that allows you to interoperate an ONS 15310-CL path protection with third-party equipment path protection configurations.
- Set path protection circuits as revertive or nonrevertive.

For the CE-100T-8 or ML-100T-8 card, you can provision circuits either before or after the cards are installed if the slots are provisioned. For the 15310-CL-CTX card, you must preprovision the small form-factor pluggables (SFPs) (called pluggable port modules [PPMs] in CTC) before you can create an optical circuit. However, circuits do not carry traffic until the cards and SFPs are installed and the ports are In-Service and Normal (IS-NR); Out-of-Service and Autonomous, Automatic In-Service (OO-AU,AINS); or Out-of-Service and Management, Maintenance (OOS-MA,MT).

7.2 Circuit Properties

You can view information about circuits in the ONS 15310-CL Circuits window, which appears in network, node, and card view. 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), VAP (VT aggregation point), STS-V (STS virtual concatenated [VCAT] circuit), or VT-V (VT VCAT circuit).
- Size—The circuit size. VT circuits are 1.5. ONS 15310-CL STS circuits are 1, 3c, 6c, 9c, or 12c. VCAT circuits are VT1.5-*n*v or STS-1-*n*v, where *n* is the number of members.
- Protection—The type of circuit protection.
- Direction—The circuit direction, either two-way or one-way.
- Status—The circuit status. See the "7.2.1 Circuit Status" section on page 7-3.
- Source—The circuit source in the format: *node/slot/port "port name"/STS/VT*. (Port name appears in quotes.) Node and slot always appear; *port "port name"/STS/VT* might appear, depending on the source card, circuit type, and whether a name is assigned to the port. If the port is anything other than an optical port, the port format is *port type-port number*, for example, pEC1-1. If the port is a DS-1 port, port number is not shown, for example, pDS1. If the circuit size is a concatenated size (3c, 6c, 9c, 12c), STSs used in the circuit are indicated by an ellipsis, for example, S7..9, (STSs 7, 8, and 9) or S10..12 (STSs 10, 11, and 12).
- Destination—The circuit destination in the same format as the circuit source.
- # of Spans—The number of internode links that constitute the circuit. Right-clicking the column displays a shortcut menu from which you can choose to show or hide circuit span detail.
- State—The circuit state. See the "7.2.2 Circuit States" section on page 7-4.

7.2.1 Circuit Status

The circuit statuses that appear in the Circuit window Status column are generated by Cisco Transport Controller (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 15310-CL Circuit Status

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

7.2.2 Circuit States

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

- If all cross-connects in a circuit are in the IS-NR service state, the circuit service state is In-Service (IS).
- If all cross-connects in a circuit are in an Out-of-Service (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 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 15310-CL Troubleshooting Guide* for troubleshooting procedures.

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

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

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.

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 15310-CL 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 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 Appendix B, "Administrative and Service States."

7.2.3 Circuit Protection Types

The Protection column on 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.
N/A	A circuit with connections on the same node is not protected.
Protected	The circuit is protected by diverse SONET topologies, for example, a path protection and 1+1.
Unknown	A circuit has a source and destination on different nodes and communication is down between the nodes. This protection type appears if not all circuit components are known.
Unprot (black)	A circuit with a source and destination on different nodes is not protected.
Unprot (red)	A circuit created as a fully protected circuit is no longer protected due to a system change, such as removal of a 1+1 protection group.
Path Protection	The circuit is protected by a path protection.

7.2.4 Edit Circuits Window

Use the Edit Circuits window to view general circuit information, create monitor circuits, and change a circuit state. For path protection circuits, use the Edit Circuits window to change path protection selectors and switch protection paths. Selectors appear as pentagons on the detailed circuit map.

From the UPSR Selectors subtab in 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 (HOT) for path protection selector switching.
- Edit the Signal Fail (SF)/Signal Degrade (SD) bit error rate (BER) thresholds.
- Change path payload defect indication (PDI-P) settings.

Note On 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.

From the Edit Circuits window, you can display a detailed circuit map by checking Show Detailed Map. The detailed map allows you to view information about ONS 15310-CL circuits. Routing information that appears includes:

- Circuit direction (unidirectional/bidirectional)
- The nodes, STSs, and VTs through which the 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, 1+1) and bandwidth (OC-N)

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.

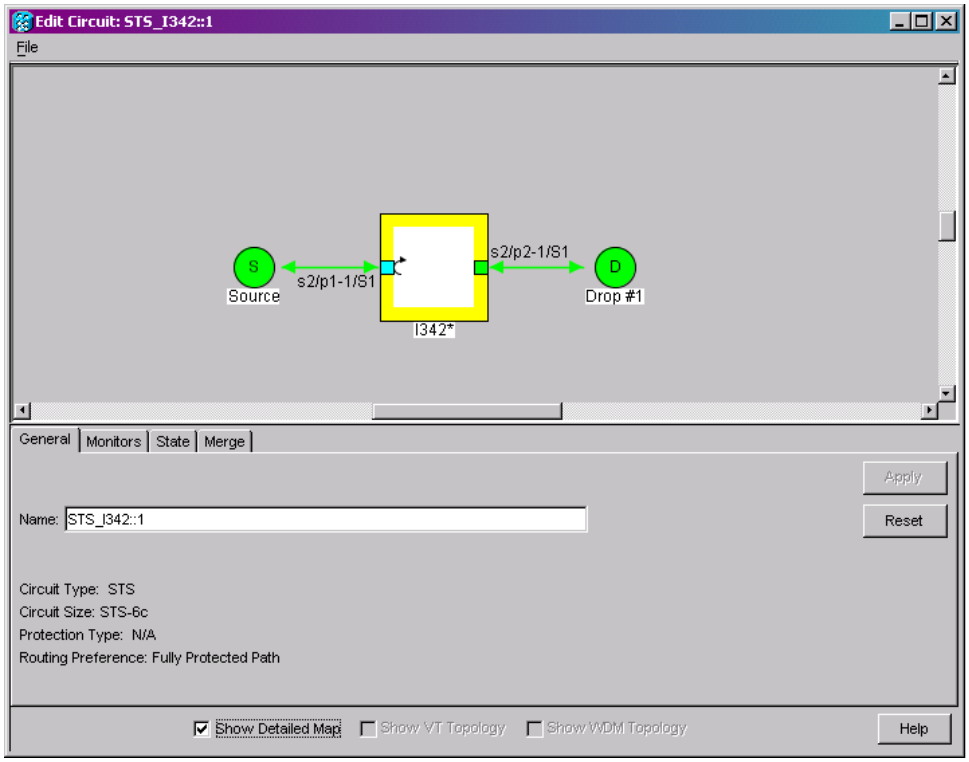
Table 7-3 Port State Color Indicators

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

Notations within or next to the squares or selector pentagons on each node indicate switches and other conditions. For example:

- F = Force switch
- M = Manual switch
- L = Lockout switch
- Arrow = Facility (outward) or terminal (inward) loopback (Figure 7-1)

Figure 7-1 Terminal Loopback in the Edit Circuits Window



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.

7.3 VT1.5 Bandwidth

The 15310-CL-CTX card performs port-to-port time-division multiplexing (TDM). Because VT1.5 multiplexing is STS-based, understanding how VT1.5 circuits use the 15310-CL-CTX VT matrix resources is necessary to avoid unexpected depletion of 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.
- 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 15310-CL-CTX card can map up to 24 STSs for VT1.5 traffic. Because one STS can carry 28 VT1.5s, the 15310-CL-CTX 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 15310-CL-CTX card VT1.5 cross-connect capacity is reached after you create 12 VT1.5 circuits.

7.4 VT Tunnels and Aggregation Points

To maximize 15310-CL-CTX VT1.5 cross-connect resources, you can tunnel VT1.5 circuits through ONS 15310-CL nodes. VT1.5 tunnels do not use VT matrix capacity at ONS 15310-CL pass-through nodes, thereby freeing the 15310-CL-CTX card cross-connect resources for other VT1.5 circuits.

VT aggregation points (VAPs) allow you to provision 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 an OC-N. 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 15310-CL card or port.

7.5 DCC Tunnels

Each SONET frame 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 15310-CL uses the Section DCC (SDCC) or Line DCC (LDCC) for ONS 15310-CL management and provisioning. When multiple DCC channels exist between two neighboring nodes, the ONS 15310-CL 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 tunnel third-party SONET equipment across ONS 15310-CL networks using one of two tunneling methods, a traditional DCC tunnel or an IP-encapsulated tunnel.

7.5.1 Traditional DCC Tunnels

In traditional DCC tunnels, you can use the three available channels of the LDCC and/or the single channel of the SDCC, when not used for ONS 15310-CL DCC terminations, to tunnel third-party SONET equipment across ONS networks. A DCC tunnel endpoint is defined by slot, port, and DCC channel. You can connect any of the four available channels to any other available channel. To create a DCC tunnel, you connect the tunnel endpoints from one ONS 15310-CL 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
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:

- An optical port used for a DCC termination cannot be used as a DCC tunnel endpoint, and an optical port that is used as a DCC tunnel endpoint cannot be used as a DCC termination.
- All DCC tunnel connections are bidirectional.

7.5.2 IP-Encapsulated Tunnels

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

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

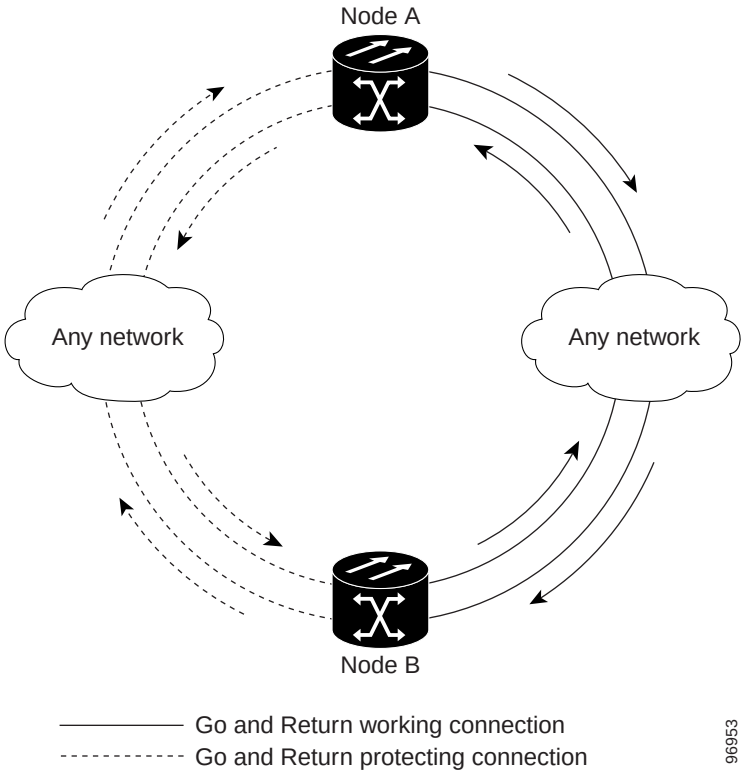
Each ONS 15310-CL supports one IP-encapsulated tunnel. You can convert a traditional DCC tunnel to an IP-encapsulated tunnel or an IP-encapsulated tunnel to a traditional DCC tunnel. Only tunnels in the Discovered status can be converted.

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

7.6 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 7-2). The working path will always be the shortest path. If a fault occurs, neither the working and protection fibers are affected. This feature only applies to bidirectional path protection circuits. The go-and-return option appears on the Circuit Attributes page of the Circuit Creation wizard.

Figure 7-2 Path Protection Go-and-Return Routing



7.7 Virtual Concatenated Circuits

Virtual concatenated (VCAT) circuits, also called VCAT groups (VCGs), transport traffic using noncontiguous TDM time slots, avoiding the bandwidth fragmentation problem that exists with contiguous concatenated (CCAT) circuits. The ONS 15310-CL cards that support VCAT circuits are the CE-100T-8 and ML-100T-8 cards.

In a VCAT circuit, circuit bandwidth is divided into smaller circuits called VCAT members. The individual members act as independent TDM circuits. All VCAT members should be the same size and must originate/terminate at the same end points.

7.7.1 VCAT Circuit States

The state of a VCAT circuit is an aggregate of its member circuits. You can view whether a VCAT member is In Group or Out of Group in the VCAT State column in the Edit Circuits window.

- If all member circuits are IS, the VCAT circuit is IS.
- If all In Group member circuits are OOS, the VCAT circuit state is OOS.
- If no member circuits exist or if all are Out of Group, the state of a VCAT circuit is OOS.
- A VCAT circuit is OOS-PARTIAL when In Group member states are mixed and not all IS.

7.7.2 VCAT Member Routing

The automatic and manual routing selection applies to the entire VCAT circuit, that is, all members are manually or automatically routed. Bidirectional VCAT circuits are symmetric, which means that the same number of members travel in each direction. With automatic routing, you can specify the constraints for individual members; with manual routing, you can select different spans for different members.

Two types of automatic and manual routing are available for VCAT members on CE-100T-8 and ML-100T-8 cards: common fiber routing and split fiber routing. In common fiber routing, all VCAT members travel on the same fibers, which eliminates delay between members. Three protection options are available for common fiber routing: Fully Protected, PCA, and Unprotected. Split fiber routing allows the individual members to be routed on different fibers or each member to have different routing constraints. This mode offers the greatest bandwidth efficiency and also the possibility of differential delay, which is handled by the buffers on the terminating cards or ports. Three protection options are available for split fiber routing: Fully Protected, Unprotected, and DRI. In both common fiber and split fiber routing, each member can use a different protection scheme; however, for common fiber routing, CTC checks the combination to make sure that a valid route exists. If it does not, the user must modify the protection type.

In both common fiber and split fiber routing, intermediate nodes treat the VCAT members as normal circuits that are independently routed and protected by the SONET network. At the terminating nodes, these member circuits are multiplexed into a contiguous stream of data. Figure 7-3 shows an example of common fiber routing.

Figure 7-3 VCAT Common Fiber Routing

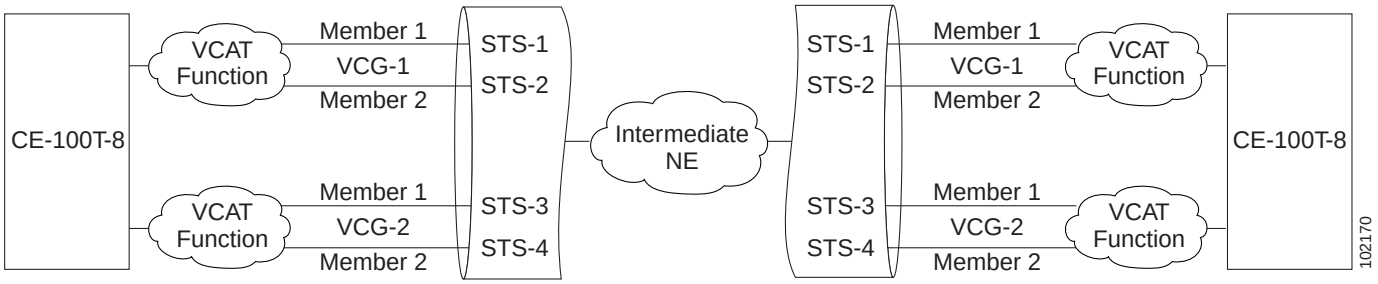
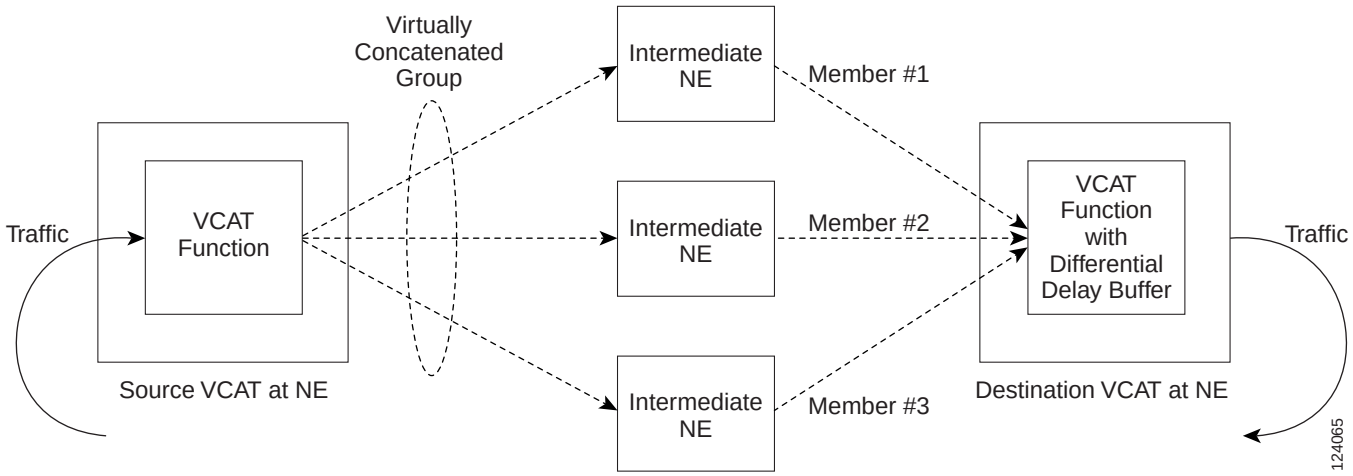


Figure 7-4 shows an example of split fiber routing.

Figure 7-4 VCAT Split Fiber Routing



7.7.3 Link Capacity Adjustment

The CE-100T-8 and ML-100T-8 cards support Link Capacity Adjustment Scheme (LCAS), which is a signaling protocol that allows dynamic bandwidth adjustment of VCAT circuits. When a member fails, LCAS temporarily removes the failed member from the VCAT circuit for the duration of the failure, leaving the remaining members to carry the traffic. When the failure clears, the member circuit is automatically added back into the VCAT circuit. You can select LCAS during VCAT circuit creation.

Note Although LCAS operations are errorless, a SONET error can affect one or more VCAT members. If this occurs, the VCAT Group Degraded (VCG-DEG) alarm is raised. For information about clearing this alarm, refer to the *Cisco ONS 15310-CL Troubleshooting Guide*.

SW-LCAS is a limited form of LCAS that allows the VCAT circuit to adapt to member failures and keep traffic flowing at a reduced bandwidth. SW-LCAS is necessary when interoperating with the ONS 15454 ML-Series cards. SW-LCAS uses legacy SONET failure indicators like path alarm indication signal (AIS-P) and path remote defect indication (RDI-P) to detect member failure. You can select SW-LCAS during VCAT circuit creation.

In addition, you can create non-LCAS VCAT circuits, which do not use LCAS or SW-LCAS. While LCAS and SW-LCAS member cross-connects can be in different service states, all In Group non-LCAS members must have cross-connects in the same service state. A non-LCAS circuit can mix Out of Group and In Group members, as long as the In Group members are in the same service state. Non-LCAS members do not support the OOS-MA,OOG service state; to put a non-LCAS member in the Out of Group VCAT state, use OOS-MA,DSBLD.

Note Protection switching for LCAS and non-LCAS VCAT circuits might exceed 60 ms. Traffic loss for VT VCAT circuits is approximately two times more than traffic loss for an STS VCAT circuit. You can minimize traffic loss by reducing path differential delay.

7.7.4 VCAT Circuit Size

Table 7-5 lists supported VCAT circuit rates and the number of members for each card.

Table 7-5 ONS 15310-CL Card VCAT Circuit Rates and Members

Card	Circuit Rate	Number of Members
CE-100T-8 [1]	VT1.5	1–64
	STS-1	1–3
ML-100T-8 [1]	STS-1	1–2

1. A VCAT circuit with an ONS 15310-CL CE-100T-8 or ML-100T-8 card as a source or destination and an ONS 15454 ML-Series card as a source or destination can have only two members.

Use the Members tab in the Edit Circuit window to add or delete members from a VCAT circuit. The capability to add or delete members depends on whether the VCAT circuit is LCAS, SW-LCAS, or non-LCAS:

- For VCAT LCAS circuits, you can add or delete members without affecting service. Before deleting a member, Cisco recommends that you put the member in the OOS-MA,OOG service state.
- For SW-LCAS circuits used when interoperating with ONS 15454 ML-Series cards, you cannot add or delete members.
- For non-LCAS VCAT circuits for the CE-100T-8 cards, adding and deleting members to the circuit is possible, but service-affecting. For ML-100T-8 cards, you cannot add or delete members from non-LCAS VCAT circuits without affecting the entire VCAT circuit.

Table 7-6 summarizes the VCAT capabilities for the CE-100T-8 and ML-100T-8 cards.

Table 7-6 ONS 15310-CL VCAT Card Capabilities

Card	Mode	Add a Member	Delete a Member	Support OOS-MA,OOG
CE-100T-8	LCAS	Yes	Yes	Yes
	SW-LCAS	No	No	No
	Non-LCAS	Yes[1]	Yes[1]	No
ML-100T-8	LCAS	Yes	Yes	Yes
	SW-LCAS	No	No	No
	Non-LCAS	No	No	No

1. For CE-100T-8 cards, you can add or delete members after creating a VCAT circuit with no protection. During the time it takes to add or delete members (from seconds to minutes), the entire VCAT circuit will be unable to carry traffic.

7.8 Path Trace

SONET J1 and J2 path trace are repeated, fixed-length strings composed of 64 consecutive bytes. You can use the strings to monitor interruptions or changes to circuit traffic. Table 7-7 shows the ONS 15310-CL cards that support J1 and/or J2 path trace.

Table 7-7 ONS 15310-CL Cards Capable of J1/J2 Path Trace

Trace Function	J1 or J2	Cards
Transmit and receive	J1	15310-CL-CTX (DS-1 and DS-3 port)
		ML-100T-8
	J1 and J2	CE-100T-8
Receive	J1	15310-CL-CTX (EC-1 port)
		15310-CL-CTX (OC-3 port)
		15310-CL-CTX (OC-12 port)

If the string received at a circuit drop port does not match the string that the port expects to receive, an alarm is raised. Two path trace modes are available:

- Automatic—The receiving port assumes that the first string it receives is the baseline string.
- Manual—The receiving port uses a string that you manually enter as the baseline string.

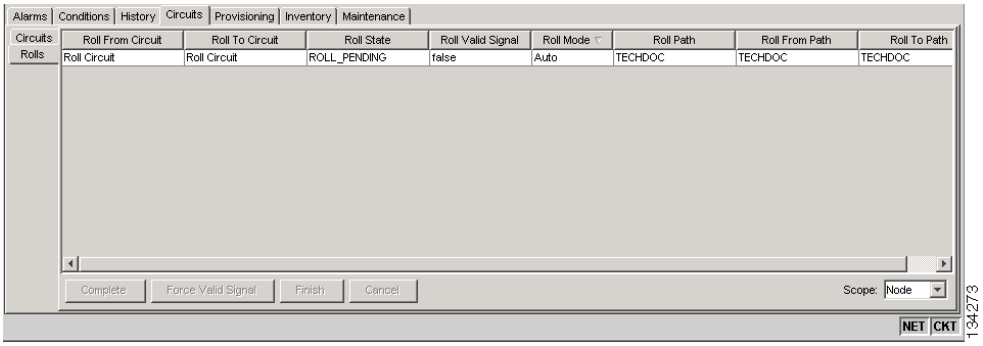
7.9 Bridge and Roll

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.

7.9.1 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 7-5 shows the Rolls window.

Figure 7-5 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 "7.9.2 Roll Status" section on page 7-15 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.

7.9.2 Roll Status

Table 7-8 lists the roll statuses. You can only reroute circuits that have a DISCOVERED status. (See Table 7-1 on page 7-3 for a list of circuit statuses.) You cannot reroute circuits that are in the ROLL_PENDING status.

Table 7-8 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.

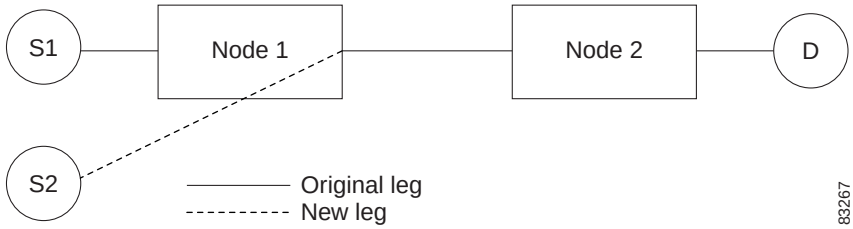
7.9.3 Single and Dual Rolls

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 7-6 and Figure 7-7, respectively).
- Roll a segment of the circuit onto another chosen circuit (Figure 7-8 on page 7-17). This roll also results in a new destination or a new source.

In Figure 7-6, you can select any available STS on Node 1 for a new source.

Figure 7-6 Single Source Roll



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

Figure 7-7 Single Destination Roll

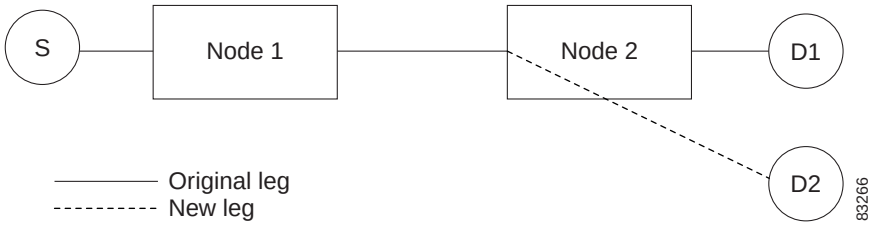


Figure 7-8 shows one circuit rolling onto another circuit at the destination. The new circuit has cross-connects on Node 1, Node 3, and Node 4. CTC deletes the cross-connect on Node 2 after the roll.

Figure 7-8 Single Roll from One Circuit to Another Circuit (Destination Changes)

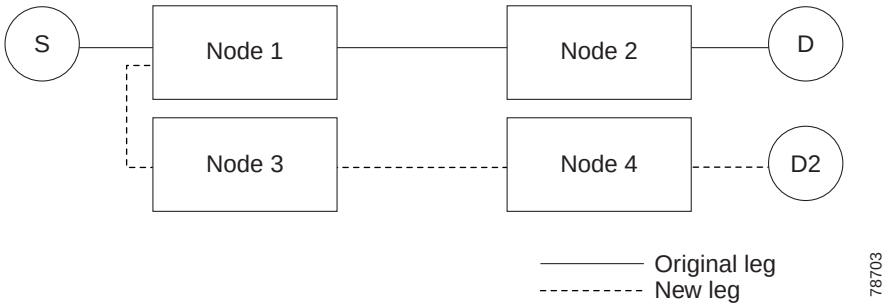
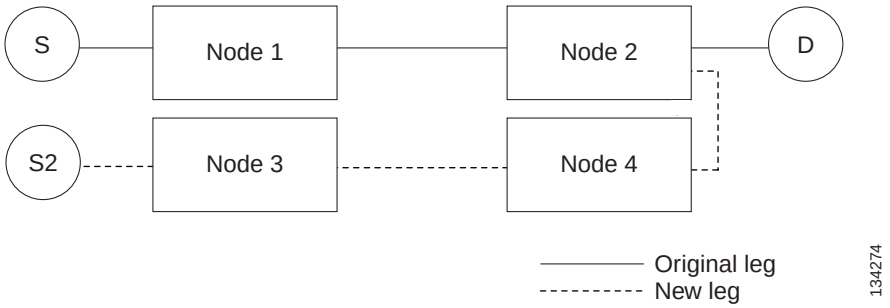


Figure 7-9 shows one circuit rolling onto another circuit at the source.

Figure 7-9 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 7-10 illustrates a dual roll on the same circuit.

Figure 7-10 Dual Roll to Reroute a Link

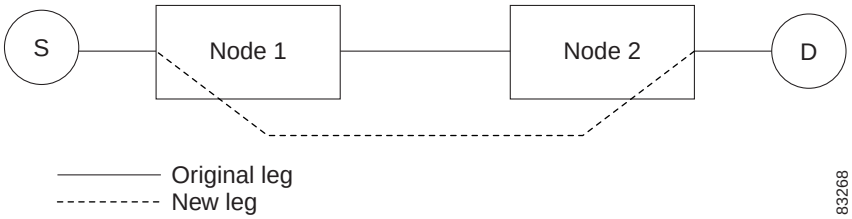
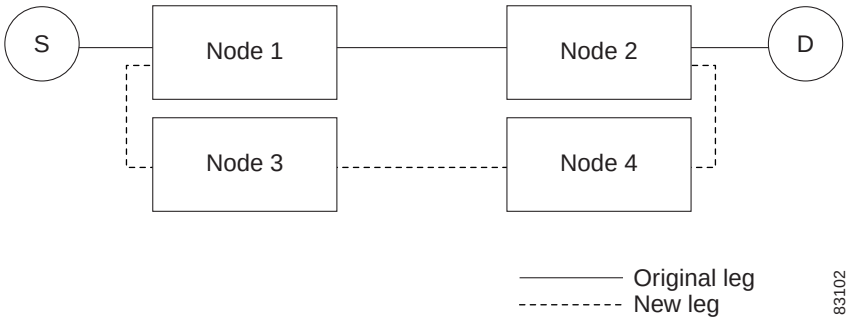


Figure 7-11 illustrates a dual roll involving two circuits.

Figure 7-11 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.

7.9.4 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.

7.9.5 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.

7.10 Merged Circuits

A circuit merge combines a single selected circuit with one or more circuits. You can merge VT tunnels, VAP circuits, orderwire and user data channel (UDC) overhead circuits, CTC-created traffic circuits, and TL1-created traffic circuits. To merge circuits, you choose a master circuit on the CTC Circuits tab. Then, you choose the circuits that you want to merge with the 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.
- Circuit endpoints 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 the 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.

7.11 Reconfigured 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, 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 might merge and others might split into multiple circuits. If the resulting circuit is a valid circuit, it appears as a DISCOVERED circuit. Otherwise, the circuit appears as a PARTIAL or PARTIAL_TL1 circuit.

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

CHAPTER 8

SONET Topologies and Upgrades

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

This chapter explains Cisco ONS 15310-CL SONET topologies and upgrades. To provision topologies, refer to the *Cisco ONS 15310-CL Procedure Guide*.

Chapter topics include:

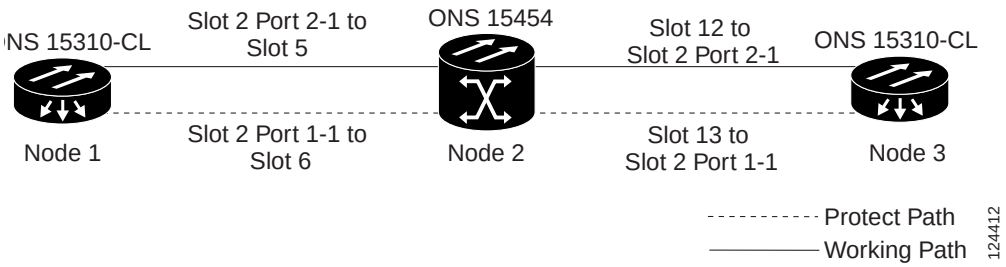
8.1 Terminal Point-to-Point and Linear ADM Configurations

You can configure ONS 15310-CLs in a terminal point-to-point network (two nodes) or as a line of add/drop multiplexers (ADMs) (3 or more nodes) by configuring the OC-3 ports as the working path and a second set as the protect path. Unlike rings, terminal and linear ADMs require that the OC-3 port at each node be in 1+1 protection to ensure that a break to the working line is automatically routed to the protect line.

Note In a linear ADM configuration, two OC-N ports in 1+1 protection are connected to two OC-N ports in 1+1 protection on a second node. On the second node, two more OC-N ports are connected to a third node. The third node can be connected to a fourth node, and so on, depending on the number of nodes in the linear ADM. The ONS 15310-CL has only two optical ports. This restricts an ONS 15310-CL to being the end node in a linear ADM network since both ports are necessary to create the 1+1 protection group to the neighbor node.

Figure 8-1 shows two ONS 15310-CLs in a linear ADM configuration with an ONS 15454. In this example, working traffic flows from the ONS 15310 Node 1/Slot 2/Port 2-1 to the ONS 15454 Node 2/Slot 5, and from Node 2/Slot 12 to the ONS 15310 Node 3/Slot 2/Port 2-1. You create the protect path by placing Slot 2/Port 2-1 in 1+1 protection with Slot 2/Port 1-1 at Nodes 1 through 3.

Figure 8-1 Linear ADM Configuration



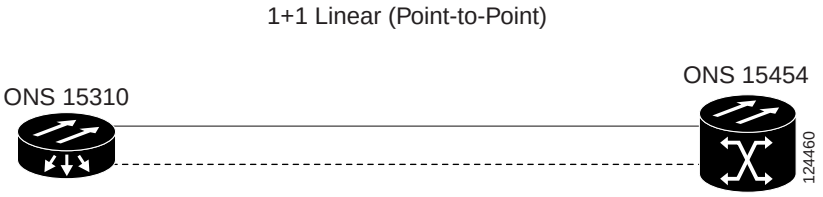
8.2 Interoperability

The ONS 15310-CL supports up to ten SONET SDCCs and 1 path protection per node. You can install ONS 15310-CL nodes into a network comprised entirely of ONS 15310-CL nodes or into a network that has a mix of ONS 15310-CL, ONS 15454, and ONS 15327 nodes. The ONS 15310-CL interoperates with the ONS 15454 and ONS 15327 in linear or path protection configurations. Because connection procedures for these 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 "Add and Remove Nodes" chapter of the *Cisco ONS 15310-CL Procedure Guide* whenever you make connections between ONS 15310-CL, ONS 15454, and ONS 15327 nodes.

8.2.1 Linear Connections

Figure 8-2 shows a basic linear or path protection connection between ONS 15310-CL and ONS 15454 nodes.

Figure 8-2 Linear or Path Protection Connection Between ONS 15454 and ONS 15310-CL Nodes



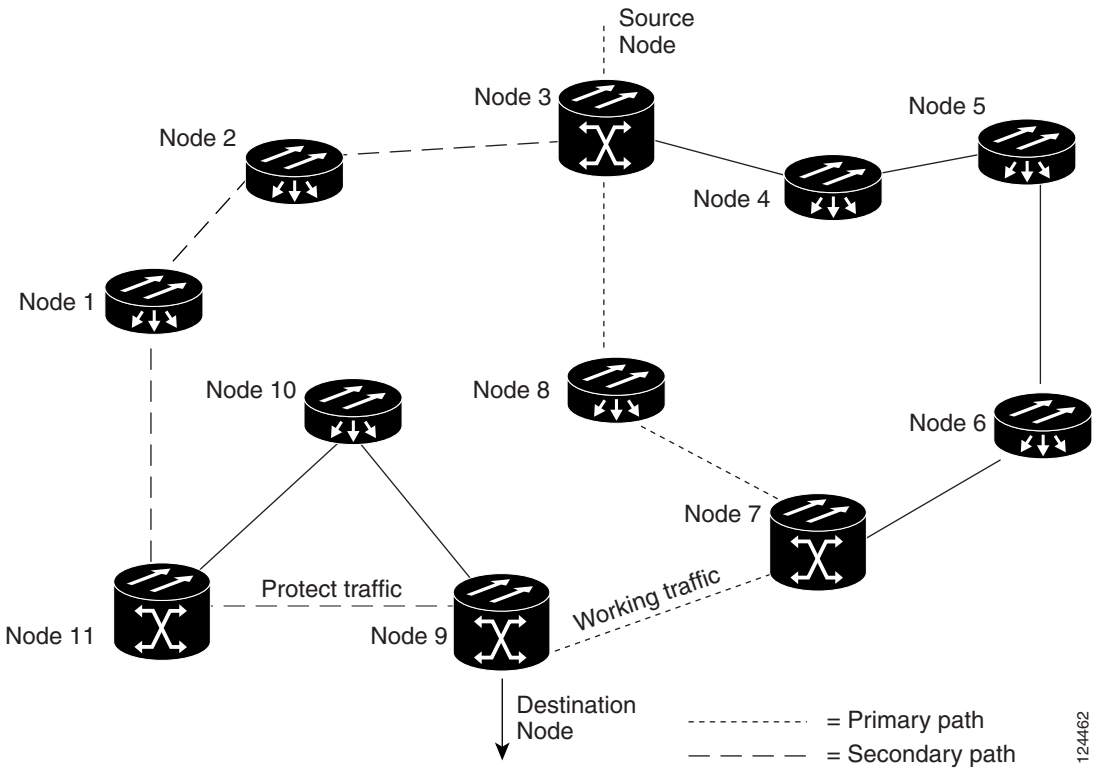
8.3 Path-Protected Mesh Networks

In addition to single path protection configurations, terminal point-to-point or linear ADMs, you can extend ONS 15310-CL traffic protection by creating path-protected mesh networks (PPMNs). PPMNs include multiple ONS 15310-CL 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 8-3, 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 8-3 Path-Protected Mesh Network



8.4 Four Node Configurations

You can link multiple ONS 15310-CLs using their OC-3 ports (also known as creating a fiber-optic bus) to accommodate more access traffic than a single ONS 15310-CL can support. For example, to drop more than 21 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 15310-CL. You can link nodes with OC-3 fiber spans as you would link any other two network nodes. The nodes can be grouped in one facility to aggregate more local traffic.

8.5 OC-N Speed Upgrades

A span is the optical fiber connection between two ONS 15310-CL nodes. In a span (optical speed) upgrade, the transmission rate of a span is upgraded from an OC-3 to OC-12 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. The ONS 15310-CL supports the span upgrade wizard if you are upgrading two ONS 15310-CLs with 1+1 protection from OC-3 to OC-12.

To perform a span upgrade, the higher-rate pluggable port module (PPM) must replace the lower-rate PPM in the same slot. If you are using a multi-rate PPM, you do not need to physically replace the PPM. All spans in the network must be upgraded. The 1+1 protection configuration of the original lower-rate PPM is retained for the higher-rate PPM.

When performing span upgrades, Cisco recommends that you upgrade all spans in a network consecutively and in the same maintenance window. Until all spans are upgraded, mismatched PPM types will be present.

If you are upgrading two ONS 15310-CLs with 1+1 protection from OC-3 to OC-12, 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 will cause no more than three switches, each of which is less than 50 ms in duration. To initiate the span upgrade, right-click the span and choose Span Upgrade.

Note Span upgrades do not upgrade SONET topologies (for example, a 1+1 group to a path protection). Refer to the “Convert Network Configurations” chapter of the *Cisco ONS 15310-CL Procedure Guide* for topology upgrade procedures.

8.5.1 Span Upgrade Wizard

The Span Upgrade Wizard automates all steps in the manual 1+1 span upgrade procedure, if you are upgrading two ONS 15310-CLs from OC3 to OC12. The wizard can upgrade both lines of a 1+1 group. 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.

8.5.2 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 1+1 protection group, if you are upgrading two ONS 15310-CLs from OC-3 to OC-12.

Downgrading can be performed to back out of a span upgrade. The procedure for downgrading is the same as upgrading except that you provision a lower-rate PPM (OC-3) and install a lower-rate PPM (if you are not using a multi-rate PPM). You cannot downgrade if circuits exist on the STSs that will be removed (the higher STSs).

Management Network Connectivity

This chapter provides an overview of ONS 15310-CL data communications network (DCN) connectivity. Cisco Optical Networking System (ONS) network communication is based on IP, including communication between Cisco Transport Controller (CTC) computers and ONS 15310-CL nodes, and communication among networked ONS 15310-CL nodes. The chapter provides scenarios showing Cisco ONS 15310-CL nodes 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.

Although ONS 15310-CL DCN communication is based on IP, ONS 15310-CL nodes can be networked to equipment that is based on the Open System Interconnection (OSI) protocol suites. This chapter describes the ONS 15310-CL OSI implementation and provides scenarios that show how the ONS 15310-CL can be networked within a mixed IP and OSI environment.

Chapter topics include:

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 15310-CL networking setup instructions, refer to the "Turn Up Node" chapter of the *Cisco ONS 15310-CL Procedure Guide*.

Note To connect ONS 15310-CL nodes 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 15310-CL nodes 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 15310-CL 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 15310-CL to serve as a gateway for ONS 15310-CL nodes that are not connected to the LAN.
- You can create static routes to enable connections among multiple Cisco Transport Controller (CTC) sessions with ONS 15310-CL nodes that reside on the same subnet with multiple CTC sessions.
- If ONS 15310-CL nodes are connected to Open Shortest Path First (OSPF) networks, ONS 15310-CL network information is automatically communicated across multiple LANs and WANs.
- The ONS 15310-CL proxy server controls the visibility and accessibility between CTC computers and ONS 15310-CL element nodes.

9.2 IP Addressing Scenarios

ONS 15310-CL IP addressing generally has seven 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 15310-CL nodes in IP networks.

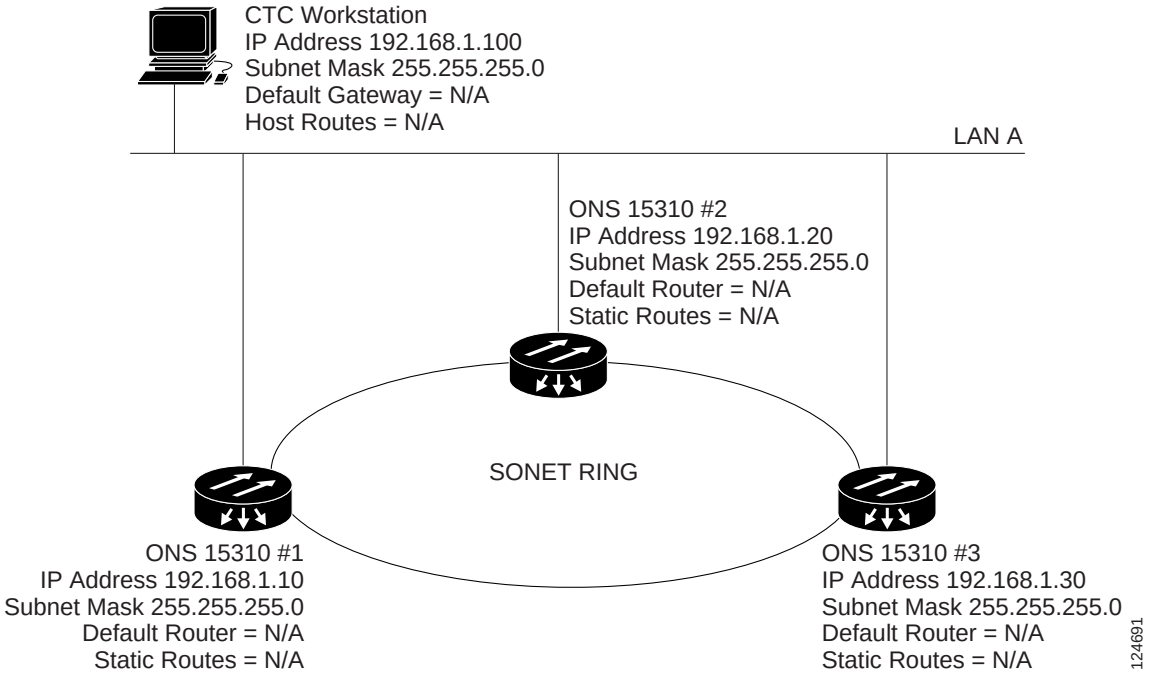
Table 9-1 General ONS 15310-CL IP Troubleshooting Checklist

Item	What to Check
Link integrity	Verify that link integrity exists between: • CTC computer and network hub/switch • ONS 15310-CL nodes (RJ-45 ports labeled LAN) and network hub/switch • Router ports and hub/switch ports
ONS 15310-CL hub/switch ports	Verify connectivity. If connectivity problems occur, set the hub or switch port that is connected to the ONS 15310-CL to 10 Mbps half-duplex.
Ping	Ping the node to test connections between computers and ONS 15310-CL nodes.
IP addresses/subnet masks	Verify that ONS 15310-CL IP addresses and subnet masks are set up correctly.
Optical connectivity	Verify that ONS 15310-CL optical trunk ports are in service and that a DCC is enabled on each trunk port.

9.2.1 Scenario 1: CTC and ONS 15310-CL Nodes on the Same Subnet

Scenario 1 shows a basic ONS 15310-CL LAN configuration (Figure 9-1). The ONS 15310-CL nodes and CTC computer reside on the same subnet. All ONS 15310-CL nodes connect to LAN A and have DCC connections.

Figure 9-1 Scenario 1: CTC and ONS 15310-CL Nodes on the Same Subnet

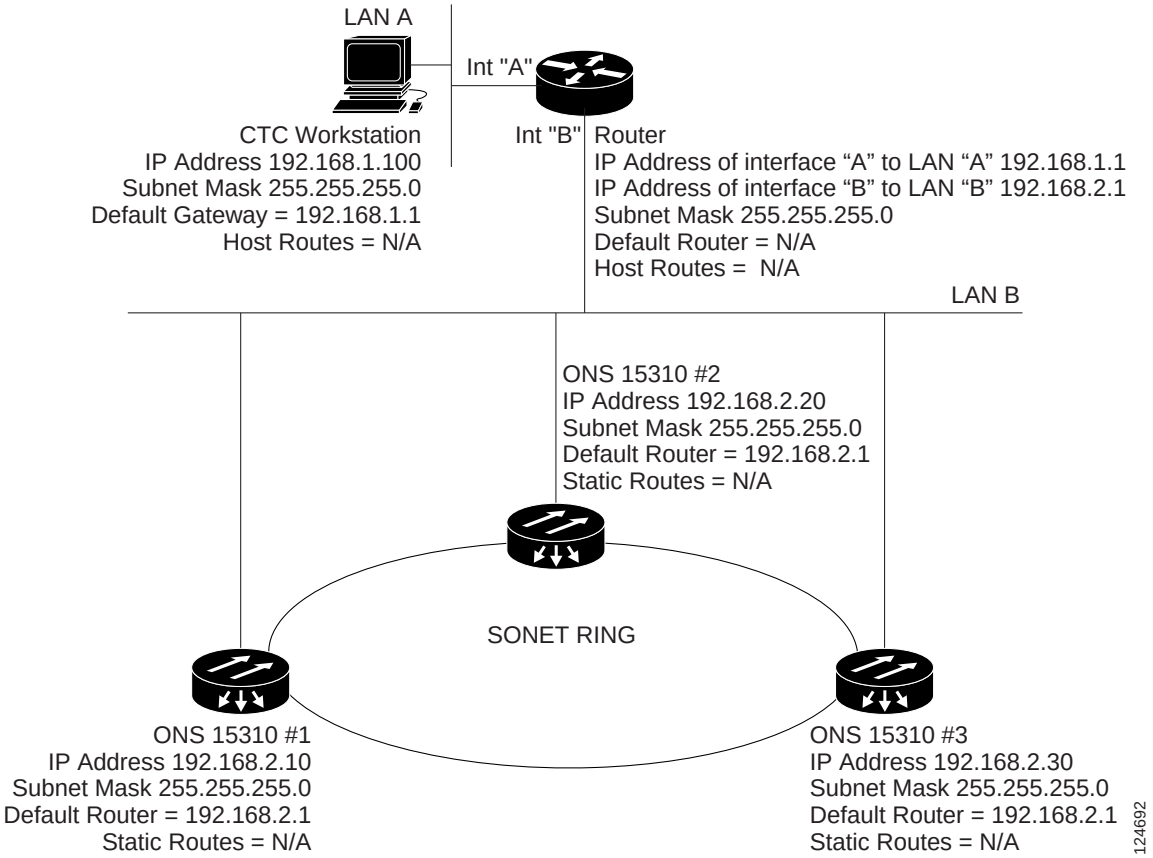


9.2.2 Scenario 2: CTC and ONS 15310-CL Nodes Connected to a Router

In Scenario 2 the CTC computer resides on a subnet (192.168.1.0) and attaches to LAN A (Figure 9-2). The ONS 15310-CL nodes 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 15310-CL Nodes Connected to Router



9.2.3 Scenario 3: Using Proxy ARP to Enable an ONS 15310-CL Gateway

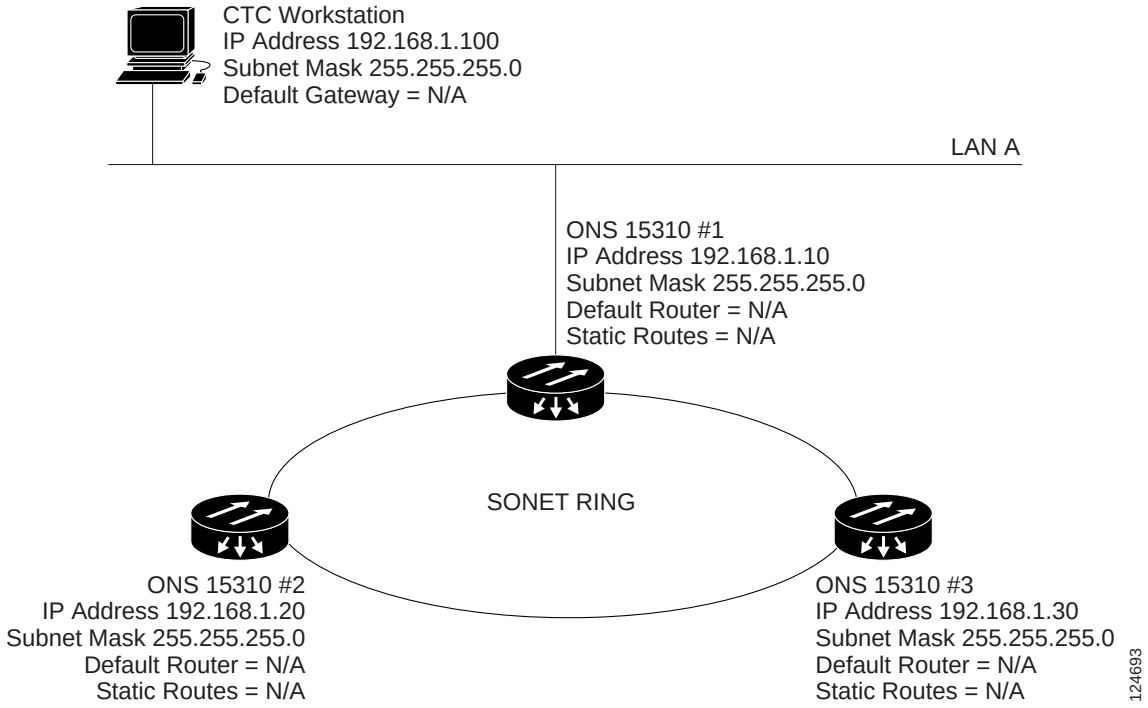
ARP matches higher-level IP addresses to the physical addresses of the destination host. It uses a lookup table (called ARP cache) to perform the translation. When the address is not found in the ARP cache, a broadcast is sent out on the network with a special format called the ARP request. If one of 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 15310-CL to respond to the ARP request for ONS 15310-CL nodes not connected to the LAN. (ONS 15310-CL proxy ARP requires no user configuration.) For the proxy ARP node to require no user confirmation, the DCC-connected ONS 15310-CL nodes must reside on the same subnet. When a LAN device sends an ARP request to an ONS 15310-CL that is not connected to the LAN, the gateway ONS 15310-CL returns its MAC address to the LAN device. The LAN device then sends the datagram for the remote ONS 15310-CL to the MAC address of the proxy ONS 15310-CL. The proxy ONS 15310-CL uses its routing table to forward the datagram to the non-LAN ONS 15310-CL.

Scenario 3 is similar to Scenario 1, but only one ONS 15310-CL (#1) connects to the LAN (Figure 9-3). Two ONS 15310-CL nodes (#2 and #3) connect to ONS 15310-CL 1 through the SONET DCC. Because all three ONS 15310-CL nodes are on the same subnet, Proxy ARP enables ONS 15310-CL #1 to serve as a gateway for ONS 15310-CL #2 and #3.

Note This scenario assumes all CTC connections are to ONS 15310-CL #1. If you connect a laptop to either #2 or #3, network partitioning occurs, and neither the laptop or 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 15310-CL proxy server (see Scenario 7).

Figure 9-3 Scenario 3: Using Proxy ARP

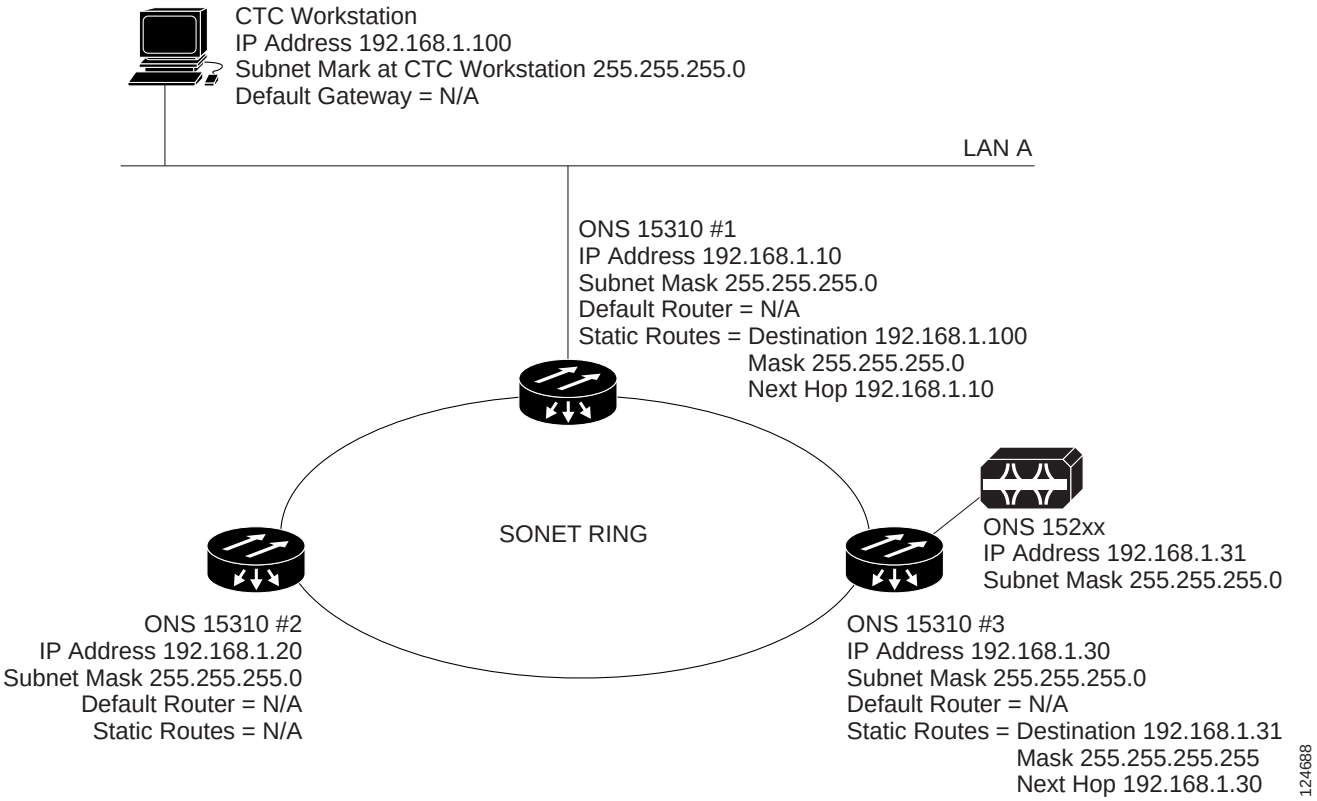


You can also use proxy ARP to communicate with hosts attached to the craft Ethernet ports of DCC-connected nodes (Figure 9-4). The node with an attached host must have a static route to the host. Static routes are propagated to all DCC peers using OSPF. The existing proxy ARP node is the gateway for 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.

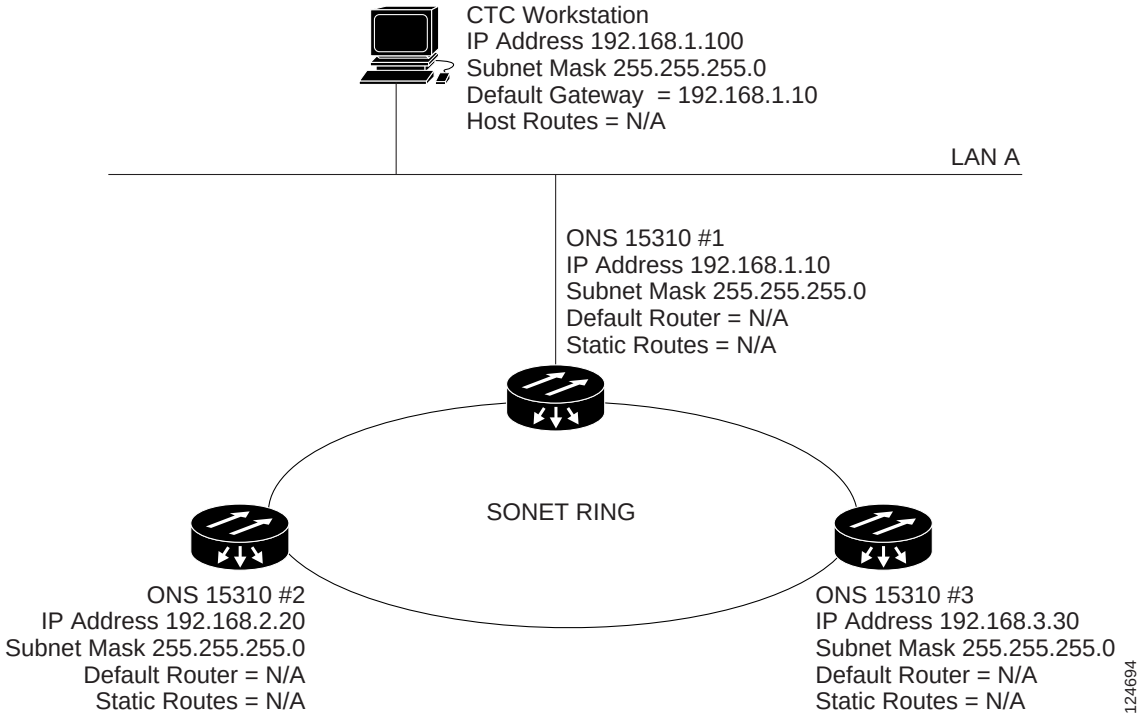
Figure 9-4 Scenario 3: Using Proxy ARP with Static Routing



9.2.4 Scenario 4: Default Gateway on CTC Computer

Scenario 4 is similar to Scenario 3, but ONS 15310-CL #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. 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



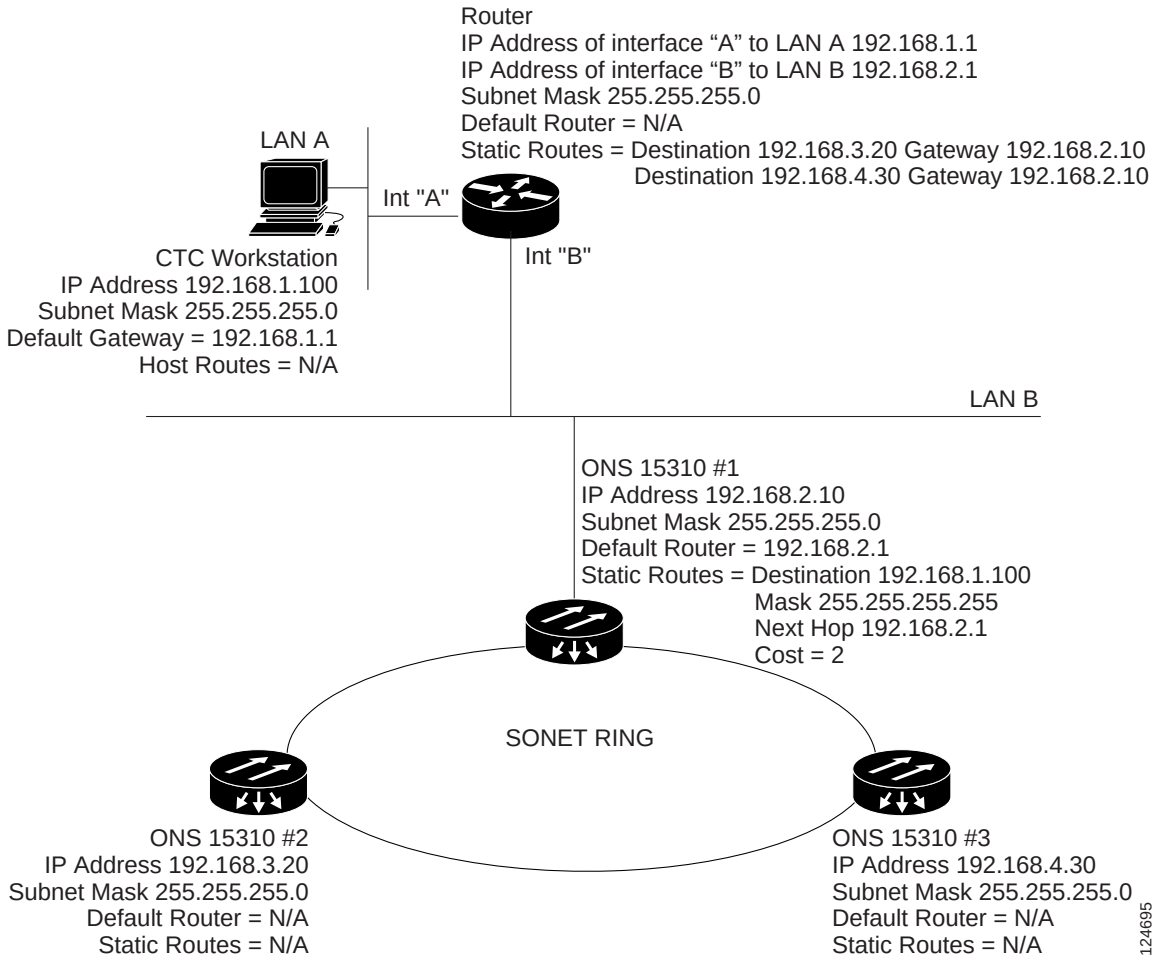
9.2.5 Scenario 5: Using Static Routes to Connect to LANs

Static routes are used for two purposes:

- To connect ONS 15310-CL nodes to CTC sessions on one subnet that are connected by a router to ONS 15310-CL nodes 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 15310-CL nodes residing on the same subnet.

In Figure 9-6, one CTC residing on subnet 192.168.1.0 connects to a router through interface A. (The router is not set up with OSPF.) ONS 15310-CL nodes 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

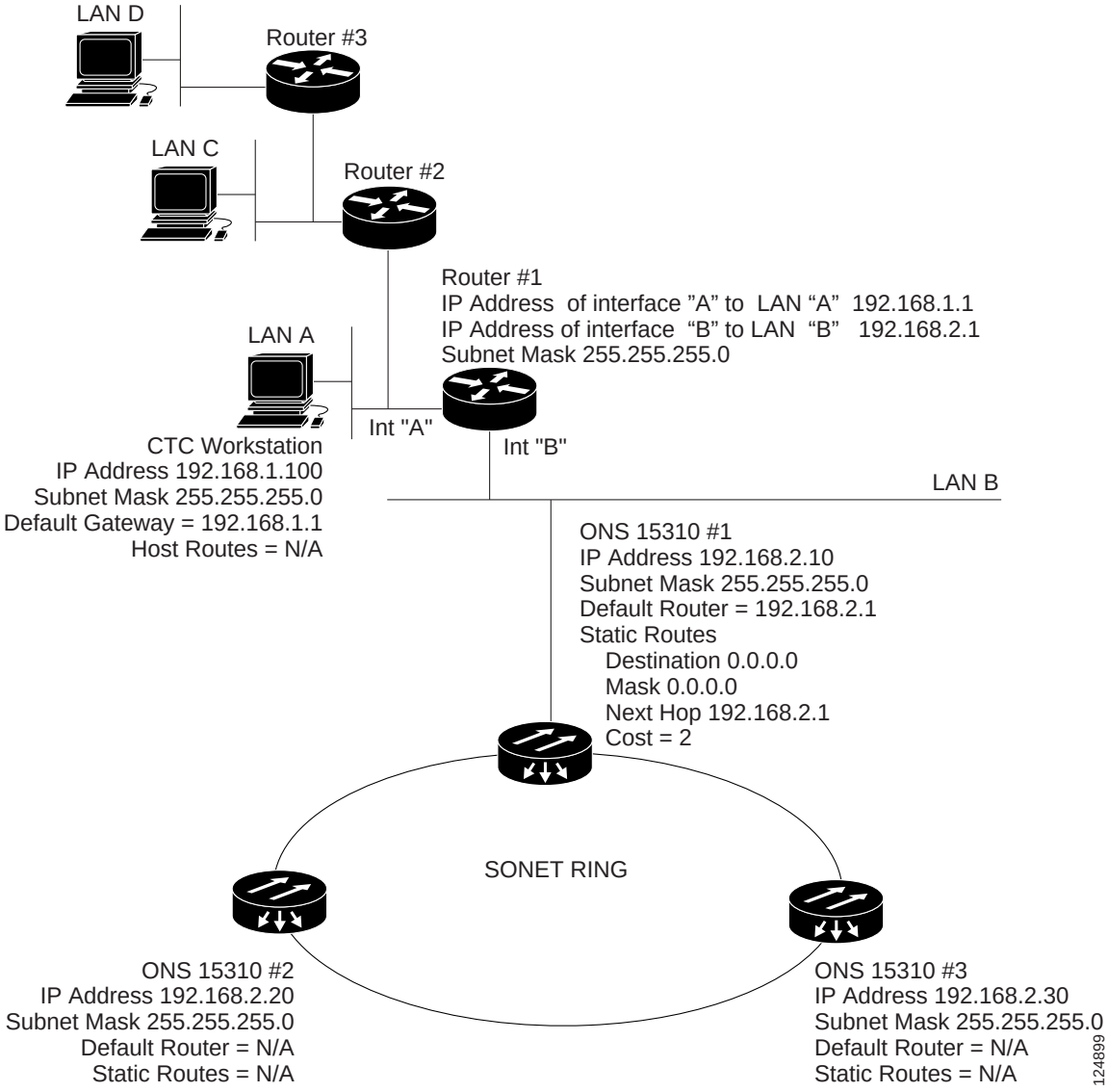


The destination and subnet mask entries control access to the ONS 15310-CL nodes:

- 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

Open Shortest Path First (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 link state "advertisements" 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 15310-CL uses OSPF protocol in internal ONS 15310-CL networks for node discovery, circuit routing, and node management. You can enable OSPF on the ONS 15310-CL so that the ONS 15310-CL topology is sent to OSPF routers on a LAN. Advertising the ONS 15310-CL network topology to LAN routers eliminates the need to enter static routes for ONS 15310-CL 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 15310-CL OSPF topology for advertising to an OSPF network, you must assign an OSPF area ID in decimal format to the ONS 15310-CL network. Coordinate the area ID number assignment with your LAN administrator. All DCC-connected ONS 15310-CL nodes should be assigned the same OSPF area ID.

Figure 9-8 shows a network enabled for OSPF.

Figure 9-8 Scenario 6: OSPF Enabled

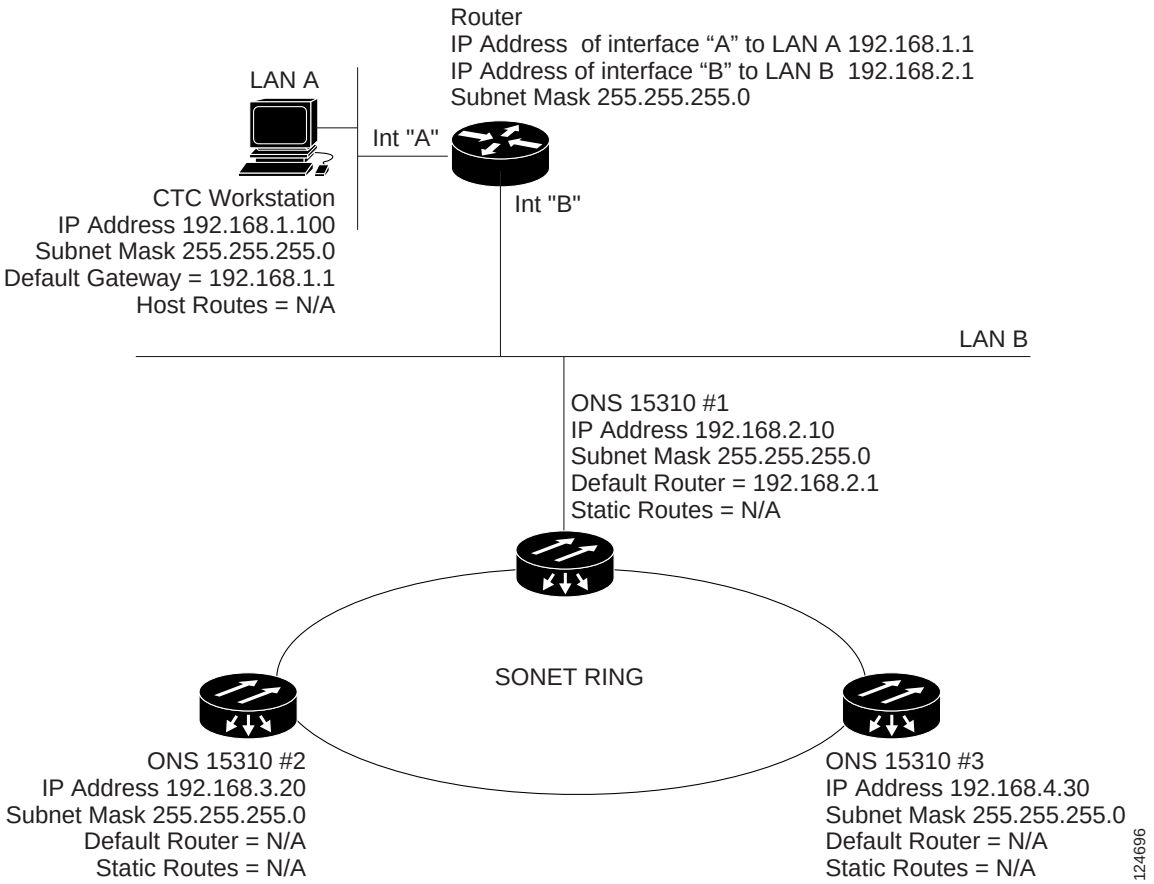
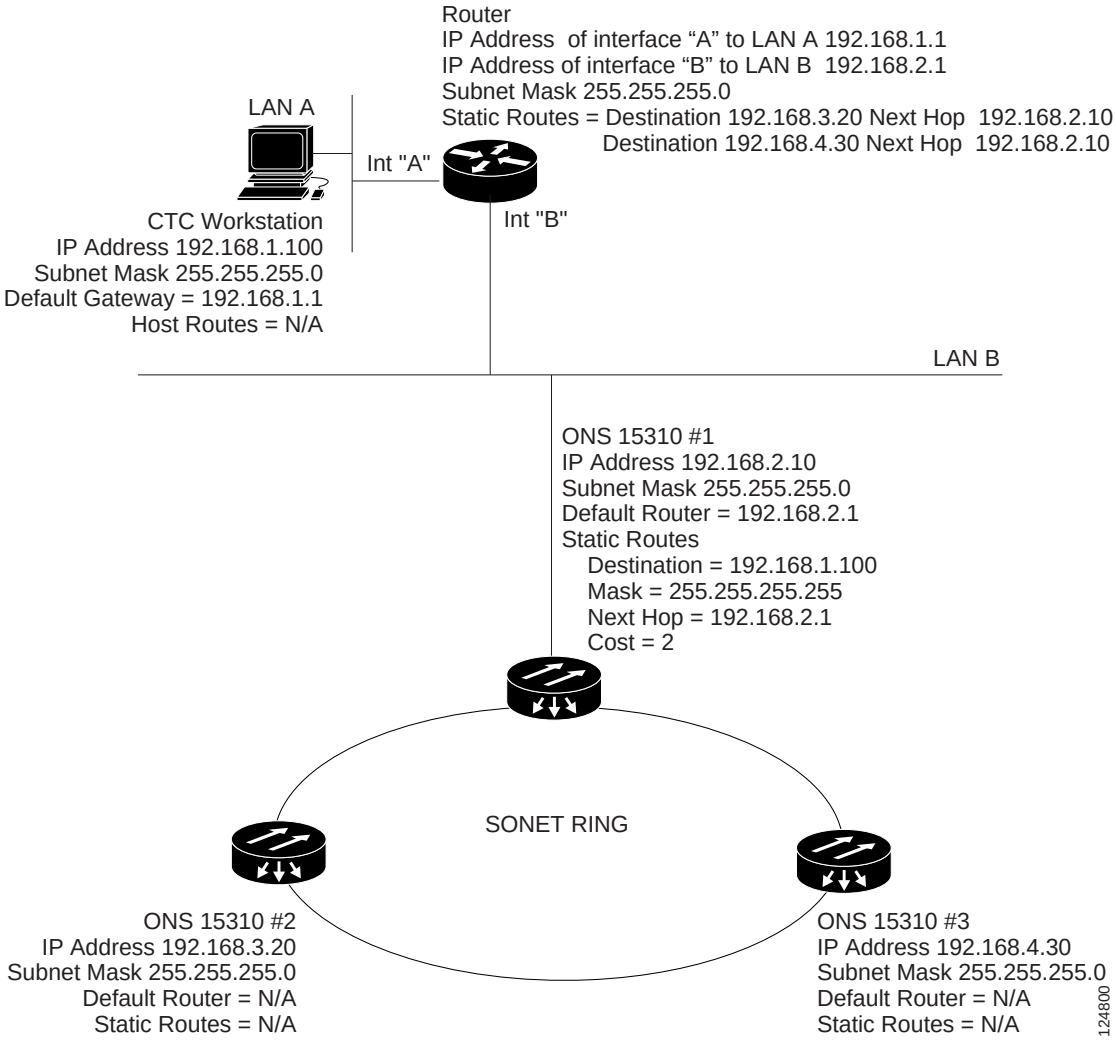


Figure 9-9 shows the same network without OSPF. Static routes must be manually added to the router for CTC computers on LAN A to communicate with Nodes 2 and 3 because these nodes reside on different subnets.

Figure 9-9 Scenario 6: OSPF Not Enabled



9.2.7 Scenario 7: Provisioning the ONS 15310-CL Proxy Server

The ONS 15310-CL proxy server is a set of functions that allows you to network ONS 15310-CL nodes in environments where visibility and accessibility between ONS 15310-CL nodes 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 15310-CL nodes while preventing the field technicians from accessing the NOC LAN. To do this, one ONS 15310-CL is provisioned as a gateway network element (GNE) and the other ONS 15310-CL nodes are provisioned as end network elements (ENEs). The GNE tunnels connections between CTC computers and ENEs, which provides management capability while preventing access for non-ONS 15310-CL management purposes.

The ONS 15310-CL 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 depend on whether the packet arrives at the DCC or CRAFT port Ethernet interface. Table 9-3 on page 9-15 and Table 9-4 on page 9-16 provide the filtering rules.

- Processes SNTP (Simple Network Timing Protocol) and NTP (Network Timing Protocol) requests. Element ONS 15310-CL NEs can derive time-of-day from an SNTP/NTP LAN server through the GNE.
- Process SNMPv1 traps. The GNE receives SNMPv1 traps from the ENE and forwards them to all provisioned SNMPv1 trap destinations.

The ONS 15310-CL proxy server is provisioned using the Enable proxy server on port check box on the Provisioning > Network > General tab. If checked, the ONS 15310-CL serves as a proxy for connections between CTC clients and ONS 15310-CL nodes that are DCC-connected to the proxy ONS 15310-CL. 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 the Enable proxy server on port check box is not checked, 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:

Note If you launch CTC against a node through a NAT (Network Address Translation) or PAT (Port Address Translation) 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.

- External Network Element (ENE)—If set as an ENE, the ONS 15310-CL neither installs nor advertises default or static routes. CTC computers can communicate with the ONS 15310-CL using the craft port, but they cannot communicate directly with any other DCC-connected ONS 15310-CL.

  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 15310-CL 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 15310-CL nodes and firewall is not enabled.

Figure 9-10 shows an ONS 15310-CL 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 LAN ports could be connected to a hub. However, the hub should have no other network connections.

Figure 9-10 ONS 15310-CL Proxy Server with GNE and ENEs on the Same Subnet

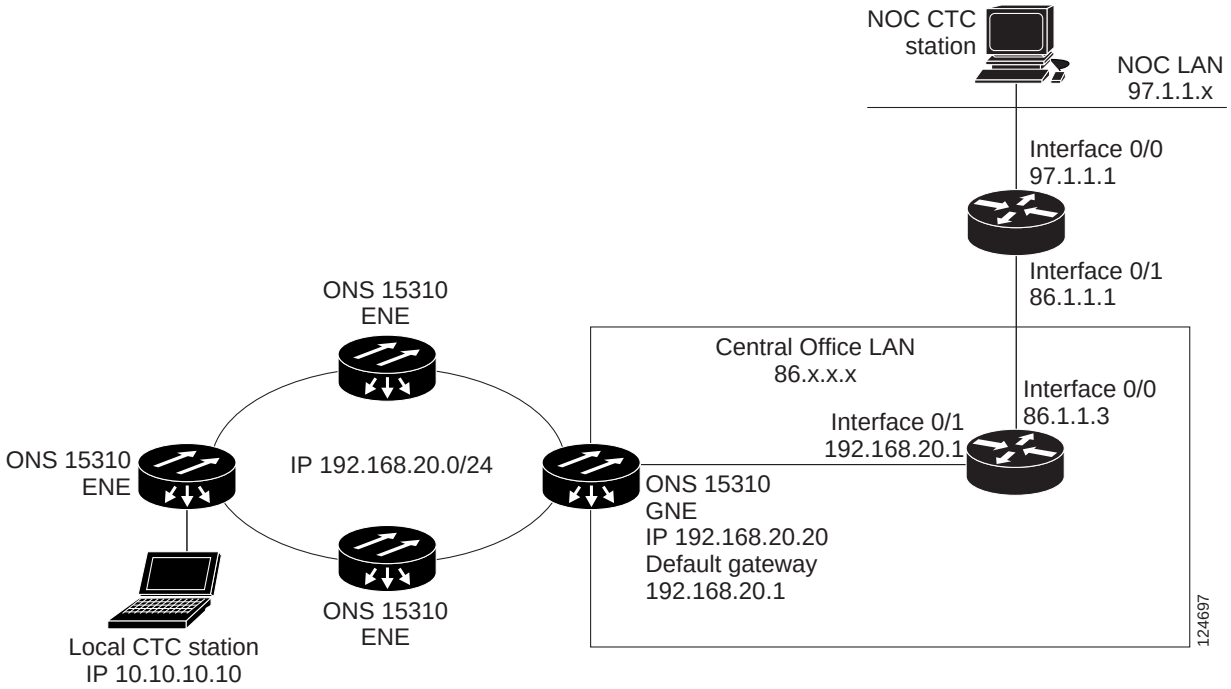


Table 9-2 shows recommended settings for ONS 15310-CL GNEs and ENEs in the configuration shown in Figure 9-10.

Table 9-2 ONS 15310-CL GNE and ENE Settings

Setting	ONS 15310-CL GNE	ONS 15310-CL 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 15310-CL GNE IP address
SNMP (if used)	SNMPv1 trap destinations	Set SNMPv1 trap destinations to ONS 15310-CL GNE

Figure 9-11 shows the same proxy server implementation with ONS 15310-CL ENEs on different subnets. In this example, ONS 15310-CL GNEs and ENEs are provisioned with the settings shown in Table 9-2.

Figure 9-11 Scenario 7: ONS 15310-CL Proxy Server with GNE and ENEs on Different Subnets

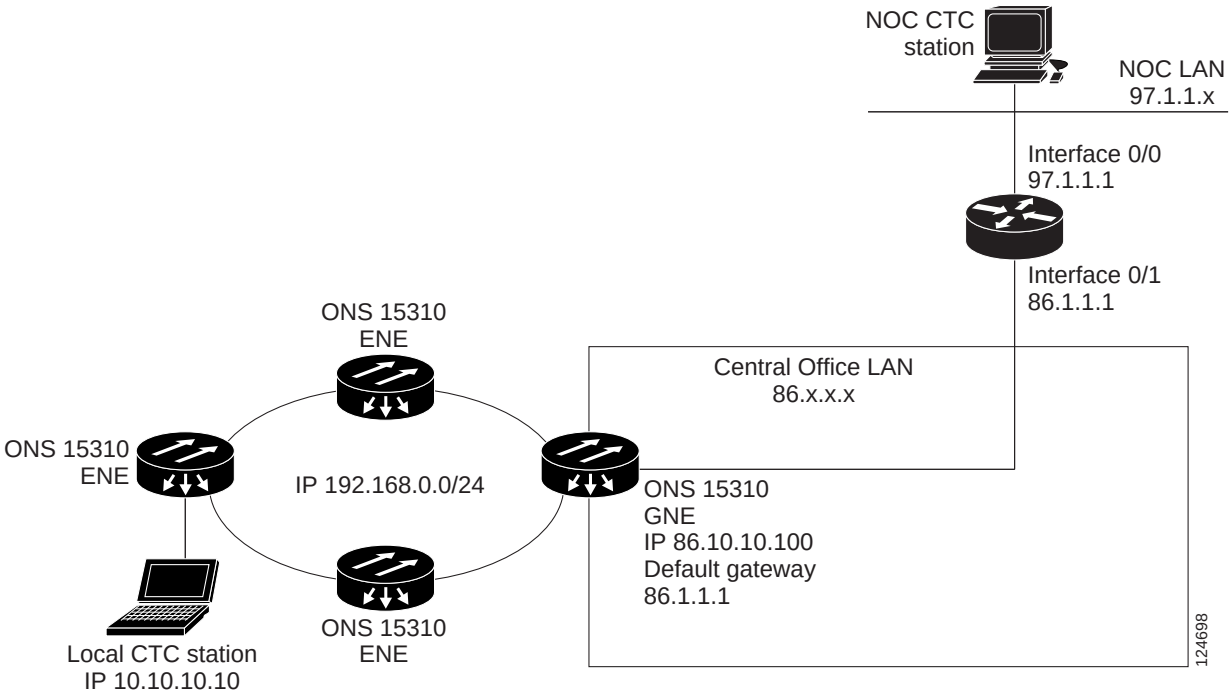


Figure 9-12 shows the implementation with ONS 15310-CL ENEs in multiple rings. In this example, ONS 15310-CL GNEs and ENEs are provisioned with the settings shown in Table 9-2.

Figure 9-12 Scenario 7: ONS 15310-CL Proxy Server with ENEs on Multiple Rings

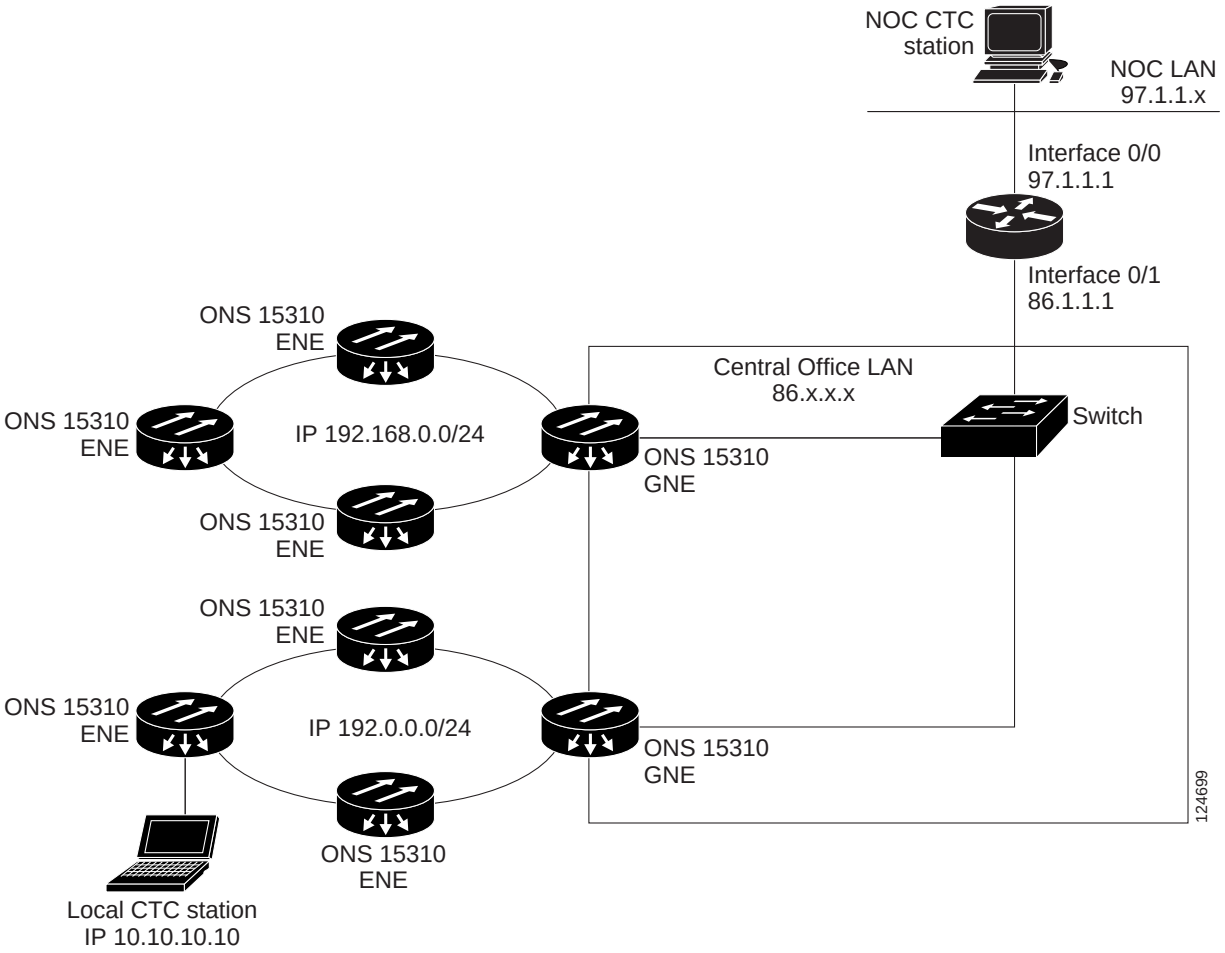


Table 9-3 shows the rules the ONS 15310-CL follows to filter packets when Enable Firewall is enabled.

Table 9-3 Proxy Server Firewall Filtering Rules

Packets arriving at:	Are accepted if the IP destination address is:
15310-CL-CTX Ethernet interface	• The ONS 15310-CL shelf itself • The ONS 15310-CL'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 15310-CL 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 15310-CL is discarded. Rejected packets are silently discarded.

Table 9-4 Proxy Server Firewall Filtering Rules When Packet Addressed to ONS 15310-CL

Packets Arrive At	Accepts	Rejects
15310-CL-CTX LAN port	• 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 packets addressed to the Telnet and SOCKS proxy server ports • 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 15310-CL nodes 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 15310-CL nodes 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 15310-CL.
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 15310-CL.

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

- Disconnect the craft computer from the unreachable ONS 15310-CL. Connect to the ONS 15310-CL through another ONS 15310-CL in the network that has a DCC connection to the unreachable ONS 15310-CL.
- Disconnect the Ethernet cable from the unreachable ONS 15310-CL. Connect a CTC computer directly to the ONS 15310-CL.

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 15310-CL 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 combinations for ONS 15310-CL optical ports 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 15310-CL Trunk Cards	**MXP_2.5G_10G/ TXP_MR_10G**	**TXP(P)_MR_2.5G**	**MXP_2.5G_10E/ TXP_MR_10E**
15310-CL-CTX (OC-3 optical port)	—	Yes	—
15310-CL-CTX (OC-12 optical port)	—	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 an SDCC/LDCC termination.
- If the optical port is the protection port in a 1+1 group, the working port must have an SDCC/LDCC termination provisioned.
- If a remote end (ONS 15454) of a provisionable patchcord is Y-cable protected, an optical port requires two patchcords.

9.4 Routing Table

ONS 15310-CL routing information appears 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 15310-CL interface used to access the destination.
  - cpm0—The ONS 15310-CL Ethernet interface (RJ45 LAN jack)
  - pdcc0—An SDCC interface, that is, an OC-N trunk port identified as the SDCC termination
  - lo0—A loopback interface

Table 9-6 shows sample routing entries for an ONS 15310-CL.

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 15310-CL 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 15310-CL 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 15310-CL-CTX.

Table 9-7 Ports Used by the 15310-CL-CTX

Port	Function	Action[1]
0	Never used	D
20	FTP	D

Table 9-7 Ports Used by the 15310-CL-CTX (continued)

Port	Function	Action[1]
21	FTP control	D
22	SSH (Secure Shell)	D
23	Telnet	D
80	HTTP	D
111	SUNRPC (Sun Remote Procedure Call)	NA
161	SNMP traps destinations	D
162	SNMP traps destinations	D
513	rlogin	NA
683	CORBA IIOP	OK
1080	Proxy server (socks)	D
2001-2017	I/O card Telnet	D
2018	DCC processor on active 15310-CL-CTX	D
2361	TL1	D
3082	Raw TL1	D
3083	TL1	D
5001	Bidirectional line switch ring (BLSR) server port	D
5002	BLSR client port	D
7200	SNMP alarm input port	D
9100	EQM port	D
9401	TCC boot port	D
9999	Flash manager	D
10240-12287	Proxy client	D
57790	Default TCC listener port	OK

1. D = deny, NA = not applicable, OK = do not deny

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 15310-CL 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 15310-CL 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 15310-CL 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 15310-CL (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 15310-CL 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 15310-CL 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 15310-CL 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 15310-CL 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 15310-CL 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 15310-CL (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 15310-CL GNE to CTC ***
```

9.6 Open GNE

The ONS 15310-CL can communicate with non-ONS nodes that do not support point-to-point protocol (PPP) vendor extensions or OSPF type 10 opaque link-state advertisements (LSA), both of which are necessary for automatic node and link discovery. An open GNE configuration allows the DCC-based network to function as an IP network for non-ONS nodes.

To configure an open GNE network, you can provision 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 9-13 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 9-13 Proxy and Firewall Tunnels for Foreign Terminations

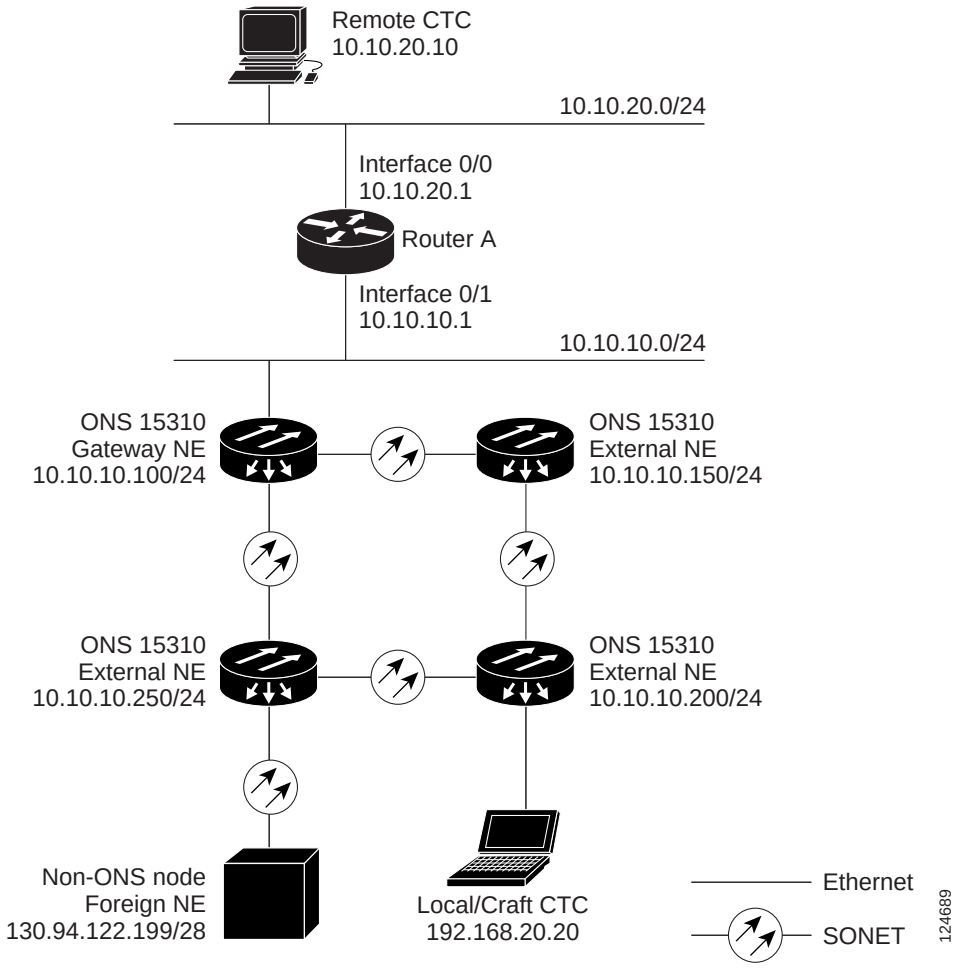
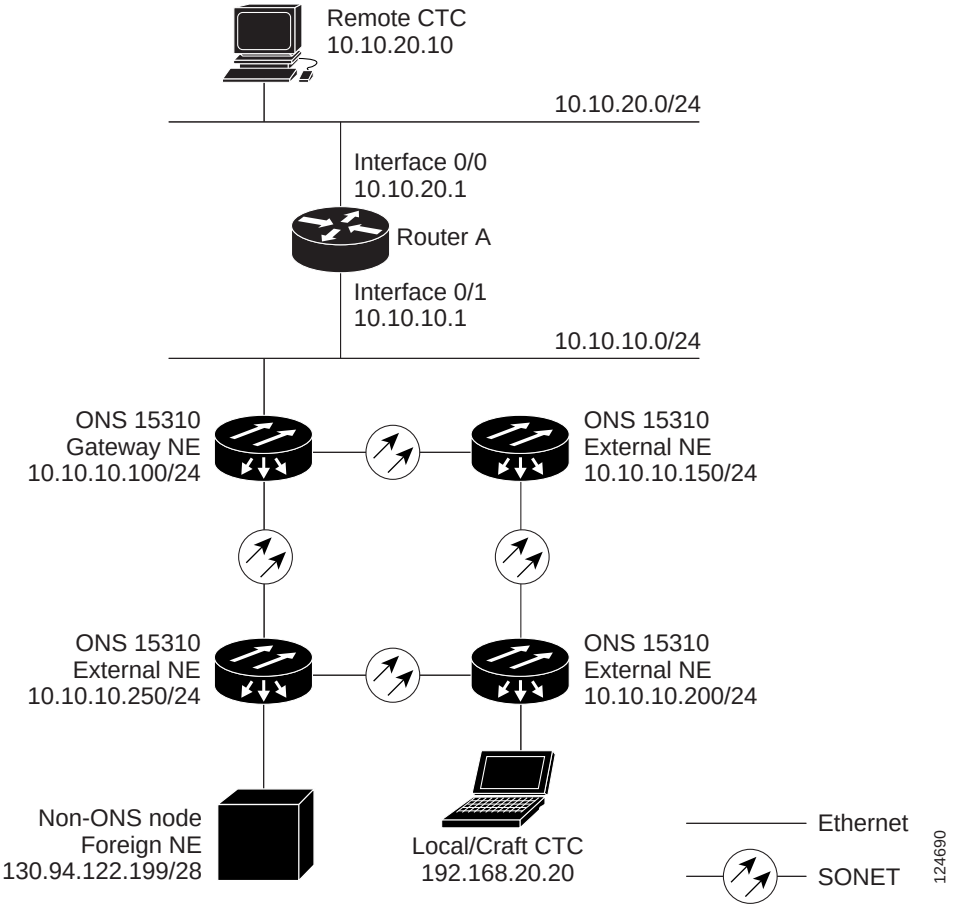


Figure 9-14 shows a remote node connected to an ENE Ethernet port. Proxy and firewall tunnels are useful in this example because the GNE would otherwise block IP access between the PC and foreign node. This configuration also requires a firewall tunnel on the ENE.

Figure 9-14 Foreign Node Connection to an ENE Ethernet Port



9.7 TCP/IP and OSI Networking

ONS 15310-CL DCN communication is based on the TCP/IP protocol suite. However, ONS 15310-CL 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

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 15310-CL 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 15310-CL 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

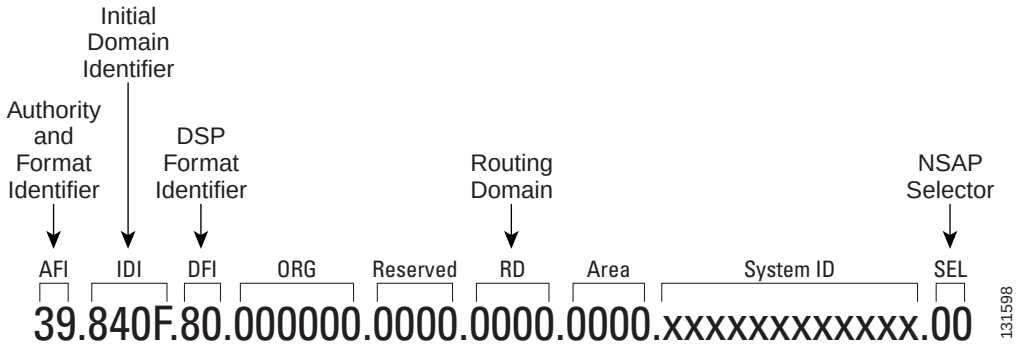
Field	Definition	Description
IDP		
AFI	Authority and format identifier	Specifies the NSAP address format. The initial value is 39 for the ISO-DCC address format.
IDI	Initial domain identifier	Specifies the country code. The initial value is 840F, the United States country code padded with an F.
DSP		
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 15310-CL system identifier is set to its IEEE 802.3 MAC address. Each ONS 15310-CL 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 15310-CL 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 9-28, and the "9.7.4.2 Intermediate System-to-Intermediate System Protocol" section on page 9-28.) • 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 9-15 shows the ISO-DCC NSAP address with the default values delivered with the ONS 15310-CL. The System ID is automatically populated with the node MAC address.

Figure 9-15 ISO-DCC NSAP Address



The ONS 15310-CL 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 the Provisioning > OSI > Routers subtab. See the "9.7.6 OSI Virtual Routers" section on page 9-32 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 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.

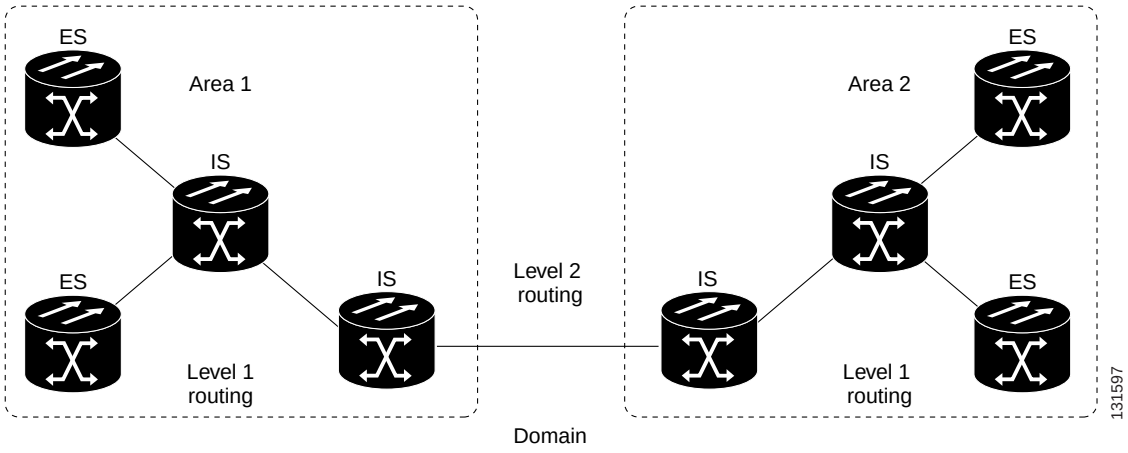
An IS composes intermediate system hello (ISH) messages to announce its configuration information to ISs and ESs that are connected to the same broadcast subnetwork. Like the ESHs, the ISH contains the addressing information for the IS (the NET and the subnetwork point-of-attachment address [SNPA]) and 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 9-16 shows an example of Level 1 and Level 2 routing.

Note The ONS 15310-CL 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 9-16 Level 1 and Level 2 OSI Routing



When you provision an ONS 15310-CL 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 15310-CL 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 15310-CL 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 Protocol

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 15310-CL. 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 9-25).

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 the Type 1 PDU.	After an NE originates a TARP Type 2 PDU, the PDU is sent to all Level 1 and Level 2 neighbors.
3	Sent as a response to Type 1, Type 2, or Type 5 PDUs.	After a TARP Request (Type 1 or 2) PDU is received, a TARP Type 3 PDU is sent to the request originator. Type 3 PDUs do not use the TARP propagation procedures.
4	Sent as a notification when a change occurs locally, for example, a TID or NSAP change. It might also be sent when an NE initializes.	A Type 4 PDU is a notification of a TID or Protocol Address change at the NE that originates the notification. The PDU is sent to all adjacencies inside and outside the NE's routing area.
5	Sent when a device needs a TID that corresponds to a specific NSAP.	When a Type 5 PDU is sent, the CLNP destination address is known, so the PDU is sent to only that address. Type 5 PDUs do not use the TARP propagation procedures.

9.7.5.1 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.

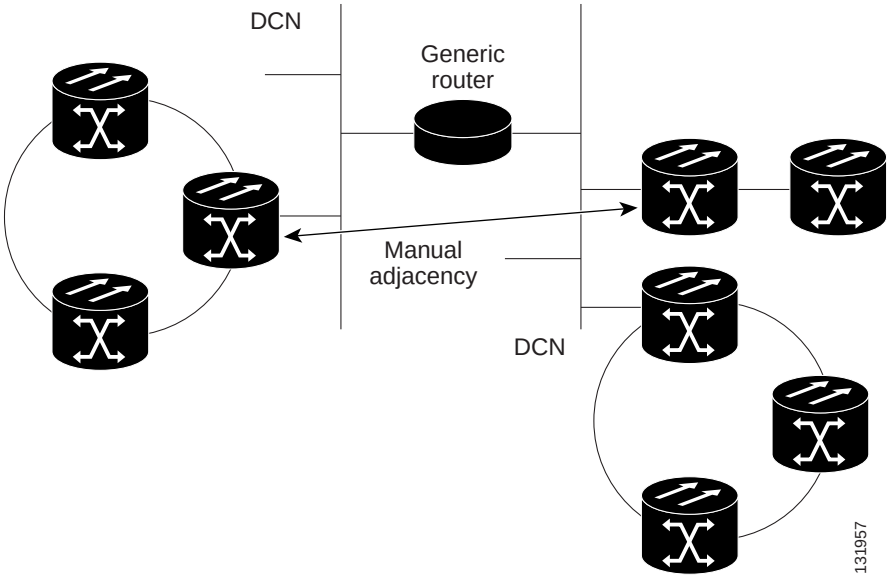
9.7.5.2 TARP Loop Detection Buffer

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 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 15310-CL 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 15310-CLs 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 9-17.

Figure 9-17 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 15310-CL 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.

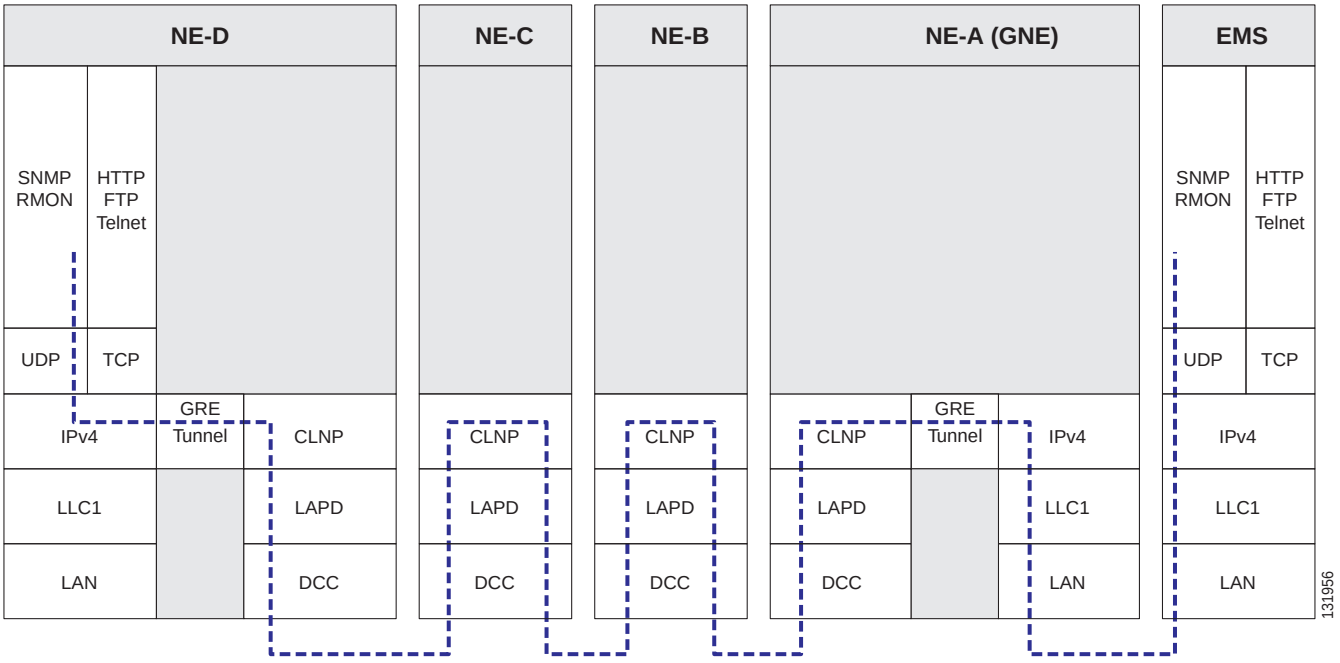
9.7.7 IP-over-CLNS Tunnels

IP-over-CLNS tunnels are used to encapsulate IP for transport across OSI NEs. The ONS 15310-CL 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 9-18 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 9-18 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, see the "Turn Up Node" chapter in the *ONS 15310-CL Procedures Guide*.

Provisioning IP-over-CLNS tunnels on Cisco routers requires the following prerequisite tasks, as well as other OSI provisioning:

- (Required) Enable IS-IS
- (Optional) Enable routing for an area on an interface
- (Optional) Assign multiple area addresses
- (Optional) Configure IS-IS interface parameters
- (Optional) Configure miscellaneous IS-IS parameters

The Cisco IOS commands used to create IP-over-CLNS tunnels (CTunnels) are shown in Table 9-14.

Table 9-14 IP Over CLNS Tunnel IOS Commands

Step	Step	Purpose
1	Router (config) # **interface ctunnel** *interface-number*	Creates a virtual interface to transport IP over a CLNS tunnel and enters interface configuration mode. The interface number must be unique for each CTunnel interface.
2	Router (config-if # **ctunnel destination** *remote-nsap-address*	Configures the destination parameter for the CTunnel. Specifies the destination NSAP1 address of the CTunnel, where the IP packets are extracted.
3	Router (config-if) # **ip address** *ip-address mask*	Sets the primary or secondary IP address for an interface.

If you are provisioning an IP-over-CLNS tunnel on a Cisco router, always follow procedures provided in the Cisco IOS documentation for the router you are provisioning. For information about ISO CLNS provisioning including IP-over-CLNS tunnels, refer to 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 9-19 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 provisioning on the ONS NE 1:

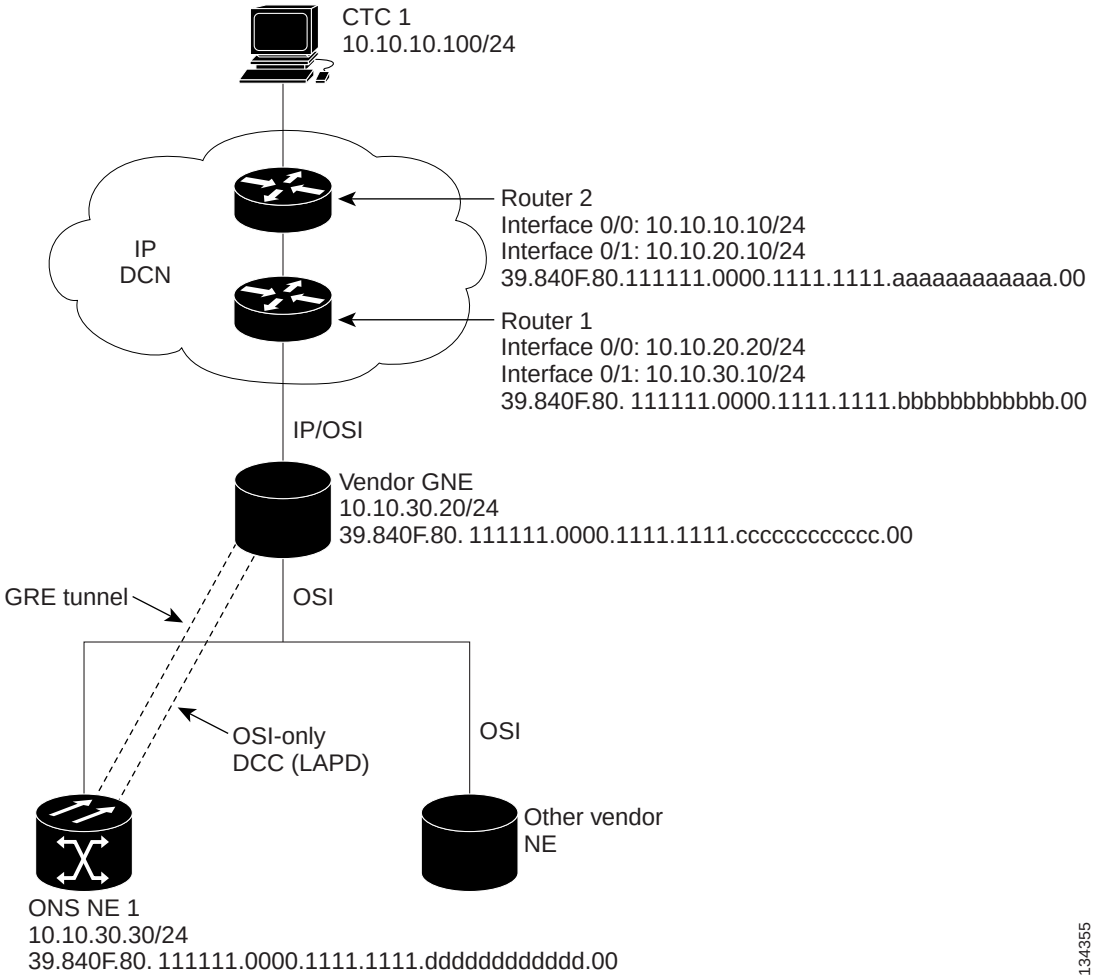
- Destination: 10.10.10.100 (CTC 1)
- Mask: 255.255.255.255 for host route (CTC 1 only), or 255.255.255.0 for subnet route (all CTC computers residing on the 10.10.10.0 subnet)
- NSAP: 39.840F.80.1111.0000.1111.1111.ccccccccccc.00 (other vendor GNE)
- Metric: 110

- Tunnel Type: GRE

IP-over-CLNS tunnel provisioning 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 9-19 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 9-20 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.

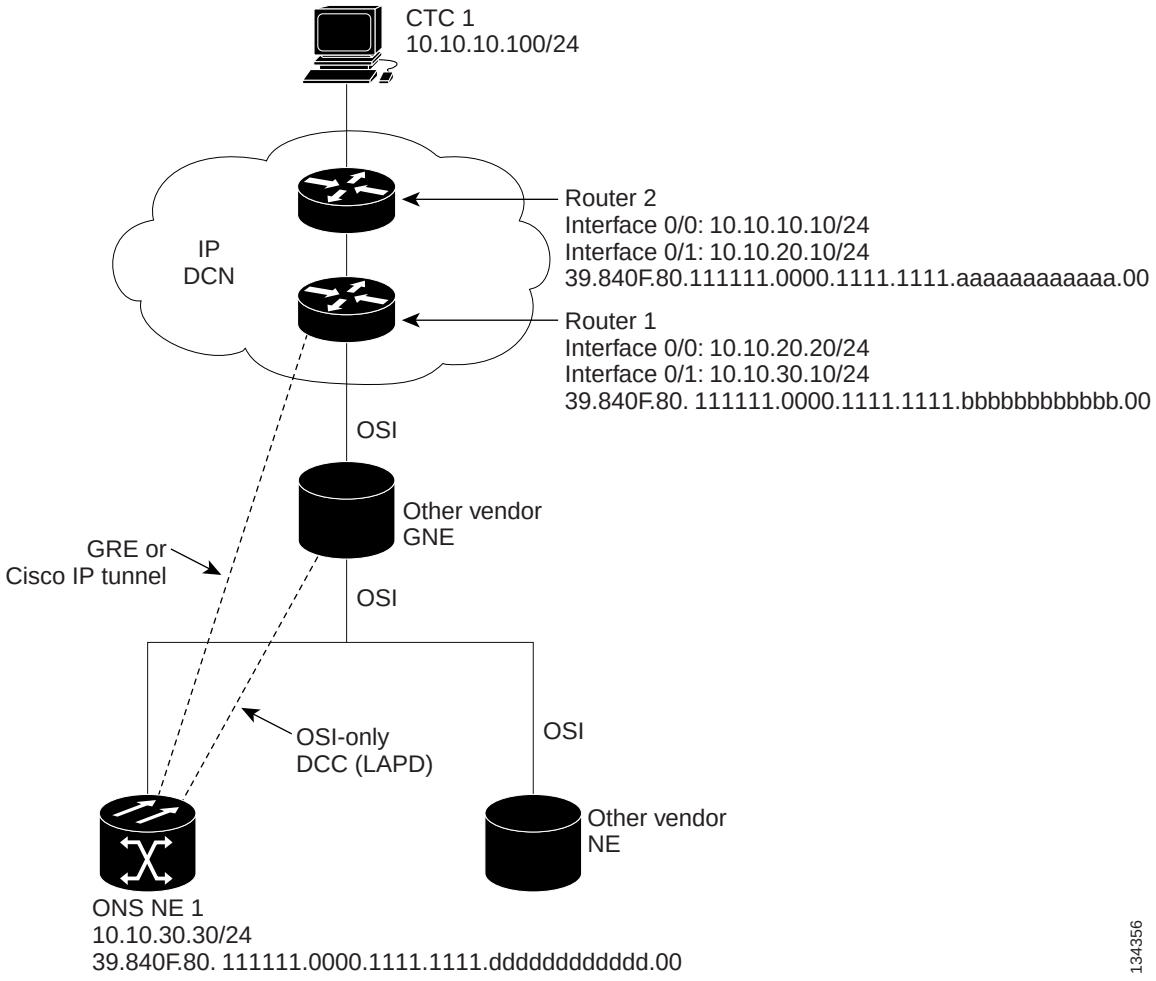
IP-over-CLNS tunnel provisioning on ONS NE 1:

- 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) provisioning on Router 1:

```
ip routing
clns routing
interface ctunnel 102
    ip address 10.10.30.30 255.255.255.0
    ctunnel destination 39.840F.80.1111.0000.1111.1111.dddddddddddd.00
interface Ethernet0/1
    clns router isis
router isis
    net 39.840F.80.1111.0000.1111.1111.bbbbbbbbbbbb.00
```

Figure 9-20 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 9-21 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.

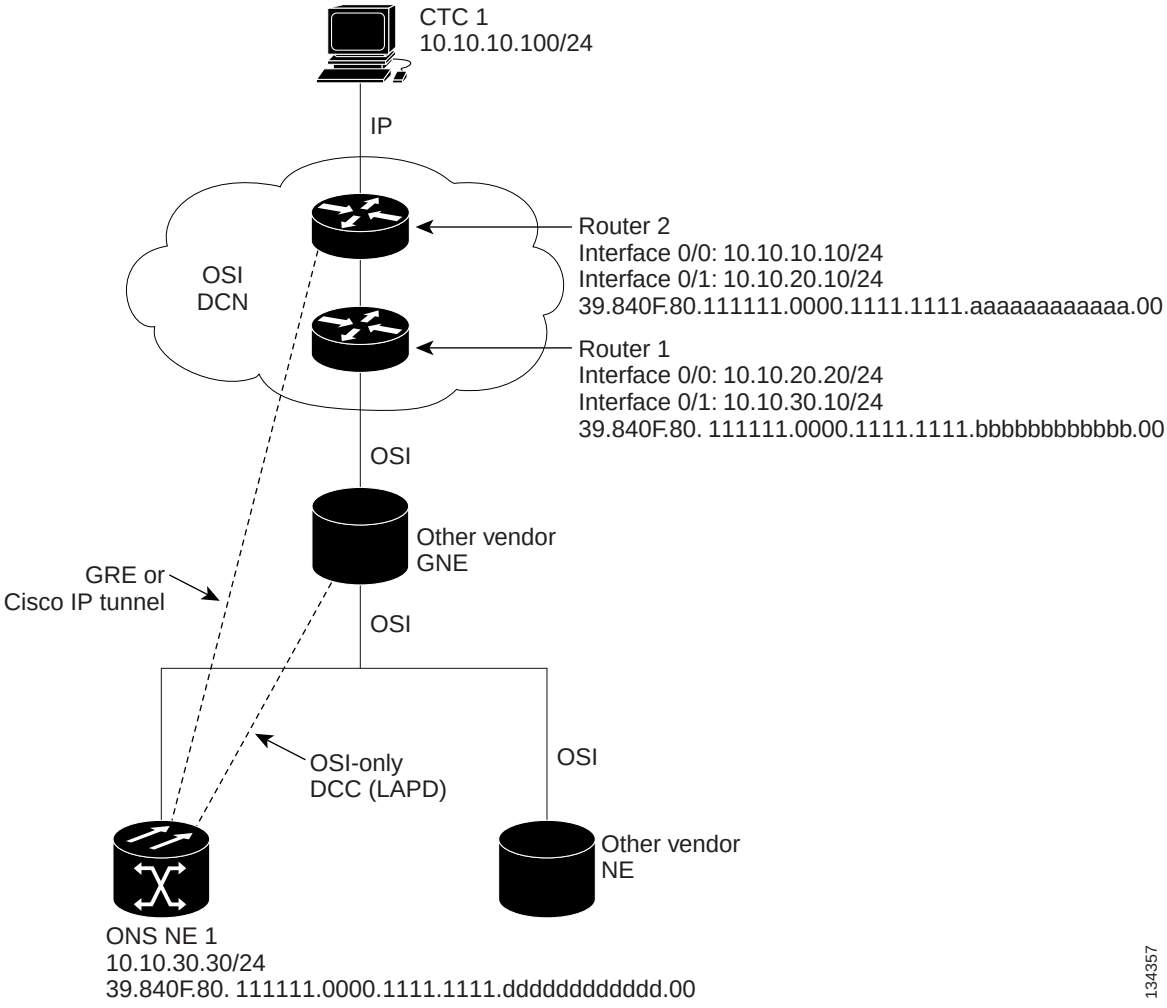
IP-over-CLNS tunnel provisioning on ONS NE 1:

- 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 provisioning on Router 2 (sample Cisco IOS provisioning):

```
ip routing
clns routing
interface ctunnel 102
    ip address 10.10.30.30 255.255.255.0
    ctunnel destination 39.840F.80.1111.0000.1111.1111.dddddddddddd.00
interface Ethernet0/1
    clns router isis
router isis
    net 39.840F.80.1111.0000.1111.1111.aaaaaaaaaaaa.00
```

Figure 9-21 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 15310-CL 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 9-16 shows the OSI actions that are performed from the node view Maintenance tab.

Table 9-16 OSI Actions from the CTC Maintenance Tab

Tab	Actions
OSI > ISIS RIB	View the IS-IS routing table.
OSI > ESIS RIB	View ESs that are attached to ISs.
OSI > TDC	• View the TARP data cache and identify static and dynamic entries. • 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 15310-CL Troubleshooting Guide*. Chapter topics include:

10.1 Overview

Cisco Transport Controller (CTC) detects and reports SONET alarms generated by the Cisco ONS 15310-CL 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 15310-CL Troubleshooting Guide.*

Note ONS 15310-CL alarms can also be monitored and managed through Transaction Language One (TL1) or a network management system (NMS).

10.2 Viewing Alarms

You can use the Alarms tab to view card, node, or network-level alarms. 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.

The Path Width column in the Alarms and Conditions tabs expands upon alarmed object information contained in the access identifier (AID) string (such as “STS-4-1-3”) by giving the number of synchronous transport signals (STSs) contained in the alarmed path. For example, the Path Width will tell you whether a Critical alarm applies to an 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 Alarms tab 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 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 compliments the alarm object notation, which is explained in Table 10-3 on page 10-3.
Sev	Severity level: CR (Critical), MJ (Major), MN (Minor), NA (Not-Alarmed), NR (Not-Reported).
ST	Status: R (raised), C (clear).
SA	When checked, indicates a service-affecting alarm.
Cond	The error message/alarm name. These names are alphabetically defined in the “Alarm Troubleshooting” chapter of the *Cisco ONS 15310-CL Troubleshooting Guide.*
Description	Description of the alarm.
Num	Num (number) is the quantity of alarm messages received and is increments 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

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

STS and VT Alarm Numbering (ONS 15310-CL)	
MON Object (Optical)	**Syntax and Examples**
OC3/OC12 STS	Syntax: STS-<Slot>-<Ppm>-<Port>-<STS> Ranges: STS-{2}-{1-2}-{1}-{1-*n*}[1] Example: STS-2-1-1-6
OC3/OC12 VT	Syntax: VT1-<Slot>-<Ppm>-<Port>-<STS>-<VT Group>-<VT> Ranges: VT1-{2}-{1-2}-{1}-{1-*n*[1]}-{1-7}-{1-4} Example: VT1-2-1-1-6-1-1
EC1 STS	Syntax: STS-<Slot>-<Port>-<STS> Ranges: STS-{2}-{1-3}-{1-*n*}[1] Example: STS-2-1-6
EC1 VT	Syntax: VT1-<Slot>-<Port>-<STS>-<VT Group>-<VT> Ranges: VT1-{2}-{1-3}-{1-*n*}[1]-{1-7}-{1-4} Example: VT1-2-1-6-1-1
TERM Object (Electrical)	**Syntax and Examples**
T1 STS	Syntax: STS-<Slot>-<STS> Ranges: STS-{2}-{1-*n*}[1] Example: STS-2-6
T1 VT	Syntax: VT1-<Slot>-<STS>-VT Group>-<VT> Ranges: VT1-{2}-{1-*n*}[1]-{1-7}-{1-3} Example: VT1-2-6-1-1
T3 STS	Syntax: STS-<Slot>-<Port>-<STS> Ranges: STS-{2}-{1-3}-{1-*n*}[1] Example: STS-2-1-6
T3 VT	VT not supported

1. The maximum number of STSs depends on the rate and size of the STS.

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. But you can set the node to report alarms (and conditions) using the time zone where the node is located by clicking Edit > Preferences, and 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 in 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 in 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 are displayed in the window. If you enable the Filter feature by clicking the Filter tool 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.
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.

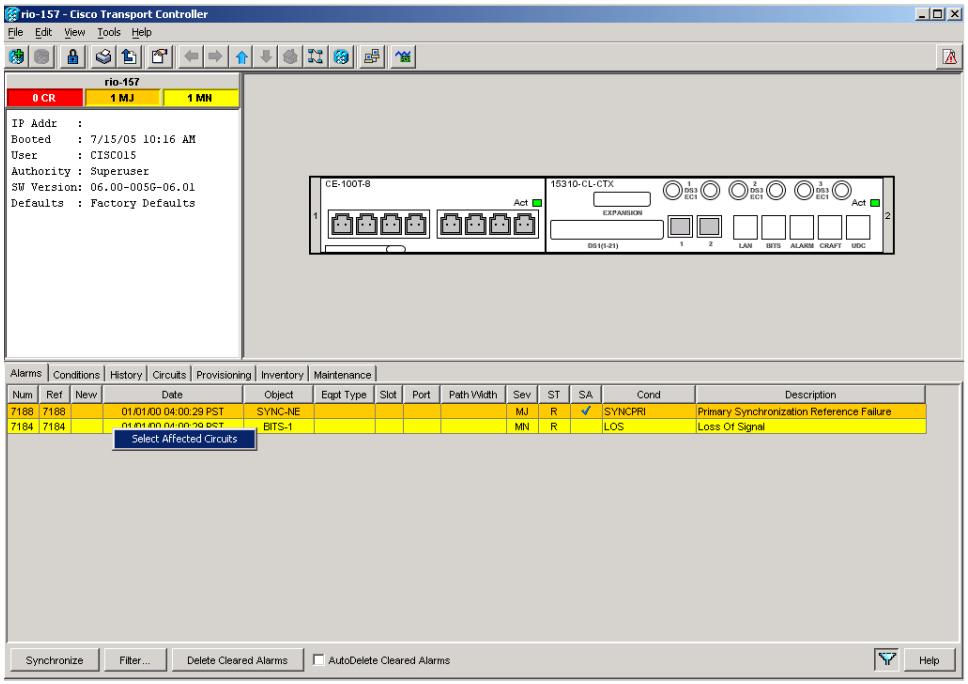
10.2.3 Filtering Alarms

The alarm display can be filtered to prevent the 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

To view which ONS 15310-CL circuits are affected by a specific alarm, right-clicking an alarm in the Alarm window. A shortcut menu appears (Figure 10-1). When you select the Select Affected Circuits option, the Circuits window opens 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 15310-CL 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 15310-CL.

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 15310-CL. 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 15310-CL 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 15310-CL.
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 tool 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 appear. If you click the button while displaying the network view, all conditions for the network (including ONS 15310 nodes and other connected nodes) appear, 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	Indicates a new condition.
Date	Date and time of the condition.
Object	TL1 AID for the condition 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 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: CR (Critical), MJ (Major), MN (Minor), NA (Not-Alarmed), NR (Not-Reported).
SA[1]	Indicates a service-affecting alarm (when checked).
Cond	The error message/alarm name; these names are alphabetically defined in the *Cisco ONS 15310-CL Troubleshooting Guide.*
Description	Description of the condition.
Node	Node where the alarm occurred (appears only in network view).

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

10.2.6.3 Filtering Conditions

The condition display can be filtered to prevent the appearance 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 you log in.

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 port.

The ONS 15310-CL 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 15310-CL discards the oldest events in that category.

Note In the Preference dialog 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, this is the monitored STS or VT object, which is explained in Table 10-3 on page 10-3.
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-view 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.

10.3 Alarm Severities

The ONS 15310-CL 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) with a severity of Not Alarmed (NA) or Not Reported (NR). These severities are reported in the CTC software Alarms, Conditions, and History windows at all levels: network, node, and card.

ONS equipment provides a standard profile named “Default” that lists all alarms and conditions with severity settings based on Telcordia GR-253-CORE and other standards, but users can create their own profiles with different settings for some or all conditions and apply these wherever needed. (See the

"10.4 Alarm Profiles" section on page 10-9 for more information.) For example, in a custom alarm profile, the default severity of a carrier loss (CARLOSS) alarm on an Ethernet port can be changed from Major to Critical.

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 a 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 the alarm might be 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 15310-CL ports, cards, or nodes. A created alarm profile can be applied to any node on the network. Alarm profiles can be saved to a file and imported elsewhere in the network, but the profile must be stored locally on a node before it can be applied to the node, cards, or ports.

CTC can store up to ten active alarm profiles at any time to apply to the node. Custom profiles can take eight of these active profile positions. Two other profiles, Default profile and Inherited profile, are reserved by the 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 is stored as files from elsewhere in the network onto the local PC or server hard drive where CTC resides, you can use 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.

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.

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. For example, 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. Or 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 is raised 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 at the bottom. 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 from 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 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:

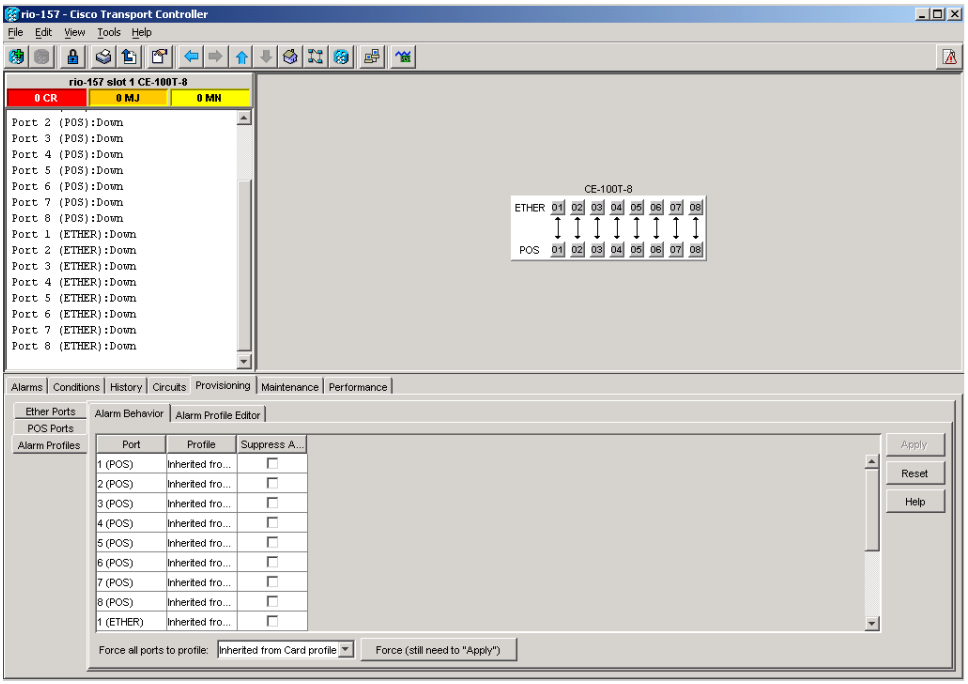
- Hide reference values—Highlights alarms with non-default severities by clearing alarm cells with default severities.
- Hide identical rows—Hides rows of alarms that contain the same severity for each profile.

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 alarm profile applies to all cards in the node except cards that have their own profiles. A card 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 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 CE-100T-8 card alarm profiles.

Figure 10-2 Alarm Profiles for a CE-100T-8 Card



10.5 Alarm Suppression

ONS 15310 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 cleared, but it does not cancel 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 with the 15310-CL ALARM port. However, the alarms are provisioned using the 15310-CL-CTX card view for external sensors such as an open door and flood sensors, temperature sensors, and other environmental conditions. External control outputs on the 15310-CL-CTX card 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.

Provision external alarms in the 15310-CL-CTX card view Provisioning > External Alarms tab and provision controls in the 15310-CL-CTX card view Provisioning > External Controls tab. Up to 32 alarm contact inputs and 8 alarm contact outputs are available with the CTX2500 cards and 15310-CL-CTX cards report some of these alarms.

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

Note If you provision an external alarm to raise when a contact is open, and you have not attached the alarm cable, the alarm will remain raised until the alarm cable is connected.

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

Specifications

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

This appendix contains shelf, card, and small-form factor pluggable (SFP) specifications for the Cisco ONS 15310-CL.

A.1 Shelf Specifications

This section includes hardware and software specifications.

A.1.1 Bandwidth

Total bandwidth: 2.054 Gbps

- Optical: 1.24 Gbps (2 x OC-12)
- Electrical: 188 Mbps
- Expansion: 622 Mbps (OC-12)

A.1.2 Expansion Slot

Total card slots: 1 expansion slot for CE-100T-8 and ML-100T-8 cards. A blank card (15310-EXP-FILLER) can also be plugged into the expansion slot.

A.1.3 Internal Cards

- Common Control, Timing, Cross-Connect Customer-Located (15310-CL-CTX)
- Interconnect card
- Connector expansion card

A.1.4 15310-CL-CTX

- Optical Ports
  - Two user upgradeable and hot swappable SFPs with SONET interface support
  - Support for multirate SFPs (155.520 Mbps and 622.080 Mbps)
  - Support for operating the two optical facilities at different line rates in unprotected facility mode (non 1+1 Automatic Protection Switching [APS] operation)
- T1 Ports
  - Supports GR499-compliant 1.544 Mbps (T1) interface
  - Performance monitoring is provided via the interface to allow validation of signal quality.
  - Any outgoing T1 signal can be retimed to eliminate accumulated jitter and wander at the point of egress from a synchronous network.
  - Any incoming T1 signal from the transport element can also be used as a timing source.
- T3/EC1 Ports
  - Supports GR499-compliant 44.736 Mbps (DS3) interfaces or EC1.
  - Performance monitoring is provided via the interface to allow validation of signal quality. Each port can be provisioned in any combination of T3 or EC1.
- BITS
  - Supports one BITS input and one BITS output
  - The BITS I/O ports support a 100-ohm termination for external 1.544 Mbps DS1 timing signals.
- Alarm
  - The alarm system provides three alarm inputs and two contacts for alarm outputs.
- LAN
  - Supports a 10/100 Mbps Ethernet interface for CTC/TL1 provisioning.
- Craft Interface
  - An RS-232 Craft interface is provided and is used for TL1 provisioning.
  - The Craft interface is set to 9600 baud, no parity, and 1 stop bit by default.
- 64 kbps User Data Channel (UDC) Digital Interface
  - The 64 kbps Digital Interface provides a digital input and output.
  - Any F1 byte that is accessible on the system is interfaced at the UDC connector.
  - The UDC provides a simplex interface. Protection for UDC overhead channel(s) follows interface line protection for traffic.
  - The UDC can be enabled or disabled through the management interfaces. The default state is disabled.
  - The UDC supports a 64 kbps serial interface adaptation function to overhead byte F1.
  - The physical interface is defined in G.703 as a 120-ohm, twisted pair connection. The jitter specification is defined in G.823.
  - The UDC supports a serial port interface adaptation function to overhead bytes F1. This is an RS-232 interface capable of 9.6, 19.2, 38.4, and 56 kbps operation. The rate is selectable through the management interface. The default is 56 kbps with no parity and 1 stop bit.

A.1.5 Configurations

- Two-fiber path protection
- 1+1 protection
- Path protected mesh network (PPMN)
- Add-drop multiplexer
- Point-to-point terminal mode

A.1.6 Cisco Transport Controller

- 10/100 Base-T
- 15310-CL-CTX access: RJ-45 connector

A.1.7 TL1 Craft Interface

- Speed: 9600 baud, no parity, 1 stop bit
- 15310-CL-CTX: RS-232 with RJ-45 type connector

A.1.8 LEDs

Table A-1 describes the possible LED colors and their significance.

Table A-1 LED Description

LED	Color
FAIL	Red for system failure or during initialization
ALARM	Red (Major and Critical) Amber (Minor)
PWR	Green (AC source present or both DC sources present) Amber (one DC source present)
SYNC	Green (primary and secondary reference sync) Amber (only one reference) Red (loss of both references)

A.1.9 Alarm Interface

- Visual: Critical (red LED), Major (red LED), Minor (amber LED)
- Three alarm inputs and two alarm contacts, all on the same RJ-45 connector (ALARM port)

A.1.10 DS1 Interface

- 21 DS-1 (1.544 Mbps) ports
- Connector: LFH96 (100-ohm balanced)
- Any two ports can be used as primary and secondary timing sources
- A DS01 output can be retimed to system clock on a per-port basis

The DS-1 connector pin assignments are shown in Table A-2.

Table A-2 DS-1 Connector Pin Assignments

Pin	Transmit Cable Signal Connection	Conductor Color	Pin	Receive Cable Signal Connection	Conductor Color
1	TX11-	blue-black	49	TX21-	blue-violet
2	TX11+	black-blue	50	TX21+	violet-blue
3	TX10-	gray-red	51	TX20-	gray-yellow
4	TX10+	red-gray	52	TX20+	yellow-gray
5	TX9-	brown-red	53	TX19-	brown-yellow
6	TX9+	red-brown	54	TX19+	yellow-brown
7	TX8-	green-red	55	TX18-	green-yellow
8	TX8+	red-green	56	TX18+	yellow-green
9	TX7-	orange-red	57	TX17-	orange-yellow
10	TX7+	red-orange	58	TX17+	yellow-orange
11	TX6-	blue-red	59	TX16-	blue-yellow
12	TX6+	red-blue	60	TX16+	yellow-blue
13	TX5-	gray-white	61	TX15-	gray-black
14	TX5+	white-gray	62	TX15+	black-gray
15	TX4-	brown-white	63	TX14-	brown-black
16	TX4+	white-brown	64	TX14+	black-brown
17	TX3-	green-white	65	TX13-	green-black
18	TX3+	white-green	66	TX13+	black-green
19	TX2-	orange-white	67	TX12-	orange-black
20	TX2+	white-orange	68	TX12+	black-orange
21	TX1-	blue-white	69	Unused	—
22	TX1+	white-blue	70	Unused	—
23	Unused	—	71	Unused	—
24	Unused	—	72	Unused	—
25	RX11-	blue-black	73	RX21-	blue-violet
26	RX11+	black-blue	74	RX21+	violet-blue
27	RX10-	gray-red	75	RX20-	gray-yellow

Table A-2 DS-1 Connector Pin Assignments (continued)

Pin	Transmit Cable Signal Connection	Conductor Color	Pin	Receive Cable Signal Connection	Conductor Color
28	RX10+	red-gray	76	RX20+	yellow-gray
29	RX9-	brown-red	77	RX19-	brown-yellow
30	RX9+	red-brown	78	RX19+	yellow-brown
31	RX8-	green-red	79	RX18-	green-yellow
32	RX8+	red-green	80	RX18+	yellow-green
33	RX7-	orange-red	81	RX17-	orange-yellow
34	RX7+	red-orange	82	RX17+	yellow-orange
35	RX6-	blue-red	83	RX16-	blue-yellow
36	RX6+	red-blue	84	RX16+	yellow-blue
37	RX5-	gray-white	85	RX15-	gray-black
38	RX5+	white-gray	86	RX15+	black-gray
39	RX4-	brown-white	87	RX14-	brown-black
40	RX4+	white-brown	88	RX14+	black-brown
41	RX3-	green-white	89	RX13-	green-black
42	RX3+	white-green	90	RX13+	black-green
43	RX2-	orange-white	91	RX12-	orange-black
44	RX2+	white-orange	92	RX12+	black-orange
45	RX1-	blue-white	93	Unused	—
46	RX1+	white-blue	94	Unused	—
47	Unused	—	95	Unused	—
48	Unused	—	96	Unused	—

A.1.11 DS3/EC1 Interface

- Three DS3 (44.736 Mbps)/EC1 (51.84 Mbps) ports
- Connector: 75-ohm mini-BNC connector
- Ports can be any combination of DS-3 and EC-1

A.1.12 Nonvolatile Memory

- 128 MB, Compact Flash card

A.1.13 BITS Interface

- 1 DS-1 BITS input

- 1 derived DS-1 output

A.1.14 RJ-45 Connector Pin Assignments

Table A-3 details wiring for the BITS.

Table A-3 RJ-45 Connector Pin Assignments

Pin	Connector					
	BITS	ALARM	CRAFT	UDC		LAN
				RS232 Mode	64K Mode	
1	BITS Output +	Alarm Contact Port 1 +	RTS	NC	TX +	TX +
2	BITS Output –	Alarm Contact Port 1 –	DTR	DTR	TX –	TX –
3	BITS Input +	Alarm Contact Port 2 +	TXD	TXD	RX +	RX +
4	—	Alarm Contact Port 2 –	GND	GND	GND	NC
5	—	Alarm Input Port 1	GND	GND	GND	NC
6	BITS Input –	Alarm Input Port 2	RXD	RXD	RX –	RX –
7	—	Alarm Input Port 3	DSR	NC	NC	NC
8	—	Alarm Input Common	CTS	NC	NC	NC

A.1.15 Pushbuttons

- Lamp test: when momentarily pushed, lights all LEDs on the ONS 15310-CL front panel. If an LED has more than one color, all the colors will be cycled when the lamp test button is pushed.

Note Another use for the lamp test button is to reset the CTC password to its default value (otbu+1). To reset the password, press the lamp test button for at least five seconds, release it for a maximum of five seconds, then press it again for at least five seconds. After the button is released, the default password is set.

- System reset: when pressed, performs a soft reset (does not impact traffic).

A.1.16 System Timing

- +/- 20 ppm SONET Minimum Clock (SMC) free-running internal clock
- Maintains SMC holdover (+/- 4.6 ppm for first 24 hours) in the event of reference frequency loss
- Timing reference: External BITS, line optical port, any DS-1 clock, and internal clock

A.1.17 Power Specifications

- Input power: -48 VDC (dual DC power supply model) or 100/240 VAC (AC power model)
- Maximum power consumption

  - DC chassis with no expansion board: 60W
  - DC chassis with expansion board: 115W
  - AC chassis with no expansion board: 70W
  - AC chassis with expansion board: 140W
- Power requirements: –42 to –56 VDC or 100/240 VAC (+/- 10%)
- Power terminals: Three-prong male locking connector for DC power supply model or three-prong male AC connector for AC power model

Note An ONS 15310-CL that uses DC power is classified as DC-I (DC Isolated). This means that the DC return (RET) conductor at the DC power input connector is not bonded to the chassis frame ground.

A.1.18 Environmental Specifications

- Operating Temperature: 0 to +55 degrees Celsius (32 to +131 degrees Fahrenheit) for AC chassis; -40 to +65 degrees Celsius (-40 to +149 degrees Fahrenheit) for dual DC chassis.
- Operating Humidity: 5 to 95%, non-condensing

A.1.19 Shelf Dimensions

- Height: 1 Rack Unit (RU), 1.75 inches (4.45 cm)
- Width:
  - 19.0 inches (48.3 cm)
  - 23.0 inches (58.4 cm) including rackmount brackets
- Depth:
  - 15.0 inches (38.1 cm) sheet metal only
  - 15.8 inches (40.2) including mini-BNC and DC inlet connectors
- Weight:
  - 11.5 lb. empty
  - 12.5 lb. maximum (line card installed)

A.2 Card Specifications

This section provides specifications for the cards that can be installed in the 15310-CL expansion slot: CE-100T-8, ML-100T-8, and Filler cards. For compliance information, refer to the Cisco Optical Transport Products Safety and Compliance Information document.

A.2.1 CE-100T-8 and ML-100T-8 Cards

- Environmental
  - Operating temperature

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

- Operating humidity: 5 to 95%, noncondensing
- Power consumption: 1.10A, 35W

- Dimensions
  - Height: 176 mm (6.93 in.)
  - Width: 34.29 mm (1.35 in.)
  - Depth: 238.25 mm (9.38 in.)
  - Weight (not including clam shell): 0.499 kg (1.1 lb)

A.2.2 Filler Card

- Environmental
  - Operating temperature

    I-Temp: -40 to +65 degrees Celsius (-40 to 149 degrees Fahrenheit)
  - Operating humidity: 5 to 95%, noncondensing
- Dimensions
  - Height: 176 mm (6.93 in.)
  - Width: 34.29 mm (1.35 in.)
  - Depth: 238.25 mm (9.38 in.)
  - Card weight (not including clam shell): 0.45 kg (0.9 lb)

A.3 SFP Specifications

Table A-4 lists specifications for available small-form factor pluggables (SFPs) that can be used with the 15310-CL-CTX card. The 15310-CL-CTX card does not have a faceplate because it is located inside the chassis; therefore, the two SFP slots are located on the 15310-CL faceplate, just to the left of the LAN port.

Table A-4 SFP Specifications

SFP Product ID	Interface	Transmitter Output Power Min/Max (dBm)	Receiver Input Power Min/Max (dBm)
ONS-SI-155-L1	OC-3	–5.0 to 0	–34 to –10
ONS-SI-155-L2	OC-3	–5.0 to 0	–34 to –10
ONS-SI-155-I1	OC-3	–15 to –8.0	–28 to –8
ONS-SI-622-L1	OC-12	–3.0 to 2.0	–28 to –8
ONS-SI-622-L2	OC-12	–3.0 to 2.0	–28 to –8
ONS-SI-622-I1	OC-12/OC-3	–15 to –8.0	–28 to –8

Table A-5 provides cabling specifications for the 15310-CL-CTX single-mode fiber (SMF) SFPs. The ports of the listed SFPs have LC-type connectors.

Table A-5 Single-Mode Fiber SFP Port Cabling Specifications

SFP Product ID	Wavelength[1]	Fiber Type	Cable Distance
ONS-SI-155-L1 Long Reach	1310 nm	9 micro SMF	50 km (31.07 miles)
ONS-SI-155-L2 Long Reach	1550 nm	9 micro SMF	100 km (62.15 miles)
ONS-SI-155-I1 Intermediate Reach	1310 nm	9 micro SMF	21 km (13.05 miles)
ONS-SI-622-L1 Long Reach	1310 nm	9 micro SMF	42 km (26.10 miles)
ONS-SI-622-L2 Long Reach	1550 nm	9 micro SMF	85 km (52.82 miles)
ONS-SI-622-I1 Intermediate Reach	1310 nm	9 micro SMF	21 km (13.05 miles)

1. Typical loss on a 1310 nm wavelength SMF is .6 dB/km.

Administrative and Service States

This appendix describes the administrative and service states for Cisco ONS 15310-CL cards, ports, and cross-connects. For circuit state information, see Chapter 7, "Circuits and Tunnels." Software Release 6.0 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 15310-CL.

Table B-1 ONS 15310-CL 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 15310-CL.

Table B-2 ONS 15310-CL 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 CTC Conditions tab or by using the 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.
OOG	(Out of Group) The virtual concatenated (VCAT) member cross-connect is not used to carry VCAT group traffic. This state is used to put a member circuit out of the group and to stop sending traffic. OOS-MA,OOG only applies to the cross-connects on an end node where VCAT resides. The cross-connects on intermediate nodes are in the OOS-MA,MT service state.
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 15310-CL. See Table B-2 on page 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 15310-CL Administrative States

Administrative State (PST,SST)	Definition
IS	Puts the entity in-service.
IS,AINS	Puts the entity in automatic in-service.
OOS,DSBLD	Removes the entity from service and disables it.
OOS,MT	Removes the entity from service for maintenance.
OOS,OOG	(VCAT circuits only) Removes a VCAT member cross-connect from service and from the group of members.

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 15310-CL 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

Table B-4 ONS 15310-CL Card Service State Transitions (continued)

Current Service State	Action	Next Service State
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
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.	OOS-MA,MT
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

Table B-4 ONS 15310-CL Card Service State Transitions (continued)

Current Service State	Action	Next Service State
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
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 port or cross-connect removes the entity from the system. The deleted entity does not transition to another service state.

Table B-5 ONS 15310-CL 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 OOS-MA,DSBLD & OOG for a VCAT cross-connect
	Put the port or cross-connect in the IS,AINS administrative state.	OOS-AU,AINS
	Put the VCAT cross-connect in the OOS,OOG administrative state.	OOS-MA,MT & OOG
	Alarm/condition is raised.	OOS-AU,FLT OOS-AU,FLT & OOG for a VCAT cross-connect
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 OOS-MA,DSBLD & OOG for a VCAT cross-connect
	Put the VCAT cross-connect in the OOS,OOG administrative state.	OOS-MA,MT and OOG
	Alarm/condition is raised.	OOS-AU,AINS & FLT OOS-AU,AINS & FLT & OOG for a VCAT cross-connect
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
	Put the VCAT cross-connect in the OOS,OOG administrative state.	OOS-AUMA,FLT & MT & OOG

Table B-5 ONS 15310-CL Port and Cross-Connect Service State Transitions (continued)

Current Service State	Action	Next Service State
OOS-AU,AINS & FLT & OOG	Alarm/condition is cleared.	OOS-AU,AINS or OOS-MA,MT • If an In Group member is IS-NR or OOS-AU,AINS, the member transitions to OOS-AU,AINS. • If an In Group member is OOS-MA,MT, the member transitions to OOS-MA,MT.
	Put the VCAT cross-connect in the IS administrative state.	OOS-AU,FLT & OOG
	Put the VCAT cross-connect in the OOS,DSBLD administrative state.	OOS-MA,DSBLD & OOG
	Put the VCAT cross-connect in the OOS,MT administrative state.	OOS-AUMA,FLT & MT & OOG
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 OOS-MA,DSBLD & OOG for a VCAT cross-connect
	Put the port or cross-connect in the OOS,MT administrative state	OOS-AUMA,FLT & MT
	Put the VCAT cross-connect in the OOS,OOG administrative state.	OOS-AUMA,FLT & MT & OOG
OOS-AU,FLT & OOG	Alarm/condition is cleared.	IS-NR or OOS-MA,MT • If an In Group member is IS-NR or OOS-AU,AINS, the member transitions to IS-NR. • If an In Group member is OOS-MA,MT, the member transitions to OOS-MA,MT
	Put the VCAT cross-connect in the IS,AINS administrative state.	OOS-AU,AINS & FLT & OOG
	Put the VCAT cross-connect in the OOS,DSBLD administrative state.	OOS-MA,DSBLD & OOG
	Put the VCAT cross-connect in the OOS,MT administrative state.	OOS-AUMA,FLT & MT & OOG

Table B-5 ONS 15310-CL Port and Cross-Connect Service State Transitions (continued)

Current Service State	Action	Next Service State
OOS-AUMA,FLT & LPBK & MT	Release the loopback.	OOS-AUMA,FLT & MT
	Alarm/condition is cleared.	OOS-MA,LPBK & MT
OOS-AUMA,FLT & LPBK & MT & OOG	Release the loopback.	OOS-AUMA,FLT & MT & OOG
	Alarm/condition is cleared.	OOS-MT,MT & OOG
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 OOS-MA,DSBLD & OOG for a VCAT cross-connect
	Put the port or cross-connect in a loopback.	OOS-AUMA,FLT & LPBK & MT
	Put the VCAT cross-connect in the OOS,OOG administrative state.	OOS-AUMA,FLT & MT & OOG
OOS-AUMA,FLT & MT & OOG	Alarm/condition is cleared.	OOS-MA,MT & OOG
	Put the VCAT cross-connect in the IS administrative state. **Note** VCAT In Group members are in the OOS-AU,FLT or IS-NR service state.	OOS-AU,FLT & OOG
	Put the VCAT cross-connect in the IS,AINS administrative state. **Note** VCAT In Group members are in the OOS-AU,AINS & FLT or IS-NR service state.	OOS-AU,AINS & FLT & OOG
	Put the VCAT cross-connect in the OOS,DSBLD administrative state.	OOS-MA,DSBLD & OOG
	Put the VCAT cross-connect in the OOS,MT administrative state. **Note** VCAT In Group members are in the OOS-MA,FLT & MT service state.	OOS-MA,FLT & MT
	Operate a loopback.	OOS-MA,FLT & LPBK & MT & OOG

Table B-5 ONS 15310-CL 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.	OOS-MA,MT
	Put the VCAT cross-connect in the OOS,OOG administrative state.	OOS-MA,MT & OOG
	Put the VCAT cross-connect in the OOS,OOG administrative state.	OOS-MA,MT & OOG
OOS-MA,LPBK & MT	Release the loopback. **Note** While in OOS-MA,LPBK & MT, both Cisco Transport Controller (CTC) and Transaction Language One (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-AUMA,FLT & LPBK & MT & OOG for a VCAT cross-connect
OOS-MA,LPBK & MT & OOG	Alarm/condition is raised.	OOS-AUMA,FLT & LPBK & MT & OOG

Table B-5 ONS 15310-CL Port and Cross-Connect Service State Transitions (continued)

Current Service State	Action	Next Service State
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 OOS-MA,DSBLD & OOG for a VCAT cross-connect
	Put the port or cross-connect in a loopback.	OOS-MA,LPBK & MT
	Put the VCAT cross-connect in the OOS,OOG administrative state.	OOS-MA,MT & OOG
	Alarm/condition is raised.	OOS-AUMA,FLT & MT OOS-AUMA,FLT & MT & OOG for a VCAT cross-connect
OOG-MA,MT & OOG	Alarm/condition is raised.	OOS-AUMA,FLT & MT & OOG

Network Element Defaults

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

This appendix describes the factory-configured (default) network element (NE) settings for the Cisco ONS 15310-CL. It includes descriptions of card default settings and node default settings. For procedures for importing, exporting and editing the settings, refer to the “Maintain the Node” chapter of the *Cisco ONS 15310-CL 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 Port Settings” chapter of the *Cisco ONS 15310-CL Procedure Guide*. To change node settings, refer to the “Change Node Settings” chapter of the *Cisco ONS 15310-CL Procedure Guide*.

C.1 Network Element Defaults Description

The NE defaults are preinstalled on each Cisco ONS 15310-CL 15310-CL-CTX card. They also ship as a file called 15310-defaults.txt on the Cisco Transport Controller (CTC) software CD in case you want to import the defaults onto existing 15310-CL-CTX cards. The NE defaults include card-level, CTC, and node-level defaults.

Changes to card provisioning made manually using procedures in the “Change Card Settings” chapter of the *Cisco ONS 15310-CL 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, or 1+1 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 15310-CL common control and data cards, including:

- Soak Time—*All 15310-CL-CTX ports and CE-100T-8 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—*15310-CL-CTX DS-1 ports*. Defines the DS-1 transmission coding type that is used.
- Line Length—*15310-CL-CTX DS-1, DS-3, and EC-1 ports*. Defines the distance (in feet) from the backplane connection to the next termination point.
- Line Type—*15310-CL-CTX DS-1 and DS-3 ports*. Defines the type of framing used.
- Port State—*All 15310-CL-CTX ports and data 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—*15310-CL-CTX DS1, DS3, EC1, and OC-N ports*. Defines the signal fail (SF) bit error rate (BER).
- SD BER Level—*15310-CL-CTX DS1, DS3, EC1, and OC-N ports*. Defines the signal degrade (SD) BER.
- ALS Mode—*15310-CL-CTX OC-N ports*. Sets the automatic laser shutdown (ALS) feature to one of four available states (disabled, auto restart, manual restart, manual restart for test).
- ALS Recovery Interval—*15310-CL-CTX OC-N ports*. Sets the automatic laser shutdown recovery time interval.
- ALS Recovery Pulse Width—*15310-CL-CTX OC-N ports*. Sets the automatic laser shutdown recovery pulse signal width.
- PJ Sts Mon—*15310-CL-CTX EC-1 and OC-N ports*. Sets the STS that will be used for pointer justification (PJ). If set to 0, no STS is monitored.
- STS IPPM Enabled—*15310-CL-CTX OC-N ports*. 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—*15310-CL-CTX OC-N and DS1 ports*. Sends a do not use (DUS) message on the S1 byte when enabled.
- Far End Inhibit Loopback—*15310-CL-CTX DS-3 ports*. Enables the 15310-CL-CTX card to inhibit loopbacks on the far end.
- PM Threshold Settings—*All 15310-CL-CTX ports*. 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 Port Settings" chapter in the *Cisco ONS 15310-CL Procedure Guide*.

Note For more information about the PM parameters, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15310-CL Troubleshooting Guide*.

C.2.1 15310-CL-CTX Card Default Settings

Table C-1 lists the 15310-CL-CTX card default settings.

Table C-1 15310-CL-CTX Card Default Settings

Default Name	Default Value	Default Domain
CTX.Broadband.portAssignment	DS3-PORT	UNASSIGNED, DS3-PORT, EC1-PORT
CTX.DS1-PORT.config.AINSSoakTime	08:00 (hours:mins)	00:00, 00:15, 00:30 .. 48:00
CTX.DS1-PORT.config.LineCoding	AMI	B8ZS, AMI
CTX.DS1-PORT.config.LineLength	0 - 131 ft	0 - 131 ft, 132 - 262 ft, 263 - 393 ft, 394 - 524 ft, 525 - 655 ft
CTX.DS1-PORT.config.LineType	D4	ESF, D4, UNFRAMED
CTX.DS1-PORT.config.RetimingEnabled	FALSE	TRUE, FALSE
CTX.DS1-PORT.config.SDBER	1E-7	1E-5, 1E-6, 1E-7, 1E-8, 1E-9
CTX.DS1-PORT.config.SendAISOnFacilityLoopback	TRUE	TRUE, FALSE
CTX.DS1-PORT.config.SendAISOnTerminalLoopback	TRUE	TRUE, FALSE
CTX.DS1-PORT.config.SendDoNotUse	FALSE	TRUE, FALSE
CTX.DS1-PORT.config.SFBER	1E-4	1E-3, 1E-4, 1E-5
CTX.DS1-PORT.config.State	IS,AINS	IS, OOS,DSBLD, OOS,MT, IS,AINS
CTX.DS1-PORT.config.SyncMsgIn	FALSE	FALSE, TRUE
CTX.DS1-PORT.pmthresholds.line.farend.15min.ES	65 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.line.farend.1day.ES	648 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.line.nearend.15min.CV	13340 (BPV count)	0–1388700
CTX.DS1-PORT.pmthresholds.line.nearend.15min.ES	65 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.line.nearend.15min.LOSS	10 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.line.nearend.15min.SES	10 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.line.nearend.1day.CV	133400 (BPV count)	0–133315200
CTX.DS1-PORT.pmthresholds.line.nearend.1day.ES	648 (seconds)	0–86400

Table C-1 15310-CL-CTX Card Default Settings (continued)

Default Name	Default Value	Default Domain
CTX.DS1-PORT.pmthresholds.line.nearend.1day.LOSS	10 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.line.nearend.1day.SES	100 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.path.farend.15min.CSS	25 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.path.farend.15min.CV	13296 (BIP count)	0–287100
CTX.DS1-PORT.pmthresholds.path.farend.15min.ES	65 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.path.farend.15min.ESA	25 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.path.farend.15min.ESB	25 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.path.farend.15min.SEFS	25 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.path.farend.15min.SES	10 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.path.farend.15min.UAS	10 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.path.farend.1day.CSS	25 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.path.farend.1day.CV	132960 (BIP count)	0–27561600
CTX.DS1-PORT.pmthresholds.path.farend.1day.ES	648 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.path.farend.1day.ESA	25 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.path.farend.1day.ESB	25 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.path.farend.1day.SEFS	25 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.path.farend.1day.SES	100 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.path.farend.1day.UAS	10 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.path.nearend.15min.AISS	10 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.path.nearend.15min.CV	13296 (BIP count)	0–287100
CTX.DS1-PORT.pmthresholds.path.nearend.15min.ES	65 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.path.nearend.15min.FC	10 (count)	0–72
CTX.DS1-PORT.pmthresholds.path.nearend.15min.SAS	2 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.path.nearend.15min.SES	10 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.path.nearend.15min.UAS	10 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.path.nearend.1day.AISS	10 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.path.nearend.1day.CV	132960 (BIP count)	0–27561600
CTX.DS1-PORT.pmthresholds.path.nearend.1day.ES	648 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.path.nearend.1day.FC	40 (count)	0–6912
CTX.DS1-PORT.pmthresholds.path.nearend.1day.SAS	17 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.path.nearend.1day.SES	100 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.path.nearend.1day.UAS	10 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.sts.farend.15min.CV	15 (B3 count)	0–2160000
CTX.DS1-PORT.pmthresholds.sts.farend.15min.ES	12 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.sts.farend.15min.FC	10 (count)	0–72
CTX.DS1-PORT.pmthresholds.sts.farend.15min.SES	3 (seconds)	0–900

Table C-1 15310-CL-CTX Card Default Settings (continued)

Default Name	Default Value	Default Domain
CTX.DS1-PORT.pmthresholds.sts.farend.15min.UAS	10 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.sts.farend.1day.CV	125 (B3 count)	0–207360000
CTX.DS1-PORT.pmthresholds.sts.farend.1day.ES	100 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.sts.farend.1day.FC	40 (count)	0–6912
CTX.DS1-PORT.pmthresholds.sts.farend.1day.SES	7 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.sts.farend.1day.UAS	10 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.sts.nearend.15min.CV	15 (B3 count)	0–2160000
CTX.DS1-PORT.pmthresholds.sts.nearend.15min.ES	12 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.sts.nearend.15min.FC	10 (count)	0–72
CTX.DS1-PORT.pmthresholds.sts.nearend.15min.SES	3 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.sts.nearend.15min.UAS	10 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.sts.nearend.1day.CV	125 (B3 count)	0–207360000
CTX.DS1-PORT.pmthresholds.sts.nearend.1day.ES	100 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.sts.nearend.1day.FC	40 (count)	0–6912
CTX.DS1-PORT.pmthresholds.sts.nearend.1day.SES	7 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.sts.nearend.1day.UAS	10 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.vt.farend.15min.CV	15 (BIP8 count)	0–2160000
CTX.DS1-PORT.pmthresholds.vt.farend.15min.ES	12 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.vt.farend.15min.SES	3 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.vt.farend.15min.UAS	10 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.vt.farend.1day.CV	125 (BIP8 count)	0–207360000
CTX.DS1-PORT.pmthresholds.vt.farend.1day.ES	100 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.vt.farend.1day.SES	7 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.vt.farend.1day.UAS	10 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.vt.nearend.15min.CV	15 (BIP8 count)	0–2160000
CTX.DS1-PORT.pmthresholds.vt.nearend.15min.ES	12 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.vt.nearend.15min.SES	3 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.vt.nearend.15min.UAS	10 (seconds)	0–900
CTX.DS1-PORT.pmthresholds.vt.nearend.1day.CV	125 (BIP8 count)	0–207360000
CTX.DS1-PORT.pmthresholds.vt.nearend.1day.ES	100 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.vt.nearend.1day.SES	7 (seconds)	0–86400
CTX.DS1-PORT.pmthresholds.vt.nearend.1day.UAS	10 (seconds)	0–86400
CTX.DS3-PORT.config.AINSSoakTime	08:00 (hours:mins)	00:00, 00:15, 00:30 .. 48:00
CTX.DS3-PORT.config.FeInhibitLpbk	FALSE	TRUE, FALSE
CTX.DS3-PORT.config.LineLength	0 - 225 ft	0 - 225 ft, 226 - 450 ft

Table C-1 15310-CL-CTX Card Default Settings (continued)

Default Name	Default Value	Default Domain
CTX.DS3-PORT.config.LineType	M13	UNFRAMED, M13, C BIT, AUTO PROVISION FMT
CTX.DS3-PORT.config.SDBER	1E-7	1E-5, 1E-6, 1E-7, 1E-8, 1E-9
CTX.DS3-PORT.config.SendAISOnFacilityLoopback	TRUE	TRUE, FALSE
CTX.DS3-PORT.config.SendAISOnTerminalLoopback	TRUE	TRUE, FALSE
CTX.DS3-PORT.config.SFBER	1E-4	1E-3, 1E-4, 1E-5
CTX.DS3-PORT.config.State	IS,AINS	IS, OOS,DSBLD, OOS,MT, IS,AINS
CTX.DS3-PORT.pmthresholds.cpbitpath.farend.15min.AISS	10 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.cpbitpath.farend.15min.CV	382 (BIP count)	0–287100
CTX.DS3-PORT.pmthresholds.cpbitpath.farend.15min.ES	25 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.cpbitpath.farend.15min.SAS	2 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.cpbitpath.farend.15min.SES	4 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.cpbitpath.farend.15min.UAS	10 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.cpbitpath.farend.1day.AISS	10 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.cpbitpath.farend.1day.CV	3820 (BIP count)	0–27561600
CTX.DS3-PORT.pmthresholds.cpbitpath.farend.1day.ES	250 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.cpbitpath.farend.1day.SAS	8 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.cpbitpath.farend.1day.SES	40 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.cpbitpath.farend.1day.UAS	10 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.cpbitpath.nearend.15min.AISS	10 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.cpbitpath.nearend.15min.CV	382 (BIP count)	0–287100
CTX.DS3-PORT.pmthresholds.cpbitpath.nearend.15min.ES	25 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.cpbitpath.nearend.15min.SAS	2 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.cpbitpath.nearend.15min.SES	4 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.cpbitpath.nearend.15min.UAS	10 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.cpbitpath.nearend.1day.AISS	10 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.cpbitpath.nearend.1day.CV	3820 (BIP count)	0–27561600
CTX.DS3-PORT.pmthresholds.cpbitpath.nearend.1day.ES	250 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.cpbitpath.nearend.1day.SAS	8 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.cpbitpath.nearend.1day.SES	40 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.cpbitpath.nearend.1day.UAS	10 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.line.nearend.15min.CV	387 (BPV count)	0–38700
CTX.DS3-PORT.pmthresholds.line.nearend.15min.ES	25 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.line.nearend.15min.LOSS	10 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.line.nearend.15min.SES	4 (seconds)	0–900

Table C-1 15310-CL-CTX Card Default Settings (continued)

Default Name	Default Value	Default Domain
CTX.DS3-PORT.pmthresholds.line.nearend.1day.CV	3865 (BPV count)	0–3715200
CTX.DS3-PORT.pmthresholds.line.nearend.1day.ES	250 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.line.nearend.1day.LOSS	10 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.line.nearend.1day.SES	40 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.pbitpath.nearend.15min.AISS	10 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.pbitpath.nearend.15min.CV	382 (BIP count)	0–287100
CTX.DS3-PORT.pmthresholds.pbitpath.nearend.15min.ES	25 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.pbitpath.nearend.15min.SAS	2 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.pbitpath.nearend.15min.SES	4 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.pbitpath.nearend.15min.UAS	10 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.pbitpath.nearend.1day.AISS	10 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.pbitpath.nearend.1day.CV	3820 (BIP count)	0–27561600
CTX.DS3-PORT.pmthresholds.pbitpath.nearend.1day.ES	250 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.pbitpath.nearend.1day.SAS	8 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.pbitpath.nearend.1day.SES	40 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.pbitpath.nearend.1day.UAS	10 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.sts.farend.15min.CV	15 (G1 count)	0–2160000
CTX.DS3-PORT.pmthresholds.sts.farend.15min.ES	12 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.sts.farend.15min.FC	10 (count)	0–72
CTX.DS3-PORT.pmthresholds.sts.farend.15min.SES	3 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.sts.farend.15min.UAS	10 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.sts.farend.1day.CV	125 (G1 count)	0–207360000
CTX.DS3-PORT.pmthresholds.sts.farend.1day.ES	100 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.sts.farend.1day.FC	40 (count)	0–6912
CTX.DS3-PORT.pmthresholds.sts.farend.1day.SES	7 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.sts.farend.1day.UAS	10 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.sts.nearend.15min.CV	15 (B3 count)	0–2160000
CTX.DS3-PORT.pmthresholds.sts.nearend.15min.ES	12 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.sts.nearend.15min.FC	10 (count)	0–72
CTX.DS3-PORT.pmthresholds.sts.nearend.15min.SES	3 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.sts.nearend.15min.UAS	10 (seconds)	0–900
CTX.DS3-PORT.pmthresholds.sts.nearend.1day.CV	125 (B3 count)	0–207360000
CTX.DS3-PORT.pmthresholds.sts.nearend.1day.ES	100 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.sts.nearend.1day.FC	40 (count)	0–6912
CTX.DS3-PORT.pmthresholds.sts.nearend.1day.SES	7 (seconds)	0–86400
CTX.DS3-PORT.pmthresholds.sts.nearend.1day.UAS	10 (seconds)	0–86400

Table C-1 15310-CL-CTX Card Default Settings (continued)

Default Name	Default Value	Default Domain
CTX.EC1-PORT.config.line.AINSSoakTime	08:00 (hours:mins)	00:00, 00:15, 00:30 .. 48:00
CTX.EC1-PORT.config.line.LineLength	0 - 225 ft	0 - 225 ft, 226 - 450 ft
CTX.EC1-PORT.config.line.PJStsMon#	0 (STS #)	0–1
CTX.EC1-PORT.config.line.SDBER	1E-7	1E-5, 1E-6, 1E-7, 1E-8, 1E-9
CTX.EC1-PORT.config.line.SendAISOnFacilityLoopback	TRUE	TRUE, FALSE
CTX.EC1-PORT.config.line.SendAISOnTerminalLoopback	FALSE	TRUE, FALSE
CTX.EC1-PORT.config.line.SFBER	1E-4	1E-3, 1E-4, 1E-5
CTX.EC1-PORT.config.line.State	IS,AINS	IS, OOS,DSBLD, OOS,MT, IS,AINS
CTX.EC1-PORT.config.sts.IPPMEnabled	FALSE	TRUE, FALSE
CTX.EC1-PORT.pmthresholds.line.farend.15min.CV	1312 (B2 count)	0–137700
CTX.EC1-PORT.pmthresholds.line.farend.15min.ES	87 (seconds)	0–900
CTX.EC1-PORT.pmthresholds.line.farend.15min.FC	10 (count)	0–72
CTX.EC1-PORT.pmthresholds.line.farend.15min.SES	1 (seconds)	0–900
CTX.EC1-PORT.pmthresholds.line.farend.15min.UAS	3 (seconds)	0–900
CTX.EC1-PORT.pmthresholds.line.farend.1day.CV	13120 (B2 count)	0–8850600
CTX.EC1-PORT.pmthresholds.line.farend.1day.ES	864 (seconds)	0–86400
CTX.EC1-PORT.pmthresholds.line.farend.1day.FC	40 (count)	0–72
CTX.EC1-PORT.pmthresholds.line.farend.1day.SES	4 (seconds)	0–86400
CTX.EC1-PORT.pmthresholds.line.farend.1day.UAS	10 (seconds)	0–86400
CTX.EC1-PORT.pmthresholds.line.nearend.15min.CV	1312 (B2 count)	0–137700
CTX.EC1-PORT.pmthresholds.line.nearend.15min.ES	87 (seconds)	0–900
CTX.EC1-PORT.pmthresholds.line.nearend.15min.FC	10 (count)	0–72
CTX.EC1-PORT.pmthresholds.line.nearend.15min.SES	1 (seconds)	0–900
CTX.EC1-PORT.pmthresholds.line.nearend.15min.UAS	3 (seconds)	0–900
CTX.EC1-PORT.pmthresholds.line.nearend.1day.CV	13120 (B2 count)	0–13219200
CTX.EC1-PORT.pmthresholds.line.nearend.1day.ES	864 (seconds)	0–86400
CTX.EC1-PORT.pmthresholds.line.nearend.1day.FC	40 (count)	0–6912
CTX.EC1-PORT.pmthresholds.line.nearend.1day.SES	4 (seconds)	0–86400
CTX.EC1-PORT.pmthresholds.line.nearend.1day.UAS	10 (seconds)	0–86400
CTX.EC1-PORT.pmthresholds.section.nearend.15min.CV	10000 (B1 count)	0–138600
CTX.EC1-PORT.pmthresholds.section.nearend.15min.ES	500 (seconds)	0–900
CTX.EC1-PORT.pmthresholds.section.nearend.15min.SEFS	500 (seconds)	0–900
CTX.EC1-PORT.pmthresholds.section.nearend.15min.SES	500 (seconds)	0–900
CTX.EC1-PORT.pmthresholds.section.nearend.1day.CV	100000 (B1 count)	0–13305600
CTX.EC1-PORT.pmthresholds.section.nearend.1day.ES	5000 (seconds)	0–86400

Table C-1 15310-CL-CTX Card Default Settings (continued)

Default Name	Default Value	Default Domain
CTX.EC1-PORT.pmthresholds.section.nearend.1day.SEFS	5000 (seconds)	0–86400
CTX.EC1-PORT.pmthresholds.section.nearend.1day.SES	5000 (seconds)	0–86400
CTX.EC1-PORT.pmthresholds.sts1.nearend.15min.CV	15 (B3 count)	0–2160000
CTX.EC1-PORT.pmthresholds.sts1.nearend.15min.ES	12 (seconds)	0–900
CTX.EC1-PORT.pmthresholds.sts1.nearend.15min.FC	10 (count)	0–72
CTX.EC1-PORT.pmthresholds.sts1.nearend.15min.NPJC-PDET	60 (count)	0–7200000
CTX.EC1-PORT.pmthresholds.sts1.nearend.15min.NPJC-PGEN	60 (count)	0–7200000
CTX.EC1-PORT.pmthresholds.sts1.nearend.15min.PJCDIFF	60 (count)	0–14400000
CTX.EC1-PORT.pmthresholds.sts1.nearend.15min.PJCS-PDET	100 (seconds)	0–900
CTX.EC1-PORT.pmthresholds.sts1.nearend.15min.PJCS-PGEN	100 (seconds)	0–900
CTX.EC1-PORT.pmthresholds.sts1.nearend.15min.PPJC-PDET	60 (count)	0–7200000
CTX.EC1-PORT.pmthresholds.sts1.nearend.15min.PPJC-PGEN	60 (count)	0–7200000
CTX.EC1-PORT.pmthresholds.sts1.nearend.15min.SES	3 (seconds)	0–900
CTX.EC1-PORT.pmthresholds.sts1.nearend.15min.UAS	10 (seconds)	0–900
CTX.EC1-PORT.pmthresholds.sts1.nearend.1day.CV	125 (B3 count)	0–207360000
CTX.EC1-PORT.pmthresholds.sts1.nearend.1day.ES	100 (seconds)	0–86400
CTX.EC1-PORT.pmthresholds.sts1.nearend.1day.FC	40 (count)	0–6912
CTX.EC1-PORT.pmthresholds.sts1.nearend.1day.NPJC-PDET	5760 (count)	0–691200000
CTX.EC1-PORT.pmthresholds.sts1.nearend.1day.NPJC-PGEN	5760 (count)	0–691200000
CTX.EC1-PORT.pmthresholds.sts1.nearend.1day.PJCDIFF	5760 (count)	0–1382400000
CTX.EC1-PORT.pmthresholds.sts1.nearend.1day.PJCS-PDET	9600 (seconds)	0–86400
CTX.EC1-PORT.pmthresholds.sts1.nearend.1day.PJCS-PGEN	9600 (seconds)	0–86400
CTX.EC1-PORT.pmthresholds.sts1.nearend.1day.PPJC-PDET	5760 (count)	0–691200000
CTX.EC1-PORT.pmthresholds.sts1.nearend.1day.PPJC-PGEN	5760 (count)	0–691200000
CTX.EC1-PORT.pmthresholds.sts1.nearend.1day.SES	7 (seconds)	0–86400
CTX.EC1-PORT.pmthresholds.sts1.nearend.1day.UAS	10 (seconds)	0–86400
CTX.OC12-PORT.config.line.AdminSSMIn	STU	PRS, STU, ST2, TNC, ST3E, ST3, SMC, ST4, DUS, RES
CTX.OC12-PORT.config.line.AINSSoakTime	08:00 (hours:mins)	00:00, 00:15, 00:30 .. 48:00
CTX.OC12-PORT.config.line.AlsMode	Disabled	Disabled, Auto Restart, Manual Restart, Manual Restart for Test

Table C-1 15310-CL-CTX Card Default Settings (continued)

Default Name	Default Value	Default Domain
CTX.OC12-PORT.config.line.AlsRecoveryPulseDuration	2.0 (seconds)	• 2.0, 2.1, 2.2 .. 100.0 when AlsMode is Disabled, Auto Restart, Manual Restart • 80.0, 80.1, 80.2 .. 100.0 when AlsMode is Manual Restart for Test
CTX.OC12-PORT.config.line.AlsRecoveryPulseInterval	100 (seconds)	60–300
CTX.OC12-PORT.config.line.PJStsMon#	0 (STS #)	0–12
CTX.OC12-PORT.config.line.SDBER	1E-7	1E-5, 1E-6, 1E-7, 1E-8, 1E-9
CTX.OC12-PORT.config.line.Send<FF>DoNotUse	FALSE	• FALSE when SendDoNotUse is TRUE • FALSE, TRUE when SendDoNotUse is FALSE
CTX.OC12-PORT.config.line.SendAISOnFacilityLoopback	TRUE	TRUE, FALSE
CTX.OC12-PORT.config.line.SendDoNotUse	FALSE	FALSE, TRUE
CTX.OC12-PORT.config.line.SFBER	1E-4	1E-3, 1E-4, 1E-5
CTX.OC12-PORT.config.line.State	IS,AINS	IS, OOS,DSBLD, OOS,MT, IS,AINS
CTX.OC12-PORT.config.line.SyncMsgIn	TRUE	FALSE, TRUE
CTX.OC12-PORT.config.sts.IPPMEnabled	FALSE	TRUE, FALSE
CTX.OC12-PORT.physicalthresholds.alarm.LBC-HIGH	200 (%)	LBC-LOW, LBC-LOW + 1.0, LBC-LOW + 2.0 .. 255.0
CTX.OC12-PORT.physicalthresholds.alarm.LBC-LOW	20 (%)	0.0, 1.0, 2.0 .. LBC-HIGH
CTX.OC12-PORT.physicalthresholds.alarm.OPR-HIGH	200 (%)	OPR-LOW, OPR-LOW + 1.0, OPR-LOW + 2.0 .. 255.0
CTX.OC12-PORT.physicalthresholds.alarm.OPR-LOW	50 (%)	0.0, 1.0, 2.0 .. OPR-HIGH
CTX.OC12-PORT.physicalthresholds.alarm.OPT-HIGH	120 (%)	OPT-LOW, OPT-LOW + 1.0, OPT-LOW + 2.0 .. 255.0
CTX.OC12-PORT.physicalthresholds.alarm.OPT-LOW	80 (%)	0.0, 1.0, 2.0 .. OPT-HIGH
CTX.OC12-PORT.physicalthresholds.warning.15min.LBC-HIGH	200 (%)	LBC-LOW, LBC-LOW + 1.0, LBC-LOW + 2.0 .. 255.0
CTX.OC12-PORT.physicalthresholds.warning.15min.LBC-LOW	20 (%)	0.0, 1.0, 2.0 .. LBC-HIGH

Table C-1 15310-CL-CTX Card Default Settings (continued)

Default Name	Default Value	Default Domain
CTX.OC12-PORT.physicalthresholds.warning.15min.OPR-HIGH	200 (%)	OPR-LOW, OPR-LOW + 1.0, OPR-LOW + 2.0 .. 255.0
CTX.OC12-PORT.physicalthresholds.warning.15min.OPR-LOW	50 (%)	0.0, 1.0, 2.0 .. OPR-HIGH
CTX.OC12-PORT.physicalthresholds.warning.15min.OPT-HIGH	120 (%)	OPT-LOW, OPT-LOW + 1.0, OPT-LOW + 2.0 .. 255.0
CTX.OC12-PORT.physicalthresholds.warning.15min.OPT-LOW	80 (%)	0.0, 1.0, 2.0 .. OPT-HIGH
CTX.OC12-PORT.physicalthresholds.warning.1day.LBC-HIGH	200 (%)	LBC-LOW, LBC-LOW + 1.0, LBC-LOW + 2.0 .. 255.0
CTX.OC12-PORT.physicalthresholds.warning.1day.LBC-LOW	20 (%)	0.0, 1.0, 2.0 .. LBC-HIGH
CTX.OC12-PORT.physicalthresholds.warning.1day.OPR-HIGH	200 (%)	OPR-LOW, OPR-LOW + 1.0, OPR-LOW + 2.0 .. 255.0
CTX.OC12-PORT.physicalthresholds.warning.1day.OPR-LOW	50 (%)	0.0, 1.0, 2.0 .. OPR-HIGH
CTX.OC12-PORT.physicalthresholds.warning.1day.OPT-HIGH	120 (%)	OPT-LOW, OPT-LOW + 1.0, OPT-LOW + 2.0 .. 255.0
CTX.OC12-PORT.physicalthresholds.warning.1day.OPT-LOW	80 (%)	0.0, 1.0, 2.0 .. OPT-HIGH
CTX.OC12-PORT.pmthresholds.line.farend.15min.CV	5315 (B2 count)	0–552600
CTX.OC12-PORT.pmthresholds.line.farend.15min.ES	87 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.line.farend.15min.FC	10 (count)	0–72
CTX.OC12-PORT.pmthresholds.line.farend.15min.SES	1 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.line.farend.15min.UAS	3 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.line.farend.1day.CV	53150 (B2 count)	0–53049600
CTX.OC12-PORT.pmthresholds.line.farend.1day.ES	864 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.line.farend.1day.FC	40 (count)	0–6912
CTX.OC12-PORT.pmthresholds.line.farend.1day.SES	4 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.line.farend.1day.UAS	10 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.line.nearend.15min.CV	5315 (B2 count)	0–552600
CTX.OC12-PORT.pmthresholds.line.nearend.15min.ES	87 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.line.nearend.15min.FC	10 (count)	0–72
CTX.OC12-PORT.pmthresholds.line.nearend.15min.PSC	1 (count)	0–600
CTX.OC12-PORT.pmthresholds.line.nearend.15min.PSC-W	1 (count)	0–600
CTX.OC12-PORT.pmthresholds.line.nearend.15min.PSD	300 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.line.nearend.15min.PSD-W	300 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.line.nearend.15min.SES	1 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.line.nearend.15min.UAS	3 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.line.nearend.1day.CV	53150 (B2 count)	0–53049600

Table C-1 15310-CL-CTX Card Default Settings (continued)

Default Name	Default Value	Default Domain
CTX.OC12-PORT.pmthresholds.line.nearend.1day.ES	864 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.line.nearend.1day.FC	40 (count)	0–6912
CTX.OC12-PORT.pmthresholds.line.nearend.1day.PSC	5 (count)	0–57600
CTX.OC12-PORT.pmthresholds.line.nearend.1day.PSC-W	5 (count)	0–57600
CTX.OC12-PORT.pmthresholds.line.nearend.1day.PSD	600 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.line.nearend.1day.PSD-W	600 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.line.nearend.1day.SES	4 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.line.nearend.1day.UAS	10 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.section.nearend.15min.CV	10000 (B1 count)	0–553500
CTX.OC12-PORT.pmthresholds.section.nearend.15min.ES	500 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.section.nearend.15min.SEFS	500 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.section.nearend.15min.SES	500 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.section.nearend.1day.CV	100000 (B1 count)	0–53136000
CTX.OC12-PORT.pmthresholds.section.nearend.1day.ES	5000 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.section.nearend.1day.SEFS	5000 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.section.nearend.1day.SES	5000 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.sts1.nearend.15min.CV	15 (B3 count)	0–2160000
CTX.OC12-PORT.pmthresholds.sts1.nearend.15min.ES	12 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.sts1.nearend.15min.FC	10 (count)	0–72
CTX.OC12-PORT.pmthresholds.sts1.nearend.15min.NPJC-PDET	60 (count)	0–7200000
CTX.OC12-PORT.pmthresholds.sts1.nearend.15min.NPJC-PGEN	60 (count)	0–7200000
CTX.OC12-PORT.pmthresholds.sts1.nearend.15min.PJCDIFF	60 (count)	0–14400000
CTX.OC12-PORT.pmthresholds.sts1.nearend.15min.PJCS-PDET	100 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.sts1.nearend.15min.PJCS-PGEN	100 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.sts1.nearend.15min.PPJC-PDET	60 (count)	0–7200000
CTX.OC12-PORT.pmthresholds.sts1.nearend.15min.PPJC-PGEN	60 (count)	0–7200000
CTX.OC12-PORT.pmthresholds.sts1.nearend.15min.SES	3 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.sts1.nearend.15min.UAS	10 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.sts1.nearend.1day.CV	125 (B3 count)	0–207360000
CTX.OC12-PORT.pmthresholds.sts1.nearend.1day.ES	100 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.sts1.nearend.1day.FC	40 (count)	0–6912
CTX.OC12-PORT.pmthresholds.sts1.nearend.1day.NPJC-PDET	5760 (count)	0–691200000
CTX.OC12-PORT.pmthresholds.sts1.nearend.1day.NPJC-PGEN	5760 (count)	0–691200000
CTX.OC12-PORT.pmthresholds.sts1.nearend.1day.PJCDIFF	5760 (count)	0–1382400000
CTX.OC12-PORT.pmthresholds.sts1.nearend.1day.PJCS-PDET	9600 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.sts1.nearend.1day.PJCS-PGEN	9600 (seconds)	0–86400

Table C-1 15310-CL-CTX Card Default Settings (continued)

Default Name	Default Value	Default Domain
CTX.OC12-PORT.pmthresholds.sts1.nearend.1day.PPJC-PDET	5760 (count)	0–691200000
CTX.OC12-PORT.pmthresholds.sts1.nearend.1day.PPJC-PGEN	5760 (count)	0–691200000
CTX.OC12-PORT.pmthresholds.sts1.nearend.1day.SES	7 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.sts1.nearend.1day.UAS	10 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.sts12c.nearend.15min.CV	75 (B3 count)	0–2160000
CTX.OC12-PORT.pmthresholds.sts12c.nearend.15min.ES	60 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.sts12c.nearend.15min.FC	10 (count)	0–72
CTX.OC12-PORT.pmthresholds.sts12c.nearend.15min.NPJC-PDET	60 (count)	0–7200000
CTX.OC12-PORT.pmthresholds.sts12c.nearend.15min.NPJC-PGEN	60 (count)	0–7200000
CTX.OC12-PORT.pmthresholds.sts12c.nearend.15min.PJCDIFF	60 (count)	0–14400000
CTX.OC12-PORT.pmthresholds.sts12c.nearend.15min.PJCS-PDET	100 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.sts12c.nearend.15min.PJCS-PGEN	100 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.sts12c.nearend.15min.PPJC-PDET	60 (count)	0–7200000
CTX.OC12-PORT.pmthresholds.sts12c.nearend.15min.PPJC-PGEN	60 (count)	0–7200000
CTX.OC12-PORT.pmthresholds.sts12c.nearend.15min.SES	3 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.sts12c.nearend.15min.UAS	10 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.sts12c.nearend.1day.CV	750 (B3 count)	0–207360000
CTX.OC12-PORT.pmthresholds.sts12c.nearend.1day.ES	600 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.sts12c.nearend.1day.FC	40 (count)	0–6912
CTX.OC12-PORT.pmthresholds.sts12c.nearend.1day.NPJC-PDET	5760 (count)	0–691200000
CTX.OC12-PORT.pmthresholds.sts12c.nearend.1day.NPJC-PGEN	5760 (count)	0–691200000
CTX.OC12-PORT.pmthresholds.sts12c.nearend.1day.PJCDIFF	5760 (count)	0–1382400000
CTX.OC12-PORT.pmthresholds.sts12c.nearend.1day.PJCS-PDET	9600 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.sts12c.nearend.1day.PJCS-PGEN	9600 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.sts12c.nearend.1day.PPJC-PDET	5760 (count)	0–691200000
CTX.OC12-PORT.pmthresholds.sts12c.nearend.1day.PPJC-PGEN	5760 (count)	0–691200000
CTX.OC12-PORT.pmthresholds.sts12c.nearend.1day.SES	7 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.sts12c.nearend.1day.UAS	10 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.15min.CV	25 (B3 count)	0–2160000
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.15min.ES	20 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.15min.FC	10 (count)	0–72
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.15min.NPJC-PDET	60 (count)	0–7200000
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.15min.NPJC-PGEN	60 (count)	0–7200000
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.15min.PJCDIFF	60 (count)	0–14400000
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.15min.PJCS-PDET	100 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.15min.PJCS-PGEN	100 (seconds)	0–900

Table C-1 15310-CL-CTX Card Default Settings (continued)

Default Name	Default Value	Default Domain
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.15min.PPJC-PDET	60 (count)	0–7200000
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.15min.PPJC-PGEN	60 (count)	0–7200000
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.15min.SES	3 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.15min.UAS	10 (seconds)	0–900
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.1day.CV	250 (B3 count)	0–207360000
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.1day.ES	200 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.1day.FC	40 (count)	0–6912
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.1day.NPJC-PDET	5760 (count)	0–691200000
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.1day.NPJC-PGEN	5760 (count)	0–691200000
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.1day.PJCDIFF	5760 (count)	0–1382400000
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.1day.PJCS-PDET	9600 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.1day.PJCS-PGEN	9600 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.1day.PPJC-PDET	5760 (count)	0–691200000
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.1day.PPJC-PGEN	5760 (count)	0–691200000
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.1day.SES	7 (seconds)	0–86400
CTX.OC12-PORT.pmthresholds.sts3c-9c.nearend.1day.UAS	10 (seconds)	0–86400
CTX.OC3-PORT.config.line.AdminSSMIn	STU	PRS, STU, ST2, TNC, ST3E, ST3, SMC, ST4, DUS, RES
CTX.OC3-PORT.config.line.AINSSoakTime	08:00 (hours:mins)	00:00, 00:15, 00:30 .. 48:00
CTX.OC3-PORT.config.line.AlsMode	Disabled	Disabled, Auto Restart, Manual Restart, Manual Restart for Test
CTX.OC3-PORT.config.line.AlsRecoveryPulseDuration	2.0 (seconds)	• 2.0, 2.1, 2.2 .. 100.0 when AlsMode is Disabled, Auto Restart, Manual Restart • 80.0, 80.1, 80.2 .. 100.0 when AlsMode is Manual Restart for Test
CTX.OC3-PORT.config.line.AlsRecoveryPulseInterval	100 (seconds)	60–300
CTX.OC3-PORT.config.line.PJStsMon#	0 (STS #)	0–3
CTX.OC3-PORT.config.line.SDBER	1E-7	1E-5, 1E-6, 1E-7, 1E-8, 1E-9
CTX.OC3-PORT.config.line.Send<FF>DoNotUse	FALSE	• FALSE when SendDoNotUse is TRUE • FALSE, TRUE when SendDoNotUse is FALSE

Table C-1 15310-CL-CTX Card Default Settings (continued)

Default Name	Default Value	Default Domain
CTX.OC3-PORT.config.line.SendAISOnFacilityLoopback	TRUE	TRUE, FALSE
CTX.OC3-PORT.config.line.SendDoNotUse	FALSE	FALSE, TRUE
CTX.OC3-PORT.config.line.SFBER	1E-4	1E-3, 1E-4, 1E-5
CTX.OC3-PORT.config.line.State	IS,AINS	IS, OOS,DSBLD, OOS,MT, IS,AINS
CTX.OC3-PORT.config.line.SyncMsgIn	TRUE	FALSE, TRUE
CTX.OC3-PORT.config.sts.IPPMEnabled	FALSE	TRUE, FALSE
CTX.OC3-PORT.physicalthresholds.alarm.LBC-HIGH	200 (%)	LBC-LOW, LBC-LOW + 1.0, LBC-LOW + 2.0 .. 255.0
CTX.OC3-PORT.physicalthresholds.alarm.LBC-LOW	20 (%)	0.0, 1.0, 2.0 .. LBC-HIGH
CTX.OC3-PORT.physicalthresholds.alarm.OPR-HIGH	200 (%)	OPR-LOW, OPR-LOW + 1.0, OPR-LOW + 2.0 .. 255.0
CTX.OC3-PORT.physicalthresholds.alarm.OPR-LOW	50 (%)	0.0, 1.0, 2.0 .. OPR-HIGH
CTX.OC3-PORT.physicalthresholds.alarm.OPT-HIGH	120 (%)	OPT-LOW, OPT-LOW + 1.0, OPT-LOW + 2.0 .. 255.0
CTX.OC3-PORT.physicalthresholds.alarm.OPT-LOW	80 (%)	0.0, 1.0, 2.0 .. OPT-HIGH
CTX.OC3-PORT.physicalthresholds.warning.15min.LBC-HIGH	200 (%)	LBC-LOW, LBC-LOW + 1.0, LBC-LOW + 2.0 .. 255.0
CTX.OC3-PORT.physicalthresholds.warning.15min.LBC-LOW	20 (%)	0.0, 1.0, 2.0 .. LBC-HIGH
CTX.OC3-PORT.physicalthresholds.warning.15min.OPR-HIGH	200 (%)	OPR-LOW, OPR-LOW + 1.0, OPR-LOW + 2.0 .. 255.0
CTX.OC3-PORT.physicalthresholds.warning.15min.OPR-LOW	50 (%)	0.0, 1.0, 2.0 .. OPR-HIGH
CTX.OC3-PORT.physicalthresholds.warning.15min.OPT-HIGH	120 (%)	OPT-LOW, OPT-LOW + 1.0, OPT-LOW + 2.0 .. 255.0
CTX.OC3-PORT.physicalthresholds.warning.15min.OPT-LOW	80 (%)	0.0, 1.0, 2.0 .. OPT-HIGH
CTX.OC3-PORT.physicalthresholds.warning.1day.LBC-HIGH	200 (%)	LBC-LOW, LBC-LOW + 1.0, LBC-LOW + 2.0 .. 255.0
CTX.OC3-PORT.physicalthresholds.warning.1day.LBC-LOW	20 (%)	0.0, 1.0, 2.0 .. LBC-HIGH
CTX.OC3-PORT.physicalthresholds.warning.1day.OPR-HIGH	200 (%)	OPR-LOW, OPR-LOW + 1.0, OPR-LOW + 2.0 .. 255.0
CTX.OC3-PORT.physicalthresholds.warning.1day.OPR-LOW	50 (%)	0.0, 1.0, 2.0 .. OPR-HIGH
CTX.OC3-PORT.physicalthresholds.warning.1day.OPT-HIGH	120 (%)	OPT-LOW, OPT-LOW + 1.0, OPT-LOW + 2.0 .. 255.0
CTX.OC3-PORT.physicalthresholds.warning.1day.OPT-LOW	80 (%)	0.0, 1.0, 2.0 .. OPT-HIGH

Table C-1 15310-CL-CTX Card Default Settings (continued)

Default Name	Default Value	Default Domain
CTX.OC3-PORT.pmthresholds.line.farend.15min.CV	1312 (B2 count)	0–137700
CTX.OC3-PORT.pmthresholds.line.farend.15min.ES	87 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.line.farend.15min.FC	10 (count)	0–72
CTX.OC3-PORT.pmthresholds.line.farend.15min.SES	1 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.line.farend.15min.UAS	3 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.line.farend.1day.CV	13120 (B2 count)	0–13219200
CTX.OC3-PORT.pmthresholds.line.farend.1day.ES	864 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.line.farend.1day.FC	40 (count)	0–6912
CTX.OC3-PORT.pmthresholds.line.farend.1day.SES	4 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.line.farend.1day.UAS	10 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.line.nearend.15min.CV	1312 (B2 count)	0–137700
CTX.OC3-PORT.pmthresholds.line.nearend.15min.ES	87 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.line.nearend.15min.FC	10 (count)	0–72
CTX.OC3-PORT.pmthresholds.line.nearend.15min.PSC	1 (count)	0–600
CTX.OC3-PORT.pmthresholds.line.nearend.15min.PSD	300 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.line.nearend.15min.SES	1 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.line.nearend.15min.UAS	3 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.line.nearend.1day.CV	13120 (B2 count)	0–13219200
CTX.OC3-PORT.pmthresholds.line.nearend.1day.ES	864 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.line.nearend.1day.FC	40 (count)	0–6912
CTX.OC3-PORT.pmthresholds.line.nearend.1day.PSC	5 (count)	0–57600
CTX.OC3-PORT.pmthresholds.line.nearend.1day.PSD	600 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.line.nearend.1day.SES	4 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.line.nearend.1day.UAS	10 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.section.nearend.15min.CV	10000 (B1 count)	0–138600
CTX.OC3-PORT.pmthresholds.section.nearend.15min.ES	500 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.section.nearend.15min.SEFS	500 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.section.nearend.15min.SES	500 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.section.nearend.1day.CV	100000 (B1 count)	0–13305600
CTX.OC3-PORT.pmthresholds.section.nearend.1day.ES	5000 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.section.nearend.1day.SEFS	5000 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.section.nearend.1day.SES	5000 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.sts1.nearend.15min.CV	15 (B3 count)	0–2160000
CTX.OC3-PORT.pmthresholds.sts1.nearend.15min.ES	12 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.sts1.nearend.15min.FC	10 (count)	0–72
CTX.OC3-PORT.pmthresholds.sts1.nearend.15min.NPJC-PDET	60 (count)	0–7200000

Table C-1 15310-CL-CTX Card Default Settings (continued)

Default Name	Default Value	Default Domain
CTX.OC3-PORT.pmthresholds.sts1.nearend.15min.NPJC-PGEN	60 (count)	0–7200000
CTX.OC3-PORT.pmthresholds.sts1.nearend.15min.PJCDIFF	60 (count)	0–14400000
CTX.OC3-PORT.pmthresholds.sts1.nearend.15min.PJCS-PDET	100 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.sts1.nearend.15min.PJCS-PGEN	100 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.sts1.nearend.15min.PPJC-PDET	60 (count)	0–7200000
CTX.OC3-PORT.pmthresholds.sts1.nearend.15min.PPJC-PGEN	60 (count)	0–7200000
CTX.OC3-PORT.pmthresholds.sts1.nearend.15min.SES	3 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.sts1.nearend.15min.UAS	10 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.sts1.nearend.1day.CV	125 (B3 count)	0–207360000
CTX.OC3-PORT.pmthresholds.sts1.nearend.1day.ES	100 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.sts1.nearend.1day.FC	40 (count)	0–6912
CTX.OC3-PORT.pmthresholds.sts1.nearend.1day.NPJC-PDET	5760 (count)	0–691200000
CTX.OC3-PORT.pmthresholds.sts1.nearend.1day.NPJC-PGEN	5760 (count)	0–691200000
CTX.OC3-PORT.pmthresholds.sts1.nearend.1day.PJCDIFF	5760 (count)	0–1382400000
CTX.OC3-PORT.pmthresholds.sts1.nearend.1day.PJCS-PDET	9600 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.sts1.nearend.1day.PJCS-PGEN	9600 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.sts1.nearend.1day.PPJC-PDET	5760 (count)	0–691200000
CTX.OC3-PORT.pmthresholds.sts1.nearend.1day.PPJC-PGEN	5760 (count)	0–691200000
CTX.OC3-PORT.pmthresholds.sts1.nearend.1day.SES	7 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.sts1.nearend.1day.UAS	10 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.sts3c.nearend.15min.CV	25 (B3 count)	0–2160000
CTX.OC3-PORT.pmthresholds.sts3c.nearend.15min.ES	20 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.sts3c.nearend.15min.FC	10 (count)	0–72
CTX.OC3-PORT.pmthresholds.sts3c.nearend.15min.NPJC-PDET	60 (count)	0–7200000
CTX.OC3-PORT.pmthresholds.sts3c.nearend.15min.NPJC-PGEN	60 (count)	0–7200000
CTX.OC3-PORT.pmthresholds.sts3c.nearend.15min.PJCDIFF	60 (count)	0–14400000
CTX.OC3-PORT.pmthresholds.sts3c.nearend.15min.PJCS-PDET	100 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.sts3c.nearend.15min.PJCS-PGEN	100 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.sts3c.nearend.15min.PPJC-PDET	60 (count)	0–7200000
CTX.OC3-PORT.pmthresholds.sts3c.nearend.15min.PPJC-PGEN	60 (count)	0–7200000
CTX.OC3-PORT.pmthresholds.sts3c.nearend.15min.SES	3 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.sts3c.nearend.15min.UAS	10 (seconds)	0–900
CTX.OC3-PORT.pmthresholds.sts3c.nearend.1day.CV	250 (B3 count)	0–207360000
CTX.OC3-PORT.pmthresholds.sts3c.nearend.1day.ES	200 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.sts3c.nearend.1day.FC	40 (count)	0–6912
CTX.OC3-PORT.pmthresholds.sts3c.nearend.1day.NPJC-PDET	5760 (count)	0–691200000

Table C-1 15310-CL-CTX Card Default Settings (continued)

Default Name	Default Value	Default Domain
CTX.OC3-PORT.pmthresholds.sts3c.nearend.1day.NPJC-PGEN	5760 (count)	0–691200000
CTX.OC3-PORT.pmthresholds.sts3c.nearend.1day.PJCDIFF	5760 (count)	0–1382400000
CTX.OC3-PORT.pmthresholds.sts3c.nearend.1day.PJCS-PDET	9600 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.sts3c.nearend.1day.PJCS-PGEN	9600 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.sts3c.nearend.1day.PPJC-PDET	5760 (count)	0–691200000
CTX.OC3-PORT.pmthresholds.sts3c.nearend.1day.PPJC-PGEN	5760 (count)	0–691200000
CTX.OC3-PORT.pmthresholds.sts3c.nearend.1day.SES	7 (seconds)	0–86400
CTX.OC3-PORT.pmthresholds.sts3c.nearend.1day.UAS	10 (seconds)	0–86400
CTX.PPM.portAssignment	UNASSIGNED	UNASSIGNED, OC3-PORT, OC12-PORT
CTX.PPM.slotAssignment	UNASSIGNED	UNASSIGNED, PPM (1 Port)
CTX.Wideband.portAssignment	DS1-PORT	DS1-PORT

C.2.2 Ethernet Card Default Settings

Table C-2 lists the CE-100T-8 and ML100T card default settings.

Table C-2 Ethernet Card Default Settings

Default Name	Default Value	Default Domain
CE-100T-8.config.AINSSoakTime	08:00 (hours:mins)	00:00, 00:15, 00:30 .. 48:00
CE-100T-8.config.State	OOS,DSBLD	IS, OOS,DSBLD, OOS,MT, IS,AINS
CE-100T-8.etherPortConfig.802-1Q-VlanCoS	7 (count)	0–7
CE-100T-8.etherPortConfig.IP-ToS	255 (count)	0–255
ML100T.ios.consolePortAccess	TRUE	TRUE, FALSE
ML100T.ios.radiusServerAccess	FALSE	TRUE, FALSE

C.3 Node Default Settings

Table C-3 on page C-19 lists the node-level default settings for the Cisco ONS 15310-CL. Cisco provides user-configurable defaults for each Cisco ONS 15310-CL node, including:

- Insert AIS-V on SDP—Instructs the node to insert AIS-V in each VT whenever the carrying STS crosses the signal degrade path BER threshold.
- SDP BER—Defines the node SD path BER.
- Path Protection settings—Set the threshold level for signal degradation and failure for path protection circuits.
- 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.
- 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 NTP 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.
- 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 LBO settings for BITS1 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 15310-CL Procedure Guide*.

Table C-3 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

Table C-3 Node Default Settings (continued)

Default Name	Default Value	Default Domain
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.RaiseConditionOnEmptySlot	FALSE	TRUE, FALSE
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-4 on page C-24.)
NODE.general.UseDST	TRUE	TRUE, FALSE
NODE.network.general.CtcIpDisplaySuppression	FALSE	TRUE, FALSE
NODE.network.general.GatewaySettings	None	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
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.LDCCISISCost	40	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

Table C-3 Node Default Settings (continued)

Default Name	Default Value	Default Domain
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.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
NODE.security.idleUserTimeout.Superuser	00:15 (hours:mins)	00:00, 00:01, 00:02 .. 16:39
NODE.security.lanAccess.LANAccess (May disconnect CTC from node)	Front Only	No LAN Access, Front Only
NODE.security.lanAccess.RestoreTimeout	5 (minutes)	0–60

Table C-3 Node Default Settings (continued)

Default Name	Default Value	Default Domain
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 • (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
NODE.security.passwordAging.superuser.AgingPeriod	45 (days)	20–90
NODE.security.passwordAging.superuser.WarningPeriod	5 (days)	2–20

Table C-3 Node Default Settings (continued)

Default Name	Default Value	Default Domain
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.ctc.AccountingPort	1813 (port)	0–32767
NODE.security.radiusServer.ctc.AuthenticationPort	1812 (port)	0–32767
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.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.Framing	ESF	ESF, D4
NODE.timing.bits-1.LBO	0-133 (ft)	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.general.Mode	External	External, Line, Mixed

Table C-3 Node Default Settings (continued)

Default Name	Default Value	Default Domain
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-4 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-4 Time Zones

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

Table C-4 Time Zones (continued)

Time Zone (GMT +/- Hours)	Location(s)
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
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

Table C-4 Time Zones (continued)

Time Zone (GMT +/- Hours)	Location(s)
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
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

Table C-4 Time Zones (continued)

Time Zone (GMT +/- Hours)	Location(s)
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-5 lists the CTC-level default settings for the Cisco ONS 15310-CL. Cisco provides the following types of 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-5 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

L

M

N

O

P

R

S

T

U

V

W