Cisco ONS 15600 SDH Procedure Guide

Product and Documentation Release 9.0
January 2010

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

Text Part Number: 78-18399-01

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 15600 SDH Procedure Guide, Release 9.0

CONTENTS

CHAPTER 2

CHAPTER 3

CHAPTER 4

CHAPTER 10

CHAPTER 11

CHAPTER 12

CHAPTER 13

CHAPTER 16

CHAPTER 17

FIGURES

TABLES

PROCEDURES

Install the Bay and Backplane Connections 1-1

Install Cards and Fiber-Optic Cable 2-1

Connect the PC and Log into the GUI 3-1

Turn Up a Node 4-1

Manage Alarms 9-1

Change Card Settings 10-1

Change Node Settings 11-1

Convert Network Configurations 12-1

Add and Remove Nodes 13-1

TASKS

Preface

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

This section provides the following information:

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

Revision History

Date	Notes
November 2008	• Added this Revision History table. • Added two new procedures DLP-F379 Set Up SNMP for a GNE and DLP-F380 Set Up SNMP for a ENE in Chapter 18. • Updated the DLP headings in Chapter 19 with correct numbers. • Added a new procedure "NTP-F249 Create FTP Host" in Chapter 4, Trun Up a Node".
December 2008	• Updated the NTP-F248 procedure title to read as Set Up the ONS 15600 in EMS Secure Access. • Updated the DLP-F416 Disable Proxy Service Using Mozilla Firefox (Windows and UNIX) in Chapter 17, DLPs F200 to F299.
February 2009	Updated a warning statement in the chapter, Install Cards and Fiber-Optic Cable.

Date	Notes
April 2009	Updated the reinitialization tool options in F278 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows) section of Chapter 19, DLPs F200 to F299.
August 2009	Updated the “Add an SNCP Node” procedure in Chapter 13, “Add and Remove Nodes”.
November 2009	Updated the section “NTP-F174 Create a Server Trail” in the chapter “Create Circuits”.
December 2009	Updated the section “NTP-F174 Create a Server Trail” in the chapter “Create Circuits”.
January 2010	Updated the “Add an SNCP Node” procedure in Chapter 13, “Add and Remove Nodes”.

Document Objectives

The procedure guide provides procedures for installation, turn up, provisioning and acceptance of ONS 15600 SDH nodes and ONS 15600 SDH designed networks. It is organized in a Cisco recommended work flow sequence for new installations, in addition to allowing easy access to procedures and tasks associated with adds, moves, and changes for existing installations.

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

Audience

To use this guide 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

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

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

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

Chapter (Director Level)

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

Non-Trouble Procedure (NTP)

Each NTP is a list of steps designed to accomplish a specific task. Follow the steps until the task is complete. For a crafts person requiring more detailed instructions, refer to the Detailed Level Procedure (DLP) specified in the procedure steps.

Note To ensure that users who are not familiar with NTP and DLP acronyms understand the hierarchy within the guide, NTPs are termed "procedures" and DLPs are termed "tasks." Every reference to a procedure includes its NTP number, and every reference to a task includes its DLP number.

Detailed Level Procedure (DLP)

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

Related Documentation

Use this *Cisco ONS 15600 SDH Procedure Guide* in conjunction with the following referenced publications:

- *Cisco ONS 15600 SDH Reference Manual*
  Provides detailed card specifications, hardware and software feature descriptions, network topology information, and network element defaults.
- *Cisco ONS 15600 SDH Troubleshooting Guide*
  Provides alarm descriptions, alarm and general troubleshooting procedures, error messages, and transient conditions.
- *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Command Guide, Release 8.0*
  Provides a full Transaction Language One (TL1) command and autonomous message set including parameters, access identifiers (AIDs), conditions, and modifiers for the Cisco ONS 15454 SDH and Cisco ONS 15600 SDH.
- *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Reference Guide, Release 8.0*
  Provides general information, procedures, and errors for TL1 in the Cisco ONS 15454 SDH and Cisco ONS 15600 SDH.

- *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Command Quick Reference Guide, Release 8.0*
  Provides most commonly used Transaction Language One (TL1) command and autonomous message set including parameters, access identifiers (AIDs), conditions, and modifiers for the Cisco ONS 15454 SDH and Cisco ONS 15600 SDH.
- *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 for Beginners, Release 8.0*
  Provides Transaction Language One (TL1) command and autonomous message set information for novice Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 users.
- *Release Notes for the Cisco ONS 15600 SDH Release 8.0*
  Provides caveats, closed issues, and new feature and functionality information.

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

Document Conventions

This publication uses the following conventions:

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

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

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

Warning **IMPORTANT SAFETY INSTRUCTIONS**

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

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

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

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

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

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

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

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

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

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

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

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

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

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

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

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

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

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

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

SPARA DESSA ANVISNINGAR

FONTOS BIZTONSÁGI ELOÍRÁSOK

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

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

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

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告 重要的安全性说明

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

请保存这些安全性说明

警告 安全上の重要な注意事項

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

これらの注意事項を保管しておいてください。

주의 중요 안전 지침

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

이 지시 사항을 보관하십시오.

Aviso

INSTRUÇÕES IMPORTANTES DE SEGURANÇA

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

GUARDE ESTAS INSTRUÇÕES

Advarsel

VIGTIGE SIKKERHEDSANVISNINGER

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

GEM DISSE ANVISNINGER

تحذير

إرشادات الأمان الهامة

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

قم بحفظ هذه الإرشادات

Upozorenje

VAŽNE SIGURNOSNE NAPOMENE

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

SAČUVAJTE OVE UPUTE

Upozornění

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

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

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

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

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

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

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

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

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie

WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

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

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie

DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY

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

USCHOVAJTE SI TENTO NÁVOD

Obtaining Optical Networking Information

This section contains information that is specific to optical networking products. For information that pertains to all of Cisco, refer to the Obtaining Documentation, Obtaining Support, and Security Guideliens section.

Where to Find Safety and Warning Information

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

Cisco Optical Networking Product Documentation CD-ROM

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

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

CHAPTER 1

Install the Bay and Backplane Connections

This chapter provides procedures for installing the Cisco ONS 15600 SDH. To view a summary of the tools and equipment required for installation, see the "Required Tools and Equipment" section on page 1-2.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs). Perform these procedures in the order they appear.

1. NTP-F108 Unpack and Inspect the ONS 15600 SDH Bay Assembly, page 1-4—Complete this procedure before continuing with the "NTP-F109 Install the Bay Assembly" procedure on page 1-5.
2. NTP-F109 Install the Bay Assembly, page 1-5—Complete this procedure to install the bay assembly.
3. NTP-F110 Install Additional Shelf Assemblies in the Bay (Two People), page 1-6—Complete this procedure to install up to two additional shelf assemblies in a bay.
4. NTP-F111 Open and Remove the Front Door, page 1-7—Complete this procedure to access the equipment before continuing with other procedures in this chapter.
5. NTP-F112 Install Cable Routing Modules and Kick Plates, page 1-9—Complete as needed to remove the existing cable routers and install the cable routing modules (CRMs).
6. NTP-F113 Install the Bay Power and Ground, page 1-10—Complete this procedure before continuing with the "NTP-F114 Remove the Rear Cover" procedure on page 1-11.
7. NTP-F114 Remove the Rear Cover, page 1-11—Complete this procedure before continuing with the "NTP-F115 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections" procedure on page 1-12.
8. NTP-F115 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-12—Complete as needed to set up connections on the backplane.
9. NTP-F116 Replace the Rear Cover, page 1-13—Complete as needed to install the rear cover.
10. NTP-F117 Perform the Bay Installation Acceptance Test, page 1-13—Complete this procedure to determine if you have correctly completed all other procedures in the chapter.

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

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Warning **This unit must be installed in a rack that is secured to the building structure.** Statement 205

Note The ONS 15600 installations are suitable for Network Telecommunication facilities and locations where NEC is applicable.

Required Tools and Equipment

You will need the following tools and equipment to install and test the ONS 15600 SDH.

Included Materials

The ONS 15600 SDH bay ship kit is shipped with the ONS 15600 SDH. The under-floor power kit is an optional item and is used in environments where power is supplied through the floor, rather than overhead. You can also order installation dollies to help you with unloading the bay from the shipping pallet; for information on obtaining the dollies, contact your Cisco sales engineer.

The number in parentheses gives the part number or the quantity of the item included in the package.

- Bay ship kit (53-2141-XX)
  - Bay label
  - Floor template
  - ESD ground strap
  - Rectangular seismic washers (4)
  - *Cisco Optical Transport Products Safety and Compliance Information*
- Under-floor power kit (800-23062-XX) (optional)
  - Screws and washers, #8 x 0.75 inch (19.05 mm) (12)
  - Screws and washers, #8 x 0.375 inch (9.525 mm) (8)
  - Power conduits (2)
  - Cable strain-relief brackets (2)
- Wide CRM kit (53-2181-XX) (optional)
  - Latch catches (2 left and 2 right)
  - Velcro tie-wrap (26)
  - Wide CRMs (2; left and right)
  - 6-32 panhead screws (8; for latch catches)
  - 8-32 panhead screws (10; for wide CRMs)

- Narrow CRM kit (53-2193-01) (optional)
  - Fiber radiuses (2; left and right)
  - Narrow CRMs (2; left and right)
  - 6-32 panhead screws (4; for fiber radiuses)
  - 8-32 panhead screws (6; for narrow CRMs)
- 900-mm kick plate kit (53-2178-01) (optional)
  - Front kick plate
  - Rear kick plate
  - Side kick plates (2)
  - 8-32 flathead screws (18)
- 600-mm kick plate kit (53-2177-XX) (optional)
  - Front kick plate
  - Rear kick plate
  - 8-32 flathead screws (10)

User-Supplied Materials

The following materials and tools are required but are not supplied with the ONS 15600 SDH:

- Power cable, rated for at least 125-A capacity
- Ground cable, rated for at least 125-A capacity
- Marking pen
- Concrete drill
- Listed pressure terminal connectors such as two-hole ring; connectors must be suitable for the chosen cable
- Two-hole power lugs, 0.625-inch (15.875 mm) hole spacing, 0.25-inch (6.35 mm) (2 for grounding, 4 for each shelf), for underfloor-routed power cables (Panduit LCCF2-14AZFW-E)
- #22 or #24 AWG CAT-5e alarm wires
- Straight-through (CAT-5) LAN cables, shielded (if using an external LAN connection)
- Male 15-pin D-sub shielded cable (if using the audible [external] alarms option)
- EIA/TIA-232C shielded cable (9 pin D-sub to 9 pin D-sub) (2)
- 75-ohm coaxial cable (BNC connectors on both ends) (optional)
- Ladder (optional)

Tools Needed

- Wire-wrap tool (suitable for #22 to #28 AWG alarm wires)
- Wire cutters
- Wire strippers
- Crimp tool

- Scissors
- #2 Phillips screwdriver, 6 inches (152.4 mm) long
- 3/4-inch (19.05 mm) socket wrench
- Ratchet
- 6-inch (154.2 mm) (or greater) ratchet extension (optional)
- 3/4-inch (19.05 mm) socket
- 1 1/8-inch (28.575 mm) socket
- 15/16-inch (23.8125 mm) socket
- 7/16-inch (11.1125 mm) nut driver or socket
- 9/64-inch (3.5719 mm) Allen wrench

Test Equipment

- Voltmeter
- Visible laser source
- Optical power meter

NTP-F108 Unpack and Inspect the ONS 15600 SDH Bay Assembly

Purpose	This procedure explains how to unpack the ONS 15600 SDH and verify the contents.
Tools/Equipment	Scissors Phillips screwdriver 3/4-inch (19.05 mm) socket wrench
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Complete the "DLP-F161 Unpack and Verify the Bay Assembly" task on page 16-1.

Step 2 Complete the "DLP-F162 Inspect the Bay Assembly" task on page 16-3.

Step 3 Continue with the "NTP-F109 Install the Bay Assembly" procedure on page 1-5.

Stop. You have completed this procedure.

NTP-F109 Install the Bay Assembly

Purpose	This procedure explains how to install the bay assembly at the site.
Tools/Equipment	Ratchet 6-inch (154.2 mm) or greater ratchet extension (optional) 1 1/8-inch (28.575 mm) socket 15/16-inch (23.8125 mm) socket Rectangular seismic washers (4) (53-2141-XX) 5/8-inch (15.88-mm) floor anchor bolts (4)
Prerequisite Procedures	NTP-F108 Unpack and Inspect the ONS 15600 SDH Bay Assembly, page 1-4
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

⚠ **Warning** **This unit must be installed in a rack that is secured to the building structure.** Statement 205

⚠ **Warning** **To prevent airflow restriction, allow at least 24 inches (60 cm) of clearance around the ventilation openings.** Statement 1076

⚠ **Warning** **To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of:**
122°F (50°C). Statement 1047

Step 1 Complete the "DLP-F248 Drill Holes to Anchor and Provide Access to the Bay Assembly" task on page 17-41.

Step 2 Complete the "DLP-F163 Install the Dollies onto the Bay Assembly" task on page 16-3.

Step 3 Complete the "DLP-F164 Install the Bay Assembly" task on page 16-6.

Step 4 Continue with the "NTP-F111 Open and Remove the Front Door" procedure on page 1-7.

Stop. You have completed this procedure.

NTP-F110 Install Additional Shelf Assemblies in the Bay (Two People)

Purpose	This procedure explains how to install a second or third shelf assembly in a previously-installed bay assembly. Due to the weight of the shelf assembly, this procedure requires two people to install a shelf assembly.
Tools/Equipment	Ratchet 6-inch (or greater) ratchet extension (optional) 1 1/8-inch (28.575 mm) socket 15/16-inch (23.8125 mm) socket Rectangular seismic washers (4) (53-2141-XX) 5/8-inch floor anchor bolts (4)
Prerequisite Procedures	NTP-F109 Install the Bay Assembly, page 1-5
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **This unit must be installed in a rack that is secured to the building structure.** Statement 205

Warning **To prevent airflow restriction, allow at least 24 inches (60 cm) of clearance around the ventilation openings.** Statement 1076

Warning **To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of:**
122°F (50°C). Statement 1047

Step 1 Remove the plastic front and rear covers.

Step 2 Slide the shelf assembly into position. (Need more detail as to how this works.)

Step 3 At the rear of the shelf assembly, locate the clear plastic covers over the bus bars. There are four plastic covers on each side of the shelf.

Step 4 Remove the nuts, and use a Phillips screwdriver to remove the screws that attach the clear plastic covers to the bus bars.

Step 5 Attach the shelf assembly to the bus bars.

Step 6 Connect the shelf assembly power cable to the PDU.

Step 7 Connect the green ground wires, which were preinstalled, to the node.

Step 8 Continue with the "NTP-F111 Open and Remove the Front Door" procedure on page 1-7.

Stop. You have completed this procedure.

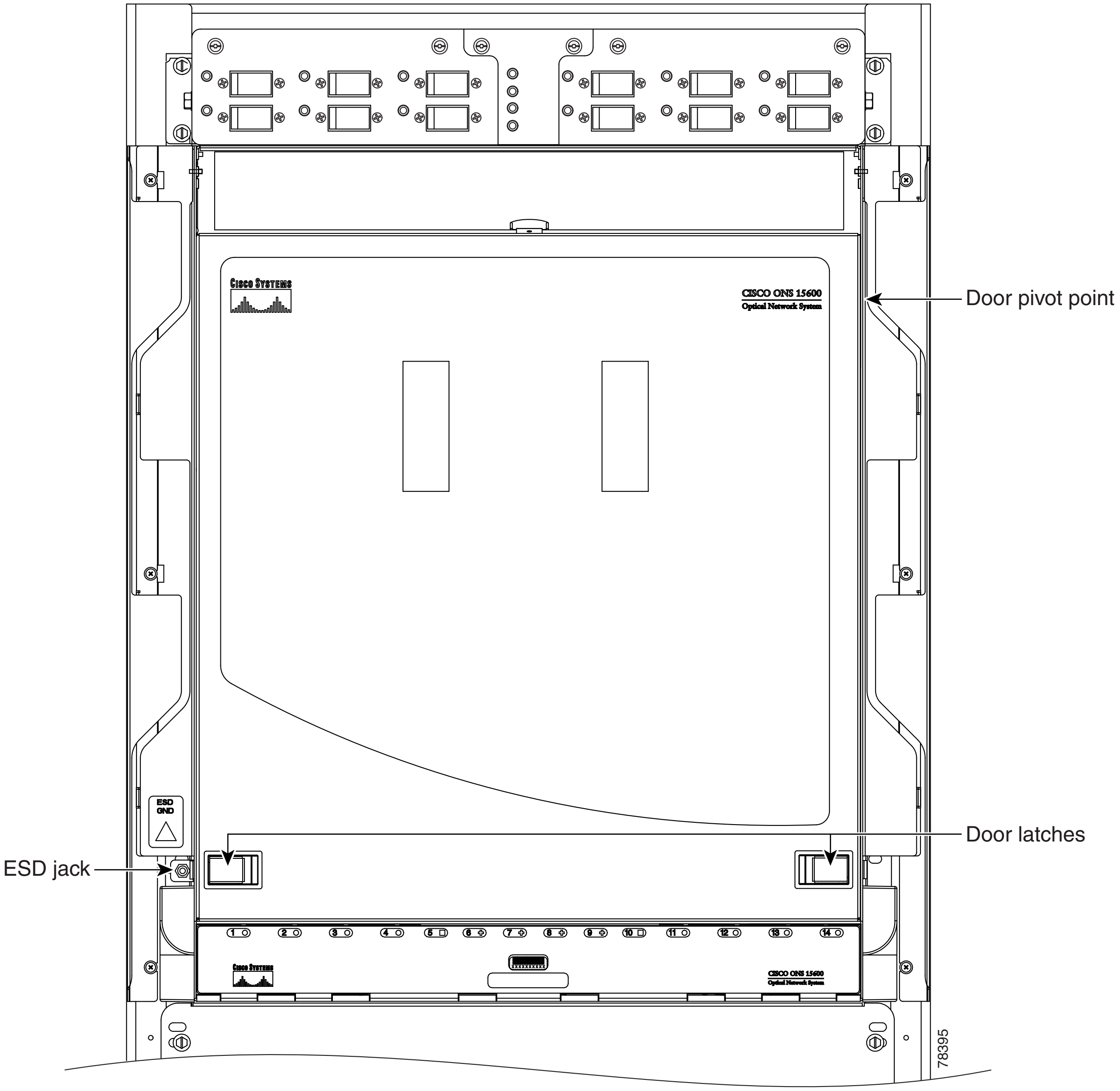
NTP-F111 Open and Remove the Front Door

Purpose	This procedure explains how to open and remove the front door to access the ONS 15600 SDH shelf, including the card cage area and fan trays.
Tools/Equipment	None
Prerequisite Procedures	NTP-F109 Install the Bay Assembly, page 1-5
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note The ONS 15600 SDH has an ESD plug input and is shipped with an ESD wrist strap. One ESD plug input is located on the outside edge of the shelf on the left-hand side, and the other is located at the bottom rear of the shelf. It is labeled "ESD." Always wear an ESD wrist strap and connect the strap to the ESD plug when working on the ONS 15600 SDH.

Step 1 Locate the latches on the bottom left and right sides of the door (Figure 1-1).

Figure 1-1 ONS 15600 SDH Front Door



Step 2 Pull each latch outward to release them.

Step 3 Swing the door up to open it.

Step 4 Lift the door off its hinge pins and remove it. Set the door aside so you can reinstall it after you complete Chapter 2, “Install Cards and Fiber-Optic Cable.”

Step 5 If you want to install CRMs, continue with the “NTP-F112 Install Cable Routing Modules and Kick Plates” procedure on page 1-9. If CRMs are already installed, continue with the “NTP-F113 Install the Bay Power and Ground” procedure on page 1-10.

Stop. You have completed this procedure.

NTP-F112 Install Cable Routing Modules and Kick Plates

Purpose	This procedure explains how to install narrow CRMs or, if necessary, remove any previously installed narrow CRMs and install the wide CRMs.
Tools/Equipment	Screwdriver Retaining screws 900-mm kick plates (53-2178-01) Wide cable routing module (CRM) kit (53-2181-XX) (optional): • Latch catches (2 left and 2 right) • Velcro tie-wrap (26) • Wide CRMs (2 left and 2 right) • 6-32 panhead screws (8; for latch catches) • 8-32 panhead screws (10; for wide CRMs) Narrow CRM kit (53-2193-01) (optional): • Fiber radiuses (2; left and right) • Narrow CRMs (2; left and right) • 6-32 panhead screws (4; for fiber radiuses) • 8-32 panhead screws (6; for narrow CRMs)
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note To accommodate the CRMs, the bay must have 150 millimeters (6 inches) of open space on either side (900-mm [35.4-inch] footprint).

Note Two people are required to perform this procedure.

Step 1 If you want to install narrow CRMs, complete the "DLP-F276 Install the Narrow CRMs" task on page 17-67.

Step 2 If you need to remove narrow CRMs (vertical fiber routers) so you can install wide CRMs, complete the "DLP-F257 Remove the Narrow CRMs" task on page 17-50.

Step 3 If you want to install wide CRMS and have 600-mm (23.6-in.) kick plates installed, complete the "DLP-F258 Replace the Existing 600-mm Kick Plates with 900-mm Kick Plates" task on page 17-52.

Step 4 If you want to install the wide CRMs, complete the "DLP-F277 Install the Wide CRMs" task on page 17-67.

Step 5 Continue with the "NTP-F113 Install the Bay Power and Ground" procedure on page 1-10.

Stop. You have completed this procedure.

NTP-F113 Install the Bay Power and Ground

Purpose	This procedure explains how to install power feeds, and ground the ONS 15600 SDH.
Tools/Equipment	7/16-inch (11.1125 mm) nut driver or socket 9/64-inch (3.5719 mm) Allen wrench Power cable, rated for at least 125-A capacity Ground cable, rated for at least 125-A capacity Listed pressure terminal connectors such as ring and fork types; connectors must be suitable for the chosen cable Wire cutters Wire strippers Crimp tool Screwdriver Nuts (4) Two-hole power lugs, 0.625-inch hole spacing; 0.25-inch bolt holes (Panduit LCCF2-14AZFW-E) (for underfloor-routed power cables) (16) Under-floor power kit (800-23062-XX) (optional): • Screws (#8 x 0.75 inch) and washers (12) • Screws (#8 x 0.375 inch) and washers (8) • Power conduits (2) • Cable strain-relief brackets (2)
Prerequisite Procedures	NTP-F109 Install the Bay Assembly, page 1-5 NTP-F111 Open and Remove the Front Door, page 1-7
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

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

Warning **Before connecting or disconnecting ground or power wires to the chassis, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.** Statement 140

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

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

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

Caution Always use the supplied ESD wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into either the ESD jack located on the lower-left outside edge of the bay assembly, or the other ESD jack located at the bottom rear of the shelf.

Step 1 Complete the "DLP-F165 Connect the Office Ground to the ONS 15600 SDH" task on page 16-7.

Step 2 Complete the "DLP-F279 Connect the PDU Ground Cables to the PDU" task on page 17-71.

Step 3 If isolated logic ground is required at this site, complete the "DLP-F280 Install Isolated Logic Ground" task on page 17-72.

Step 4 Complete the "DLP-F167 Connect Office Power to the ONS 15600 SDH Bay" task on page 16-10.

Step 5 If the site is in a raised-floor environment with underfloor power, complete the optional "DLP-F168 Route and Terminate Raised-Floor Power Cables" task on page 16-12.

Step 6 Complete the "DLP-F169 Verify Office Power" task on page 16-14.

Step 7 Complete the "DLP-F299 Verify Fan Operation" task on page 17-88.

Step 8 Continue with the "NTP-F115 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections" procedure on page 1-12.

Stop. You have completed this procedure.

NTP-F114 Remove the Rear Cover

Purpose	This procedure removes the rear cover to provide access to the customer access panel (CAP or CAP2).
Tools/Equipment	None
Prerequisite Procedures	NTP-F109 Install the Bay Assembly, page 1-5
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Partially unscrew the retaining screws that hold the plastic cover in place.

Step 2 Grasp the cover on each side and slide it to the left so it is free of the key holes.

Step 3 Pull the cover away from the bay.

Step 4 Continue with the "NTP-F115 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections" procedure on page 1-12.

Stop. You have completed this procedure.

NTP-F115 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections

Purpose	This procedure explains how to install alarm, timing, LAN, and craft wires.
Tools/Equipment	Wire-wrap tool (suitable for #22 to #28 AWG alarm wires) #22 or #24 AWG alarm wires
Prerequisite Procedures	NTP-F113 Install the Bay Power and Ground, page 1-10
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

⚠ **Caution** This equipment is suitable for intrabuilding wiring only.

Step 1 Complete the "DLP-F392 Install Alarm Wires on the CAP/CAP2" task on page 18-108 as necessary. Alarm wires are necessary to create external alarms and controls.

Step 2 Complete the "DLP-F170 Install T1 (100 Ohm) Timing Connections on the CAP/CAP2" task on page 16-15 if you are using a 100-ohm T1 building integrated timing supply (BITS) timing source.

Step 3 Complete the "DLP-F171 Install LAN Cables on the CAP/CAP2" task on page 16-16 as needed. LAN cables (or the LAN port on the Timing and Shelf Controller [TSC] card) are necessary to create an external LAN connection.

Step 4 Complete the "DLP-F172 Install the TL1 Craft Interface Cable" task on page 16-16 as needed. Craft cables (or the RJ-45 port on the TSC) are required to access TL1.

⚠ **Caution** Always use the supplied ESD wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into either the ESD jack located on the lower-left outside edge of the bay assembly, or the other ESD jack located at the bottom rear of the shelf.

Step 5 Complete the "NTP-F116 Replace the Rear Cover" procedure on page 1-13.

Step 6 Continue with the "NTP-F117 Perform the Bay Installation Acceptance Test" procedure on page 1-13.

Stop. You have completed this procedure.

NTP-F116 Replace the Rear Cover

Purpose	This procedure replaces the rear cover.
Tools/Equipment	Screwdriver Retaining screws
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Grasp the clear plastic cover on each side.

Step 2 Align the cover with the holes provided for the screws.

Step 3 Screw the retaining screws that hold the clear plastic cover in place.

Stop. You have completed this procedure.

NTP-F117 Perform the Bay Installation Acceptance Test

Purpose	This procedure performs a bay installation acceptance test.
Tools/Equipment	Voltmeter
Prerequisite Procedures	NTP-F108 Unpack and Inspect the ONS 15600 SDH Bay Assembly, page 1-4 NTP-F109 Install the Bay Assembly, page 1-5 NTP-F111 Open and Remove the Front Door, page 1-7 NTP-F113 Install the Bay Power and Ground, page 1-10 NTP-F114 Remove the Rear Cover, page 1-11 NTP-F115 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-12
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 In Table 1-1, verify that each procedure was completed.

Table 1-1 ONS 15600 SDH Bay Installation Task Summary

Description	Completed
NTP-F108 Unpack and Inspect the ONS 15600 SDH Bay Assembly, page 1-4	
NTP-F109 Install the Bay Assembly, page 1-5	
NTP-F111 Open and Remove the Front Door, page 1-7	

Table 1-1 ONS 15600 SDH Bay Installation Task Summary (continued)

Description	Completed
NTP-F112 Install Cable Routing Modules and Kick Plates, page 1-9	
NTP-F113 Install the Bay Power and Ground, page 1-10	
NTP-F114 Remove the Rear Cover, page 1-11	
NTP-F115 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-12	
NTP-F116 Replace the Rear Cover, page 1-13	

Step 2 Complete the "DLP-F173 Inspect the Bay Installation and Connections" task on page 16-17.

Stop. You have completed this procedure.

CHAPTER 2

Install Cards and Fiber-Optic Cable

This chapter explains how to install the Cisco ONS 15600 SDH cards and fiber-optic cable (fiber).

Before You Begin

Before beginning this chapter, complete Chapter 1, "Install the Bay and Backplane Connections."

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

1. NTP-F118 Install the Common Control Cards, page 2-2—Complete this procedure before continuing with the "NTP-F119 Install the STM-N Cards" procedure on page 2-4.
2. NTP-F119 Install the STM-N Cards, page 2-4—Complete this procedure before continuing with the "NTP-F124 Install the Fiber-Optic Cables" procedure on page 2-9.
3. NTP-F120 Install the ASAP Card, page 2-6—Complete as needed to install the ASAP card, which provides STM-1, STM-4, STM-16, STM-64, and Gigabit Ethernet ports.
4. NTP-F121 Install the Filler Cards, page 2-7—Complete as needed to fill any unused optical card slots with filler cards.
5. NTP-F122 Preprovision a Card Slot, page 2-7—Complete as needed to provision an empty card slot.
6. NTP-F123 Remove and Replace a Card, page 2-8—Complete as needed.
7. NTP-F124 Install the Fiber-Optic Cables, page 2-9—Complete this procedure to install and route the fiber-optic cables.
8. NTP-F125 Replace the Front Door, page 2-12—Complete as needed.

Warning **The intra-building ports of the ONS 15600 are only suitable for connecting intra-building, unexposed wiring, or cabling. The intra-building ports of ONS 15600 must not be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed only to be used as intra-building interfaces (Type 2 ports as described in** GR-1089-CORE, Issue 4**) and require isolation from the exposed OSP cabling. Adding primary protectors is not sufficient to connect these interfaces metallically to OSP wiring.**

Warning **The intrabuilding ports of the ONS 15600 are only suitable for connecting to shielded intra-building cabling grounded at both ends.**

Note The Cisco ONS 15600 is designed only for a Common Bonding Network (CBN), in accordance with the definitions in Section 9.3 of GR1089 Issue 4.

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

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.** Statement 1029

NTP-F118 Install the Common Control Cards

Purpose	This procedure installs the TSC cards and then the SSXC cards, which are required to operate the ONS 15600 SDH.
Tools/Equipment	Redundant TSC cards and SSXC cards
Prerequisite Procedures	NTP-F117 Perform the Bay Installation Acceptance Test, page 1-13
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

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

Caution Always use the supplied ESD wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-left outside edge of the shelf.

Note For information about the TSC and SSXC cards (such as LED information), refer to the *Cisco ONS 15600 SDH Reference Manual*.

Step 1 Remove the card from the box and antistatic sleeve.

Step 2 Install cards in the following sequence:

- Slot 5, TSC card
- Slot 10, TSC card
- Slots 6 and 7, SSXC card
- Slots 8 and 9, SSXC card

Note Software Release 8.0 and later requires the SSXC card, so when upgrading to ONS 15600 SDH Software R8.0 or higher, you must install an SSXC card. Refer to the release-specific software upgrade guide for more information on upgrading the ONS 15600 SDH software.

Step 3 Open the card ejectors.

Step 4 Slide a card along the top and bottom guide rails into the correct slot (follow the sequence given in Step 2), noting that the SSXC faceplate occupies two slots. Insert the card until it contacts the backplane.

Note The software on the active TSC card is automatically copied to the TSC that is plugged into the standby (empty) slot. It does not matter if the software on the newly installed TSC is newer or older than that on the active TSC. After loading the new software for several minutes, the newly installed TSC card becomes the standby card. You should install a single TSC, allow it to boot, then open a CTC session and verify that the TSC is running the desired software. If the TSC is not running the desired software version, do an upgrade or remove the current TSC and install the other one to see if it is running the desired software. After you are sure you have the right software load, you can then safely install the SSXC cards.

Note A CTC session is not available until at least one TSC card has been installed and has booted up. Therefore, SSXC cards do appear in CTC until at least one TSC card is installed.

Step 5 Close the ejectors.

Step 6 Verify the LED activity as described in Table 2-1.

Table 2-1 LED Activity During TSC and SSXC Card Installation

Card Type	LED Activity
TSC	**1.** All LEDs turn on for 20 to 60 seconds. **2.** The STAT LED blinks and all other LEDs turn off for 30 to 50 seconds. **3.** All LEDs blink once and then turn off for 10 seconds. **4.** The SRV LED goes green and the applicable timing indicator goes green (line, external, freerun, holdover).
SSXC	**1.** The STAT and SRV LEDs turn on for 10 to 15 seconds. **2.** The STAT LED blinks and the SRV LED turns off for 30 seconds. **3.** All LEDs blink once and the SRV LED comes on.

Note Be careful to insert the TSC and SSXC cards only in their appropriate slots (see Step 2). If you do insert a card into a slot provisioned for a different card in CTC, all red LEDs turn on.

Step 7 On the TSC card, verify that the ACT/STBY LED is on if the card is active (green) and off if the card is standby. If it is not, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Step 8 Repeat Steps 1 through 7 for each TSC and SSXC card that you need to install.

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

Step 9 After you have logged into CTC, verify that the card appears in the correct slot in the CTC node view. See Chapter 3, "Connect the PC and Log into the GUI" for CTC information and setup instructions.

Stop. You have completed this procedure.

NTP-F119 Install the STM-N Cards

Purpose	This procedure installs optical (STM-N) cards, including STM-16 and STM-64 cards.
Tools/Equipment	STM-16 and STM-64 cards (as applicable)
Prerequisite Procedures	NTP-F117 Perform the Bay Installation Acceptance Test, page 1-13 NTP-F118 Install the Common Control Cards, page 2-2
Required/As Needed	At least one optical card is required to carry traffic. Install according to site plan, if available.
Onsite/Remote	Onsite
Security Level	None

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

Caution Always use the supplied ESD wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-left outside edge of the shelf.

Warning **Class 1 laser product.** Statement 1008

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

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

Note For information about optical cards, refer to the *Cisco ONS 15600 SDH Reference Manual.*

Step 1 Remove the card from the box and antistatic sleeve.

Caution Setting an STM-N card on its connectors can cause damage to the connectors.

Step 2 Open the card ejectors.

Step 3 Slide the card along the top and bottom guide rails into the correct slot. Slots 1 through 4 and 11 through 14 are available for optical cards. Insert the card until it contacts the backplane.

Step 4 Close the ejectors.

Step 5 Verify the LED activity on the card faceplate:

1. The STAT, SRV, SD, SF, and LASER ON LEDs turn on for 20 seconds.
2. The STAT LED blinks and all other LEDs turn on for 30 to 50 seconds.
3. All LEDs blink once and the SRV and LASER ON LEDs turn on.

Note If the LEDs do not turn on, verify that the power breakers on the power distribution unit (PDU) are on. If the LEDs do not behave as expected, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Note If you install an optical card in a slot provisioned for another optical rate, the same LED sequence occurs but at the end of the sequence the SRV LED does not turn on. Only the LASER ON LED turns on.

Note If you insert a card into a slot provisioned for a different card, all red LEDs turn on and you will see a mismatched equipment (MEA) alarm for that slot when you open CTC.

Step 6 After you have logged into CTC, verify that the card appears in the correct slot on the CTC node view. See Chapter 3, "Connect the PC and Log into the GUI" for CTC information and setup instructions.

Note If you deleted circuits, data communication channels (DCCs), and timing references for the STM-N card, you must restore them.

Step 7 Complete the "NTP-F120 Install the ASAP Card" procedure on page 2-6 and the "NTP-F124 Install the Fiber-Optic Cables" procedure on page 2-9.

Stop. You have completed this procedure.

NTP-F120 Install the ASAP Card

Purpose	This procedure installs the ASAP card. The ASAP card installation consists of installing the following components: • Carrier module (card) • 1-port I/O modules (1PIOs) and/or 4-port I/O modules (4PIOs), also known as Pluggable Interface Modules (PIMs) • Small form-factor pluggables (SFPs)
Tools/Equipment	ASAP card(s)
Prerequisite Procedures	NTP-F117 Perform the Bay Installation Acceptance Test, page 1-13 NTP-F118 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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

Caution Always use the supplied ESD wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-left outside edge of the shelf.

Warning **Class 1 laser product.** Statement 1008

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

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

Note For information about the ASAP card, refer to the *Cisco ONS 15600 SDH Reference Manual.*

Step 1 Complete the "DLP-F333 Install the ASAP Carrier Modules" task on page 18-33.

Step 2 Complete the "DLP-F385 Install the ASAP 1PIO and 4PIO (PIM) Modules" task on page 18-98 to install any combination of up to four ASAP 1PIO and 4PIO (PIM) modules in the ASAP carrier modules.

Step 3 Complete the "DLP-F388 Install an SFP/XFP" task on page 18-104 to install SFPs in the 1PIO and 4PIO (PIM) modules, or preprovision an SFP using the "DLP-F335 Preprovision an SFP" task on page 18-35. The optical line rate for SFPs must be assigned in CTC.

Step 4 Continue with the "NTP-F124 Install the Fiber-Optic Cables" procedure on page 2-9 as needed.

Note If you deleted circuits, DCCs, and timing references for the ASAP card, you must restore them.

Stop. You have completed this procedure.

NTP-F121 Install the Filler Cards

Purpose	This procedure installs the filler cards (blank faceplates) in any unused optical card slots.
Tools/Equipment	Filler card(s) (Cisco P/N 15600-IO-FILLER)
Prerequisite Procedures	NTP-F118 Install the Common Control Cards, page 2-2 NTP-F119 Install the STM-N Cards, page 2-4
Required/As Needed	As needed for any unused card slots
Onsite/Remote	Onsite
Security Level	None

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

Step 1 Open the card ejectors.

Step 2 Slide the card along the top and bottom guide rails into the correct optical card slot.

Step 3 Close the ejectors.

Step 4 Repeat for any remaining unused card slots.

Note CTC automatically detects filler cards and includes them in the graphical shelf display.

Stop. You have completed this procedure.

NTP-F122 Preprovision a Card Slot

Purpose	This procedure preprovisions a slot before card installation.
Tools/Equipment	None

Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1 NTP-F127 Set Up CTC Computer for Local Craft Connection to the ONS 15600 SDH, page 3-3 or NTP-F128 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15600 SDH, page 3-4
Required/As Needed	As needed
Onsite/Remote	Onsite or Remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to preprovision the slot.

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

Step 3 From the Add Card shortcut menu, choose the card type that will be installed.

Note A preprovisioned slot appears violet in CTC. An installed card appears white in CTC.

Stop. You have completed this procedure.

NTP-F123 Remove and Replace a Card

Purpose	This procedure removes a card from an ONS 15600 SDH shelf.
Tools/Equipment	None
Prerequisite Procedures	NTP-F118 Install the Common Control Cards, page 2-2 or NTP-F119 Install the STM-N Cards, page 2-4
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 If you are not logged into CTC and you need to remove a card, remove the card as described in Step 4. When you log into CTC, troubleshoot the mismatched equipment alarm (MEA) with the procedure in the *Cisco ONS 15600 SDH Troubleshooting Guide*.

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

- "DLP-F174 Delete a Card from CTC" task on page 16-17
- "DLP-F294 Change an STM-N Card" task on page 17-85 (to delete a card and replace it with a different STM-N card)

Note Provisioning is not maintained during a card change. To change a card, you must first delete all circuits, DCCs, and timing references on the card.

Step 3 If you are removing an optical card with cables connected to the front:

a. Rotate the plastic cable latch over the cable routing channel that corresponds to the optical card so that the latch is open (not blocking the routing channel).

b. Squeeze the latches on both sides of the connector and pull the connector out of the adapter on the front of the card.

Step 4 Physically remove the card:

a. Open the card latches/ejectors.

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

Caution Do not allow the connectors on the card to touch anything as you remove the card.

Step 5 Insert the new card using one of the following procedures as applicable:

- NTP-F118 Install the Common Control Cards, page 2-2
- NTP-F119 Install the STM-N Cards, page 2-4

Stop. You have completed this procedure.

NTP-F124 Install the Fiber-Optic Cables

Purpose	This procedure explains how to install fiber-optic cables on the optical cards.
Tools/Equipment	OGI fiber-optic cables: • 15600-OGI-6M. OGI Male to SC SM UPC, 6.10m, 0.80m breakout • 15600-OGI-8M. OGI Male to SC SM UPC, 8.00m, 0.80m breakout • 15600-OGI-12M. OGI Male to SC SM UPC, 12.00m, 0.80m breakout ASAP PPM fiber-optic cables: 9-micron SMF fiber-optic cables with LC connectors, available from multiple fiber-optic cable suppliers DWDM PPM fiber-optic cables: 9-micron SMF fiber-optic cables with SC connectors, available from multiple fiber-optic cable suppliers. Attenuators suitable for STM-16 and STM-64 attenuation (3 dB for short reach and 15 to 20 dB for long reach) Optical power meter
Prerequisite Procedures	NTP-F119 Install the STM-N Cards, page 2-4
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **Class 1 laser product.** Statement 1008

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

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

Warning **Because invisible radiation may be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to radiation and do not stare into open apertures.** Statement 125

Caution Always use the supplied ESD wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the left-hand outside edge of the shelf.

Note The STM-16 cable can terminate both STM-16 and STM-64 signals but when used with STM-64 cards the cable has six unused optical connectors. STM-64 cables are recommended for termination of STM-64 signals.

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

Table 2-2 Optical Card Transmit and Receive Levels

		Transmit		Receive	
Card	**SFPs (if applicable)**	**Minimum**	**Maximum**	**Minimum**	**Maximum**
OC48/STM16 LR/LH 16 Port 1550	—	–2 dBm	+3 dBm	–28 dBm	–9 dBm
OC192/STM64 LR/LH 4 Port 1550	—	+4 dBm	+7 dBm	–22 dBm	–9 dBm
OC48/STM16 SR/SH 16 Port 1310	—	–10 dBm	–3 dBm	–18 dBm	–3 dBm
OC192/STM64 SR/SH 4 Port 1310	—	–6 dBm	–1 dBm	–11 dBm	–1 dBm

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

		Transmit		Receive	
Card	**SFPs (if applicable)**	**Minimum**	**Maximum**	**Minimum**	**Maximum**
ASAP	ONS-SE-Z1 (Supports STM-1 SR-1, STM-4 SR-1, STM-16 IR-1 or GE LX)	–5.0 dBm	0 dBm	–23 dBm[1] –19 dBm[2] –18 dBm[3]	–3 dBm[2] –3 dBm[3] 0 dBm[4]
	ONS-SI-155-L2 (Supports STM-1 LR-2)	–15 dBm	–8.0 dBm	–28 dBm	–8 dBm
	ONS-SI-622-L2: (Supports STM-4 LR-2)	–5.0 dBm	0 dBm	–34 dBm	–10 dBm
	ONS-SE-2G-L2: (Supports STM-16 LR-2)	–2.0 dBm	3.0 dBm	–28 dBm	–10 dBm
	ONS-SI-2G-S1: (Supports OC-48 LR-2)	–2.0 dBm	3.0 dBm	–9.0 dBm	–9 dBm

[1] 155.52/622.08 Mbps

[2] 1250 Mbps

[3] 2488.32 Mbps

Caution Never create physical (hard) fiber loopbacks on the STM-N LR ports unless you use the proper attenuator. Using fiber loopbacks without the proper attenuator causes damage to STM-N LR card receivers.

Step 2 As necessary, complete the "DLP-F175 Install Fiber-Optic Cables in a 1+1 Configuration" task on page 16-18.

Step 3 As necessary, complete the "DLP-F300 Install Fiber-Optic Cables for SNCP Configurations" task on page 18-1.

Step 4 As necessary, complete the "DLP-F349 Install Fiber-Optic Cables for MS-SPRing Configurations" task on page 18-54.

Step 5 Complete the "DLP-F176 Route Fiber-Optic Cables" task on page 16-21.

Stop. You have completed this procedure.

NTP-F125 Replace the Front Door

Purpose	This procedure reattaches the front door of the ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	NTP-F111 Open and Remove the Front Door, page 1-7
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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

Step 2 Lower the door onto the face of the ONS 15600 SDH.

Step 3 Pull the metal latches on the door outward and gently push the door toward the shelf, making sure that no optical cables are caught or pinched in the door.

Step 4 Click the latches in place and release.

Stop. You have completed this procedure.

CHAPTER 3

Connect the PC and Log into the GUI

This chapter explains how to connect PCs and workstations to the Cisco ONS 15600 SDH and how to log into Cisco Transport Controller (CTC) software, which is the Cisco ONS 15600 SDH Operation, Administration, Maintenance, and Provisioning (OAM&P) user interface. Procedures for connecting to the ONS 15600 SDH using TL1 are provided in the *Cisco ONS SDH TL1 Command Guide*.

Before You Begin

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

1. NTP-F126 Set Up Computer for CTC, page 3-1—Complete this procedure if your PC or workstation has never been connected to an ONS 15600 SDH.
2. NTP-F127 Set Up CTC Computer for Local Craft Connection to the ONS 15600 SDH, page 3-3—After your PC or workstation is set up for CTC, complete this procedure to set up your computer to connect to the ONS 15600 SDH.
3. NTP-F128 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15600 SDH, page 3-4—Complete this procedure to set up your computer to connect to the ONS 15600 SDH using a corporate LAN.
4. NTP-F129 Log into the ONS 15600 SDH GUI, page 3-5—Complete this procedure to log into CTC.
5. NTP-F130 Use the CTC Launcher Application to Manage Multiple ONS Nodes, page 3-6—Complete this procedure to use the CTC launcher application.

NTP-F126 Set Up Computer for CTC

Purpose	This procedure explains how to configure your PC or UNIX workstation to run CTC.
Tools/Equipment	Cisco ONS 15600 SDH Release 8.0 software CD
Prerequisite Procedures	Chapter 1, "Install the Bay and Backplane Connections"
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	None

Note JRE 5.0 is required to log into nodes running Software Release 8.0. To log into nodes running Release 4.5 or earlier, you must uninstall JRE 5.0 and install JRE 1.3.1_2. JRE 5.0 is provided on the software CD. See the "DLP-F310 Change the JRE Version" task on page 18-11 as needed.

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

- To install Netscape 7.x, download the browser at the following site: http://browser.netscape.com/releases.
- To install Internet Explorer 6.x on a PC, download the browser at the following site: http://www.microsoft.com.
- To install Mozilla 1.7 on a Solaris 9 or 10, download the browser at the following site: http://www.mozilla.org.
- Choose Tools->options->security, uncheck 'Remember password for sites in the Mozilla Firefox browser.

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

Step 2 Complete the "DLP-F387 Adjust the Java Virtual Memory Heap Size" task on page 18-104 to increase the size of the JVM heap in order to improve the CTC performance.

Step 3 If your computer is a Windows PC, complete the "DLP-F177 Run the CTC Installation Wizard for Windows" task on page 16-24, then go to Step 5.

Step 4 If your computer is a UNIX workstation, complete the "DLP-F178 Run the CTC Installation Wizard for UNIX" task on page 16-27.

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

- NTP-F127 Set Up CTC Computer for Local Craft Connection to the ONS 15600 SDH, page 3-3
- NTP-F128 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15600 SDH, page 3-4

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

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

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

Stop. You have completed this procedure.

NTP-F127 Set Up CTC Computer for Local Craft Connection to the ONS 15600 SDH

Purpose	This procedure tells you how to set up a PC running Windows or a Solaris workstation for a local onsite connection to the ONS 15600 SDH.
Tools/Equipment	Network interface card (NIC), also referred to as an Ethernet card Straight-through (CAT 5) LAN cable
Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Note Only the active Timing and Shelf Controller (TSC) card connector carries traffic. If you connect to the standby TSC or switch TSCs, you will lose connectivity. Cisco recommends that you use the RJ-45 connector on the Customer Access Panel (CAP) so that connection to the ONS 15600 SDH will not be lost during a TSC switch.

Note For initial shelf turn-up, you must use a local craft connection to the ONS 15600 SDH.

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

Table 3-1 CTC Computer Setup for Local Craft Connections to the ONS 15600 SDH

CTC Connection Environment	CTC Computer Setup Task
• You are connecting from a Windows PC. • You will connect to one ONS 15600 SDH. • You need to access non-ONS 15600 SDH applications such as ping and tracert (trace route).	"DLP-F179 Set Up a Windows PC for Craft Connection to an ONS 15600 SDH on the Same Subnet Using Static IP Addresses" task on page 16-30
• You are connecting from a Solaris Workstation. • You will connect to one ONS 15600 SDH; if you will connect to multiple ONS 15600 SDHs, you might need to configure your computer's IP settings each time you connect to an ONS 15600 SDH. • You need to access non-ONS 15600 SDH applications such as ping and tracert (trace route).	"DLP-F180 Set Up a Solaris Workstation for a Craft Connection to an ONS 15600 SDH" task on page 16-32

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

- The RJ-45 port on the active TSC
- The A or B RJ-45 port on the backplane
- The RJ-45 port on a hub or switch to which the ONS 15600 SDH is physically connected

Note For instructions on crimping your own CAT-5 (LAN) cables, refer to the *Cisco ONS 15600 Troubleshooting Guide*.After setting up your CTC computer, continue with the "NTP-F129 Log into the ONS 15600 SDH GUI" procedure on page 3-5, if applicable.

Stop. You have completed this procedure.

NTP-F128 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15600 SDH

Purpose	This procedure sets up your computer to access the ONS 15600 SDH through a corporate LAN.
Tools/Equipment	NIC, also referred to as an Ethernet card Straight-through (CAT 5) LAN cable
Prerequisite Procedures	• NTP-F126 Set Up Computer for CTC, page 3-1 • The ONS 15600 SDH must be provisioned for LAN connectivity, including IP address, subnet mask, and default gateway. • The ONS 15600 SDH must be physically connected to the corporate LAN. • The CTC computer must be connected to the corporate LAN that has connectivity to the ONS 15600 SDH.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 If your computer is already connected to the corporate LAN, go to Step 3. If you changed your computer's network settings for craft access to the ONS 15600 SDH, change the settings back to the corporate LAN access settings. This generally means:

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

Step 2 Connect a CAT-5 (LAN) cable from the PC or Solaris workstation NIC card to one of the LAN ports on the backplane.

Step 3 If your computer is connected to a proxy server, disable proxy service or add the ONS 15600 SDH nodes as exceptions. To disable proxy service, complete one of the following tasks, depending on the web browser that you use:

- DLP-F274 Disable Proxy Service Using Internet Explorer (Windows), page 17-64
- DLP-F275 Disable Proxy Service Using Netscape (Windows and UNIX), page 17-65
- DLP-F416 Disable Proxy Service Using Mozilla Firefox (Windows and UNIX), page 17-66

Step 4 Continue with the "NTP-F129 Log into the ONS 15600 SDH GUI" procedure on page 3-5.

Stop. You have completed this procedure.

NTP-F129 Log into the ONS 15600 SDH GUI

.

Purpose	This procedure logs into CTC, the graphical user interface software used to manage the ONS 15600 SDH. This procedure includes optional node login tasks.
Tools/Equipment	None
Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1 One of the following procedures: • NTP-F127 Set Up CTC Computer for Local Craft Connection to the ONS 15600 SDH, page 3-3 • NTP-F128 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15600 SDH, page 3-4
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34.

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

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

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

Step 2 As needed, complete the "DLP-F307 Create Login Node Groups" task on page 18-9. Login node groups display nodes that are not connected to the log-in node via DCC.

Step 3 As needed, complete the "DLP-F183 Add a Node to the Current Session or Login Group" task on page 16-37.

Step 4 As needed, complete the "DLP-F308 Delete a Node from the Current Session or Login Group" task on page 18-10.

Step 5 As needed, complete the "DLP-F309 Configure the CTC Alerts Dialog Box for Automatic Popup" task on page 18-11.

Stop. You have completed this procedure.

NTP-F130 Use the CTC Launcher Application to Manage Multiple ONS Nodes

Purpose	This procedure uses the CTC Launcher to start a CTC session with an ONS NE that has an IP connection to the CTC computer; create TL1 tunnels to connect to ONS NEs on the other side of third-party, OSI-based GNEs; and view, manage, and delete TL1 tunnels using CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1 One of the following procedures: • NTP-F127 Set Up CTC Computer for Local Craft Connection to the ONS 15600 SDH, page 3-3 • NTP-F128 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15600 SDH, page 3-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note JRE 5.0 must be installed on the PC you are using with the CTC Launcher application.

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

- DLP-F399 Install the CTC Launcher Application from a Release 8.0 Software CD, page 18-122
- DLP-F400 Install the CTC Launcher Application from a Release 8.0 Node, page 18-122

Step 2 As needed, complete the "DLP-F401 Connect to ONS Nodes Using the CTC Launcher" task on page 19-1 to connect to an ONS network element with direct IP connectivity.

Step 3 As needed, complete one of the following tasks to create a TL1 tunnel, which enables you to connect to an ONS network element residing behind OSI-based, third-party GNEs:

- DLP-F402 Create a TL1 Tunnel Using the CTC Launcher, page 19-3
- DLP-F403 Create a TL1 Tunnel Using CTC, page 19-4

Step 4 As needed, complete the "DLP-F404 View TL1 Tunnel Information" task on page 19-5.

Step 5 As needed, complete the "DLP-F405 Edit a TL1 Tunnel Using CTC" task on page 19-6.

Step 6 As needed, complete the "DLP-F406 Delete a TL1 Tunnel Using CTC" task on page 19-7.

Stop. You have completed this procedure.

CHAPTER 4

Turn Up a Node

This chapter explains how to provision a single Cisco ONS 15600 SDH node and turn it up for service, including node name, date and time, timing references, network attributes such as IP address and default router, users and user security, and card protection groups.

Before You Begin

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

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

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

1. NTP-F131 Verify Card Installation, page 4-2—Complete this procedure first.
2. NTP-F132 Create Users and Assign Security, page 4-3—Continue with this procedure to create Cisco Transport Controller (CTC) users and assign their security levels.
3. NTP-F133 Set Up Date, Time, and Contact Information, page 4-4—Continue with this procedure to set the node name, date, time, location, and contact information.
4. NTP-F134 Set Power Monitor Thresholds, page 4-6—Continue with this procedure on a node with a customer access panel version 2 (CAP2) installed to provision power thresholds within a –48 VDC environment.
5. NTP-F135 Set Up CTC Network Access, page 4-6—Continue with this procedure if the ONS 15600 SDH will be accessed behind firewalls.
6. NTP-F248 Set Up the ONS 15600 in EMS Secure Access, page 4-7—Continue with this procedure to connect the CTC in secure mode.
7. NTP-F136 Set Up the ONS 15600 SDH for Firewall Access, page 4-8—Continue with this procedure to provision the IP address, default router, subnet mask, and network configuration settings.
8. NTP-F249 Create FTP Host, page 4-8 -- Continue with this procedure if to create FTP host for ENE database backup.
9. NTP-F137 Set Up Timing, page 4-9—Continue with this procedure to set up the node SDH timing references.
10. NTP-F138 Create a 1+1 Protection Group, page 4-10—Complete as needed to set up 1+1 protection groups for ONS 15600 SDH optical cards.

11. NTP-F139 Set Up SNMP, page 4-11—Continue with this procedure, as needed.
12. NTP-F140 Set the User Code for Card Inventory, page 4-12—Continue with this procedure, as needed.
13. NTP-F141 Configure a Node Using an Existing Database, page 4-12—Continue with this procedure, as needed.
14. NTP-F142 Set External Alarms and Controls, page 4-13—As needed, complete these tasks to set external alarm reporting, assign external alarms to virtual wires, and view external alarms for ONS 15600 SDH nodes and ONS 15454 SDH nodes.
15. NTP-F143 Provision OSI, page 4-14—complete this procedure if the ONS 15600 SDH will be connected in networks with network elements (NEs) that are based on the Open System Interconnection (OSI) protocol stack. This procedure provisions the TID Address Resolution Protocol (TARP), OSI routers, manual area addresses, subnetwork points of attachment, and IP-over-OSI tunnels.

NTP-F131 Verify Card Installation

Purpose	This procedure verifies that the ONS 15600 SDH node is ready for turn-up.
Tools/Equipment	None
Prerequisite Procedures	Chapter 1, "Install the Bay and Backplane Connections" Chapter 2, "Install Cards and Fiber-Optic Cable"
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Verify that the TSC cards are installed in Slots 5 and 10.

Step 2 Verify that the green ACT/STBY LED is illuminated on the active TSC. The ACT/STBY LED will not be illuminated on the standby TSC.

Note If the TSCs are not installed or their LEDs are not illuminated as described, do not proceed. See Chapter 2, "Install Cards and Fiber-Optic Cable" or refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* to resolve installation problems before proceeding.

Step 3 Verify that the SSXC cards are installed in Slots 6 and 8. The SSXC card faceplates extend to cover Slots 7 and 9, respectively.

Step 4 Verify that the SRV LED is illuminated on both SSXC cards.

Note If the SSXC cards are not installed, or their LEDs are not illuminated as described, do not proceed. See Chapter 2, "Install Cards and Fiber-Optic Cable" or refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* to resolve installation problems before proceeding.

Step 5 Verify that the STM-N cards are installed in the slots designated by your site plan. Slots 1 to 4 and 11 to 14 are used for all optical cards.

Step 6 Verify that fiber-optic cables are installed and connected to the locations indicated in the site plan.

Step 7 Verify that fiber is routed correctly in the shelf assembly.

Step 8 Verify that the SSXC cards are working:

a. Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node that you will turn up.

b. Click the **Maintenance > Diagnostic** tabs.

c. Click **Run Diagnostics Test**.

- If errors exist, the Cross Connect Diagnostics Error box appears with a list of errors. Click **Close**.
- If no errors exist, click **OK** to close the confirmation dialog box.

Note You must run the diagnostics test before the optical cards are provisioned.

For more information about Diagnostics refer to "Using CTC Diagnostics" in the General Troubleshooting chapter of the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Step 9 Set the optical power received threshold for each optical card. See the "DLP-F261 Set the Optical Power Received Nominal Value" task on page 17-54.

Step 10 If all cards and fiber are installed in the ONS 15600 SDH shelf as described in Steps 1 through 9, continue with the "NTP-F132 Create Users and Assign Security" procedure on page 4-3.

Note If cards are not installed or the LEDs are not shown as described, do not continue. Go to Chapter 2, "Install Cards and Fiber-Optic Cable" or the *Cisco ONS 15600 SDH Troubleshooting Guide* to resolve the installation problems before continuing with shelf turn up.

Stop. You have completed this procedure.

NTP-F132 Create Users and Assign Security

Purpose	This procedure creates ONS 15600 SDH users and assigns security levels.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you need to create users. If you are already logged in, continue with Step 2.

Note You must log in as a Superuser to create additional users. The CISCO15 user provided with each ONS 15600 SDH can be used to set up other ONS 15600 SDH users. You can add up to 500 users to one ONS 15600 SDH.

Step 2 Complete the "DLP-F269 Change User Password and Security Levels for a Single Node" task on page 17-61 or the "DLP-F270 Change User and Security Settings for Multiple Nodes" task on page 17-62 as needed.

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

Stop. You have completed this procedure.

NTP-F133 Set Up Date, Time, and Contact Information

Purpose	This procedure provisions identification information for the node, including the node name, a contact name and phone number, the location of the node, and the date, time, and time zone.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 for the node you will turn up. If you are already logged in, continue with Step 2.

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

Step 3 Enter the following information in the fields listed:

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

Tip You can also position nodes manually in network view. Press Ctrl while you drag and drop the node icon. To create the same network map visible for all ONS 15600 SDH users, complete the "NTP-F162 Create a Logical Network Map" procedure on page 5-33.

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

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

If you do not use an SNTP or NTP server, complete the Date and Time fields. The ONS 15600 SDH will use these fields for alarm dates and times. By default, CTC displays all alarms in the CTC computer time zone for consistency. To change the display to the node time zone, complete the "DLP-F198 Display Events Using Each Node's Time Zone" task on page 16-58.

Note Using an NTP or SNTP server ensures that all ONS 15600 SDH network nodes use the same date and time reference. The server synchronizes node time after power outages or software upgrades.

If you check the Use NTP/SNTP Server check box, enter the IP address of one of the following:

- An NTP/SNTP server connected to the ONS 15600 SDH
- Another ONS 15600 SDH with NTP/SNTP enabled that is connected to the ONS 15600 SDH

If you check Gateway Network Element (GNE) for the ONS 15600 SDH SOCKS proxy server (see the "DLP-F185 Provision IP Settings" task on page 16-38), external ONS 15600 SDHs must reference the gateway ONS 15600 SDH for NTP/SNTP timing. For more information about the ONS 15600 SDH gateway settings, refer to the *Cisco ONS 15600 SDH Reference Manual*.

Note In ONS 15600 Software Release 9.0 and later, you can configure an IPv6 address for an NTP/SNTP server, in addition to an IPv4 address.

Caution If you reference another ONS 15600 SDH for the NTP/SNTP server, make sure the second ONS 15600 SDH references an NTP/SNTP server and not the first ONS 15600 SDH (that is, do not create an NTP/SNTP timing loop by having two ONS 15600 SDHs reference each other).

- Date—If Use NTP/SNTP Server is not selected, enter the current date in the format mm/dd/yyyy, for example, September 24, 2002 is 09/24/2002.
- Time—If Use NTP/SNTP Server is not selected, enter the current time in the format hh:mm:ss, for example, 11:24:58. The ONS 15600 SDH uses a 24-hour clock, so 10:00 PM is entered as 22:00:00.
- Time Zone—Click the field and choose a city within your time zone from the drop-down list. The menu displays the 80 World Time Zones from –11 through 0 (GMT) to +14. Continental United States time zones are GMT-05:00 (Eastern), GMT-06:00 (Central), GMT-07:00 (Mountain), and GMT-08:00 (Pacific).

Step 4 Click **Apply**.

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

Step 6 Review the node information. If you need to make corrections, repeat Steps 3 through 5 to enter the corrections. If the information is correct, continue with the "NTP-F135 Set Up CTC Network Access" procedure on page 4-6.

Stop. You have completed this procedure.

NTP-F134 Set Power Monitor Thresholds

Purpose	This procedure provisions extreme high and extreme low input battery power thresholds within a –48 VDC environment. When the thresholds are crossed, the TSC generates warning alarms in CTC. You must have a CAP2 installed to be able to set power thresholds.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to set power monitor thresholds. If you are already logged in, continue with Step 2.

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

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

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

Step 5 Click **Apply**.

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

NTP-F135 Set Up CTC Network Access

Purpose	This procedure provisions network access for a node, including its subnet mask, default router, Dynamic Host Configuration Protocol (DHCP) server, (Internet Inter-Orb Protocol) IIOP listener port, SOCKS proxy server settings, static routes, Open Shortest Path First (OSPF) protocol, and designated SOCKS servers.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-F185 Provision IP Settings" task on page 16-38 to provision the ONS 15600 SDH IP address, subnet mask, default router, DHCP server, IIOP listener port, and SOCKS proxy server settings.

Step 3 If static routes are needed, complete the "DLP-F186 Create a Static Route" task on page 16-41. Refer to the *Cisco ONS 15600 SDH Reference Manual* for more information about static routes.

Step 4 If the ONS 15600 SDH is connected to a LAN or WAN that uses OSPF and you want to share routing information between the LAN/WAN and the ONS network, complete the "DLP-F187 Set Up or Change Open Shortest Path First Protocol" task on page 16-42.

Step 5 Complete the "DLP-F398 Provision the Designated SOCKS Servers" task on page 18-121 after the network is provisioned and one or more of the following conditions exist:

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

Stop. You have completed this procedure.

NTP-F248 Set Up the ONS 15600 in EMS Secure Access

Purpose	This procedure provisions ONS 15600s and CTC computers for secure access.
Tools/Equipment	None
Prerequisite Procedures	NTP-F135 Set Up CTC Network Access, page 4-6
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

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

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

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

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

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

Stop. You have completed this procedure.

NTP-F136 Set Up the ONS 15600 SDH for Firewall Access

Purpose	This procedure provisions ONS 15600 SDHs and CTC computers for access through firewalls.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 If the ONS 15600 SDH resides behind a firewall, complete the "DLP-F262 Provision the IIOP Listener Port on the ONS 15600 SDH" task on page 17-54.

Step 3 If the CTC computer resides behind a firewall, complete the "DLP-F263 Provision the IIOP Listener Port on the CTC Computer" task on page 17-55.

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

NTP-F249 Create FTP Host

Purpose	This procedure provisions an FTP Host that you can use to perform database backup and restore or software download to an End Network Element (ENE) when proxy or firewall is enabled.
Tools/Equipment	None
Prerequisite Procedures	NTP-F135 Set Up CTC Network Access, page 4-6 NTP-F136 Set Up the ONS 15600 SDH for Firewall Access, page 4-8
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 If you want to turn on the ONS 15600 secure mode, which allows two IPv4 addresses to be provisioned for the node if TCC2P cards are installed, complete the "NTP-F248 Set Up the ONS 15600 in EMS Secure Access" task on page 4-7. Refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15600 SDH Reference Manual* for information about secure mode.

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

Step 4 Click **Create**.

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

Note In ONS 15600 Software Release 9.0 and later, you can configure an IPv6 address for an FTP server, in addition to an IPv4 address.

Step 6 The Mask is automatically set according to the Net/Subnet Mask length specified in "DLP-F185 Provision IP Settings" task on page 16-38. To change the Mask, click the Up/Down arrows on the **Length** menu.

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

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

Step 9 Click OK.

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

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

NTP-F137 Set Up Timing

Purpose	This procedure provisions the ONS 15600 SDH timing.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to set up timing. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-F188 Set Up External or Line Timing" task on page 16-45 if an external building integrated timing supply (BITS) source is available. This is the common SDH timing setup procedure.

Step 3 If you cannot complete Step 2 (an external BITS source is not available), complete the "DLP-F189 Set Up Internal Timing" task on page 16-47. This task can only provide Stratum 3E timing.

Note For information about SDH timing, refer to the *Cisco ONS 15600 SDH Reference Manual* or to ITU-T G.784.

Stop. You have completed this procedure.

NTP-F138 Create a 1+1 Protection Group

Purpose	This procedure creates a 1+1 protection group. A 1+1 protection group pairs a working STM-N port with a protect STM-N port. The ports on cards can be either working or protect. You can mix working and protect ports on the same card: any STM-64 port can protect another STM-64 port, and any STM-16 port can protect another STM-16 port. You cannot mix STM-64 and STM-16 ports in protection schemes.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to create the protection group. If you are already logged in, continue with Step 2.

Step 2 Verify that the STM-N cards are installed.

Step 3 Click the **Provisioning** > **Protection** tabs.

Step 4 Click **Create**.

Step 5 In the Create Protection Group dialog box, enter the following:

- Name—Enter a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (") characters.
- Type—Choose **1+1 (port)** from the drop-down list.
- Protect (Entity) Port—Choose the protect port from the drop-down list. When you choose 1+1 (port) from the Type drop-down list, this field changes from Protect Entity to Protect Port. The list displays the available STM-N ports. If STM-N cards are not installed, no ports appear in the drop-down list.

After you choose the protect port, a list of working ports available for protection appears in the Available Ports list. If no cards are available, no ports appear. If this occurs, you cannot complete this task until you install the physical cards or preprovision the ONS 15600 SDH slots using the "NTP-F122 Preprovision a Card Slot" procedure on page 2-7.

Step 6 From the Available Ports list, choose the working port that will be protected by the port chosen in the Protect Port field. Click the top arrow button to move each port to the Working Ports list.

Step 7 Complete the remaining fields:

- Bidirectional switching—If checked, both the near-end and far-end nodes switch to the designated protection ports. For example, if the near-end node has a loss of signal (LOS) alarm, it switches to the protection port and transmits a switch request to the far-end node to switch to the protection port also. This ensures that both nodes process traffic from the same span.

  If the Bidirectional switching check box is not checked, the near-end and far-end nodes switch independently of each other. For example, if the near-end node has an LOS on its working port it switches to the protection port. If the far-end node does not have an LOS, traffic remains on the working port.
- Revertive—Check this check box if you want traffic to revert to the working port after failure conditions stay corrected for the amount of time entered in the Reversion time field.

- Reversion time—If Revertive is checked, click the Reversion time field and choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. Reversion time is the interval between the point when the fault is cleared and the point when the traffic switches to the working port. The reversion timer starts after conditions causing the switch are cleared.

Step 8 Click **OK**.

Stop. You have completed this procedure.

NTP-F139 Set Up SNMP

Purpose	This procedure sets up Simple Network Management Protocol (SNMP) parameters so that you can use SNMP management software with the ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	Required if SNMP is used at your installation
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to set up SNMP. If you are already logged in, continue with Step 2.

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

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

Step 4 In the Create SNMP Traps Destination dialog box, complete the following:

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

Note In ONS 15600 Software R9.0 and later, you can configure IPv6 addresses for SNMPv1/v2/v3 trap destinations, Get/Set requests and proxy targets, in addition to IPv4 addresses.

- Community—Enter the SNMP community name.

Note The community name is a form of authentication and access control. The community name assigned to the ONS 15600 SDH is case-sensitive and must match the community name of the NMS. For a description of SNMP community names, refer to the "SNMP" chapter in the *Cisco ONS 15600 SDH Troubleshooting Guide*.

- UDP Port—The default User Datagram Protocol (UDP) port for SNMP is 162.
- Trap Version—Choose either SNMPv1 or SNMPv2 from the drop-down list. Refer to your NMS documentation to determine whether to use SNMP v1 or v2.

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

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

Stop. You have completed this procedure.

NTP-F140 Set the User Code for Card Inventory

Purpose	This procedure creates a user code to help identify the SSXC, TSC, and optical (traffic) cards. The user code is stored in nonvolatile memory on the card so it is not lost when a card is moved or stored as a spare.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Click the **Inventory** tab.

Step 3 In the User Code field, type the code you want to use to identify the card. The user code is a 20-character ASCII string.

Step 4 Click **Apply**.

Stop. You have completed this procedure.

NTP-F141 Configure a Node Using an Existing Database

Purpose	This procedure downloads the provisioning database file from one node to a designated node and assigns a new IP address to the designated node. You can use this procedure to turn up a node or to reconfigure a node.
Tools/Equipment	Database backup file
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note Only the provisioning database is downloaded from the specified database backup even if the alarm, performance, or audit logs are included in the database backup.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node that you want to configure. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "NTP-F221 Back Up the Database" procedure on page 14-4 to back up the logged in node before reconfiguration.

Step 3 Click the **Maintenance > Database tabs.**

Step 4 Click **Configure**. The Configure Node dialog box appears. In the Current Node Configuration area, the Version field displays the current software version.

Step 5 Click **Browse** and navigate to the database backup file you will use to configure the node.

Step 6 In the Database Configuration area, verify the following:

- Provisioning—(Display only) Automatically checked to download the provisioning data from the selected database file.
- Version—(Display only) Displays the software version of the selected database file.
- IP address—(Display only) Displays the IP address assigned to the node of the selected database file.

Step 7 In the New Node Configuration area, verify the following:

- Provisioning—(Display only) Downloads the provisioning data from the selected database file.
- Version—(Display only) Displays the current software version.
- IP address—Displays the current IP address. To assign a new IP address, type a new IP address in the field.

Step 8 Click **OK**. When the Node Configuration warning message appears, click **Yes** to continue. The database restoration window appears. The CTC session closes when the TSC reboots.

Step 9 After the TSC completes its reboot, log into the node using the IP address assigned in Step 7. For login instructions, see the "DLP-F181 Log into CTC" task on page 16-34.

Stop. You have completed this procedure.

NTP-F142 Set External Alarms and Controls

Purpose	This procedure provisions the reporting parameters and/or virtual wires for external alarms and controls (environmental alarms) that are wired to the CAP or CAP2 alarm contacts.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-F204 Provision External Alarms and Virtual Wires" task on page 17-5 to set external alarm inputs.

Step 3 Complete the "DLP-F205 Provision External Controls for External Alarms and Virtual Wires" task on page 17-6 to set external control outputs.

Stop. You have completed this procedure.

NTP-F143 Provision OSI

Purpose	This procedure provisions the ONS 15600 SDH so it can be networked with other vendor NEs that use the OSI protocol stack for data communications network (DCN) communications. This procedure provisions the TARP, OSI routers, manual area addresses, subnetwork points of attachment, and IP-over-OSI tunnels.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

⚠ **Caution** This procedure requires an understanding of OSI protocols, parameters, and functions. Before you begin, review the OSI reference sections in the "Management Network Connectivity" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

⚠ **Caution** Do not begin this procedure until you know the role of the ONS 15600 SDH within the OSI and IP network.

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

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to provision the OSI routing mode. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the following:

- "DLP-F361 Provision OSI Routing Mode" task on page 18-73—Complete this task first.
- "DLP-F362 Provision or Modify TARP Operating Parameters" task on page 18-74—Complete this task next.
- "DLP-F363 Add a Static TID-to-NSAP Entry to the TARP Data Cache" task on page 18-76—Complete this task as needed.
- "DLP-F365 Add a TARP Manual Adjacency Table Entry" task on page 18-77—Complete this task as needed.
- "DLP-F366 Provision OSI Routers" task on page 18-78—Complete this task as needed.

- "DLP-F367 Provision Additional Manual Area Addresses" task on page 18-79—Complete this task as needed.
- "DLP-F368 Enable the OSI Subnet on the LAN Interface" task on page 18-79—Complete this task as needed.
- "DLP-F369 Create an IP-Over-CLNS Tunnel" task on page 18-80—Complete this task as needed.

Stop. You have completed this procedure.

NTP-E200 Provision Node for SNMPv3

Purpose	This procedure provisions the node to allow SNMPv3 access.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

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

Step 3 Complete the following tasks as required:

- DLP-F407 Create an SNMPv3 User, page 19-8
- DLP-F409 Create Group Access, page 19-9

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

- DLP-F408 Create MIB Views, page 19-9

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

Stop. You have completed this procedure.

NTP-E201 Provision Node to Send SNMPv3 Traps

Purpose	This procedure provisions a node to send SNMP v3 traps.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

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

Step 3 Complete the following tasks as required:

- DLP-F407 Create an SNMPv3 User, page 19-8
- DLP-F409 Create Group Access, page 19-9
- DLP-F408 Create MIB Views, page 19-9
- DLP-F412 Create Notification Filters, page 19-12
- DLP-F410 Configure SNMPv3 Trap Destination, page 19-10. When you configure an SNMPv3 trap destination, use the IP address of the NMS, and the port number on which the NMS is listening for traps.

Stop. You have completed this procedure.

NTP-E202 Manually Provision a GNE/ENE to Manage an ENE using SNMPv3

Purpose	This procedure describes how to manually configure a GNE/ENE to allow the NMS to manage an ENE using SNMPv3.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 Go to network view.

Step 3 Double-click the ENE.

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

Step 5 Double-click the GNE.

Step 6 Complete the "DLP-F407 Create an SNMPv3 User" task on page 19-8 to create an SNMPv3 user on the GNE.

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

- DLP-F407 Create an SNMPv3 User, page 19-8
- DLP-F409 Create Group Access, page 19-9
- DLP-F408 Create MIB Views, page 19-9

Step 8 Complete the "DLP-F413 Manually Configure the SNMPv3 Proxy Forwarder Table" task on page 19-12. Use the context engine ID from Step 4, the local user details created in Step 6, and the remote user created in Step 7.

Stop. You have completed this procedure.

NTP-E203 Automatically Provision a GNE to Manage an ENE using SNMPv3

Purpose	This procedure describes how to automatically configure a GNE to allow an NMS to manage an ENE using SNMPv3.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 Go to network view.

Step 3 Double-click the GNE.

Step 4 Complete the "DLP-F407 Create an SNMPv3 User" task on page 19-8 to create an SNMPv3 user on the GNE.

Step 5 Complete the"DLP-F414 Automatically Configure the SNMPv3 Proxy Forwarder Table" task on page 19-13. Use the GNE user that you defined in Step 4 when you configure the Proxy Forwarder table.

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

Stop. You have completed this procedure.

NTP-E204 Manually Provision a GNE/ENE to Send SNMPv3 Traps from an ENE using SNMPv3

Purpose	This procedure describes how to manually configure the GNE/ENE to allow an ENE to send SNMPv3 traps to the NMS.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 Go to network view.

Step 3 Double-click the GNE.

Step 4 Complete the "DLP-F407 Create an SNMPv3 User" task on page 19-8 to create an SNMPv3 user on the GNE.

Step 5 On the GNE, complete the "DLP-F410 Configure SNMPv3 Trap Destination" task on page 19-10. The target IP address must be the IPv4 or IPv6 address of the NMS. For the UDP Port number, use the port number on which the NMS is listening for traps. Use the user name configured in Step 4. Also, specify a target tag name.

Step 6 Double-click the ENE.

Step 7 Complete the "DLP-F407 Create an SNMPv3 User" task on page 19-8 to create an SNMPv3 user on the ENE.

Step 8 Complete the following tasks as required:

- DLP-F409 Create Group Access, page 19-9 to create a group on the ENE
- DLP-F408 Create MIB Views, page 19-9to create a MIB view on the ENE
- DLP-F412 Create Notification Filters, page 19-12

Step 9 On the ENE, complete the "DLP-F410 Configure SNMPv3 Trap Destination" task on page 19-10. The target IP address should be the IP address of the GNE. The UDP port number is 161. Use the user name configured in Step 7.

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

Step 11 Complete the "DLP-F415 Manually Configure the SNMPv3 Proxy Trap Forwarder Table" task on page 19-14.

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

Stop. You have completed this procedure.

NTP-E205 Automatically Provision a GNE/ENE to Send SNMPv3 Traps from an ENE Using SNMPv3

Purpose	This procedure describes how to automatically configure the GNE/ENE to allow an ENE to send SNMPv3 traps to the NMS.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	Required if you want to implement SNMPv3 on your network.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 on the node on which you want to set up SNMPv3. If you are already logged in, go to Step 2.

Step 2 Go to Network View.

Step 3 Double-click the GNE.

Step 4 Complete the task "DLP-F407 Create an SNMPv3 User" task on page 19-8 to create an SNMPv3 user on the GNE.

Step 5 On the GNE, complete the following tasks:

- DLP-F410 Configure SNMPv3 Trap Destination, page 19-10. The target IP address must be the IPv4 or IPv6 address of the NMS. For the UDP Port number, use the port number on which the NMS is listening for traps. Also, specify a target tag name.
- DLP-F416 Automatically Configure the SNMPv3 Proxy Trap Forwarder Table, page 19-15. Use the target tag configured in Step 4. Use the IP address of the ENE as the source of trap. Create a trap destination on the ENE with an IP address of the GNE as the target IP and 161 as the UDP port number. The following details are created automatically:
  - A user named ons_trap_user on the ENE
  - Remote user details of the ENE on the GNE

Stop. You have completed this procedure.

CHAPTER 5

Turn Up a Network

This chapter explains how to turn up and test Cisco ONS 15600 SDHs in point-to-point networks, multiplex section-shared protection rings (MS-SPRing), subnetwork connection protection (SNCP) rings, and dual-ring interconnects (DRIs).

Before You Begin

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

1. NTP-F144 Verify Node Turn-Up, page 5-2—Complete this procedure before beginning network turn-up.
2. NTP-F145 Provision a Point-to-Point Connection, page 5-3—Complete this procedure as needed to connect two ONS 15600 SDHs in a point-to-point network.
3. NTP-F146 Point-to-Point Network Acceptance Test, page 5-4—Complete this procedure after you provision the point-to-point network.
4. NTP-F147 Provision MS-SPRing Nodes, page 5-6—Complete this procedure to provision ONS 15600 SDH nodes for a two-fiber MS-SPRing.
5. NTP-F148 Create an MS-SPRing, page 5-8—Complete this procedure after provisioning the MS-SPRing nodes.
6. NTP-F149 Two-Fiber MS-SPRing Acceptance Test, page 5-8—Complete this procedure after you provision a two-fiber MS-SPRing.
7. NTP-F150 Provision a Traditional MS-SPRing Dual-Ring Interconnect, page 5-10—As needed, complete this procedure after you provision an MS-SPRing.
8. NTP-F151 Provision an Integrated MS-SPRing Dual-Ring Interconnect, page 5-12—As needed, complete this procedure after you provision an MS-SPRing.
9. NTP-F152 Provision SNCP Nodes, page 5-13—Complete this procedure as needed to create an SNCP.
10. NTP-F153 SNCP Acceptance Test, page 5-15—Complete this procedure after you provision the SNCP.
11. NTP-F154 Provision a Traditional SNCP Dual-Ring Interconnect, page 5-17—As needed, complete this procedure after you provision an SNCP.
12. NTP-F155 Provision an Integrated SNCP Dual-Ring Interconnect, page 5-19—As needed, complete this procedure after you provision an SNCP.

13. NTP-F156 Provision a Traditional MS-SPRing/SNCP Dual-Ring Interconnect, page 5-20—As needed, complete this procedure after you provision an SNCP and MS-SPRing.
14. NTP-F157 Provision an Integrated MS-SPRing/SNCP Dual-Ring Interconnect, page 5-23—As needed, complete this procedure after you provision an SNCP and MS-SPRing.
15. NTP-F158 Provision an Open-Ended SNCP, page 5-24—As needed, complete this procedure after you provision an SNCP.
16. NTP-F159 Open-Ended SNCP Acceptance Test, page 5-26—As needed, complete this procedure after you provision an open-ended SNCP.
17. NTP-F160 Provision an ONS 15600 SDH Node as a Protection Domain Hub, page 5-28—As needed, complete this procedure to configure the ONS 15600 SDH as a hub node in a mixed protection domain for low-order traffic routing.
18. NTP-F161 Mixed Protection Domain Hub Acceptance Test, page 5-30—As needed, complete this procedure after you provision an ONS 15600 SDH node as a hub node for mixed protection domains.
19. NTP-F162 Create a Logical Network Map, page 5-33—Complete as needed.

NTP-F144 Verify Node Turn-Up

Purpose	This procedure verifies that each ONS 15600 SDH is ready for network turn-up.
Tools/Equipment	None
Prerequisite Procedures	Chapter 4, “Turn Up a Node”
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the “DLP-F181 Log into CTC” task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Complete the “DLP-F292 Single Shelf Control Card Switch Test” task on page 17-82.

Step 3 From the View menu, choose **Go To Network View**.

Step 4 Click the **Alarms** tab. Complete the following steps:

a. Verify that the alarm filter is not on. See the “DLP-F288 Disable Alarm Filtering” task on page 17-80 for instructions.

b. Verify that no critical or major alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for procedures.

Step 5 From the View menu, choose **Go To Previous View** to return to node view.

Step 6 Verify that the SW Version and Defaults that appear in the node view status area match the software version and NE defaults shown in your site plan. If either is not correct, complete the following procedures as needed:

- If the software is not the correct version, install the correct version from the ONS 15600 SDH software CD. Upgrade procedures are located on the CD. Follow the upgrade procedures appropriate to the software currently installed on the node.

- If the node defaults are not correct, refer to the “Network Element Defaults” appendix in the *Cisco ONS 15600 SDH Reference Manual.*

Step 7 Click the **Provisioning > General** tabs. Verify that all general node information settings match the settings of your site plan. If not, see the “NTP-F133 Set Up Date, Time, and Contact Information” procedure on page 4-4.

Step 8 Click the **Provisioning > Timing** tabs. Verify that timing settings match the settings of your site plan. If not, see the “NTP-F220 Inspect and Maintain the Air Filter” procedure on page 14-2.

Step 9 Click the **Provisioning > Network** tabs. Ensure that the IP settings and other CTC network access information is correct. If not, see the “NTP-F201 Change CTC Network Access” procedure on page 11-2.

Step 10 Click the **Provisioning > Protection** tabs. Verify that all protection groups have been created according to your site plan. If not, see the “NTP-F138 Create a 1+1 Protection Group” procedure on page 4-10 or the “NTP-F204 Modify or Delete Optical 1+1 Port Protection Settings” procedure on page 11-4.

Step 11 Click the **Provisioning > Security** tabs. Verify that all users have been created and their security levels match the settings indicated by your site plan. If not, see the “NTP-F206 Modify Users and Change Security” procedure on page 11-6.

Step 12 If Simple Network Management Protocol (SNMP) is provisioned on the shelf, click the **Provisioning > SNMP** tabs. Verify that all SNMP settings match the settings of your site plan. If not, see the “NTP-F207 Change SNMP Settings” procedure on page 11-6.

Step 13 Provision the network using the applicable procedure shown in the “Before You Begin” section on page 5-1.

Stop. You have completed this procedure.

NTP-F145 Provision a Point-to-Point Connection

Purpose	This procedure provisions 1+1 protected spans between two ONS 15600 SDH nodes, or between an ONS 15600 SDH and an ONS 15454 SDH node.
Tools/Equipment	PC or UNIX workstation set up for ONS 15600 SDH access
Prerequisite Procedures	NTP-F144 Verify Node Turn-Up, page 5-2
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Attach fiber from working port to working port and from protect port to protect port on the two nodes that you will provision for a point-to-point configuration.

Step 2 Complete the “DLP-F181 Log into CTC” task on page 16-34 at either node. The node view appears. If you are already logged in, continue with Step 3.

Step 3 Click the **Provisioning > Protection** tabs. Verify that 1+1 protection is created for the STM-N ports. Complete the “NTP-F138 Create a 1+1 Protection Group” procedure on page 4-10 if protection has not been created.

Note The switching direction (unidirectional versus bidirectional) and the revertive setting (nonrevertive versus revertive) must be the same at each end.

Step 4 Repeat Steps 2 and 3 for the second node.

Step 5 Verify that the working and protect ports in the 1+1 protection groups correspond to the physical fiber connections between the nodes; that is, verify that the working port in one node connects to the working port in the other node and that the protect port in one node connects to the protect port in the other node.

Step 6 Complete the "DLP-F253 Provision RS-DCC Terminations" task on page 17-46 for the working STM-N port on both point-to-point nodes. Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-F314 Provision MS-DCC Terminations" task on page 18-14.

Note Data communications channel (DCC) terminations are not provisioned on the protect port.

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

Step 7 As needed, complete the "DLP-F315 Provision a Proxy Tunnel" task on page 18-16.

Step 8 As needed, complete the "DLP-F316 Provision a Firewall Tunnel" task on page 18-17.

Step 9 Verify that timing is set up at both point-to-point nodes. If not, complete the "NTP-F137 Set Up Timing" procedure on page 4-9. If a node uses line timing, set the working STM-N as the timing source.

Step 10 Complete the "DLP-F254 Change the Service State for a Port" task on page 17-48 to put the protect STM-N ports in service at both nodes.

Step 11 Complete the "NTP-F146 Point-to-Point Network Acceptance Test" procedure on page 5-4.

Stop. You have completed this procedure.

NTP-F146 Point-to-Point Network Acceptance Test

Purpose	This procedure tests a point-to-point ONS 15600 SDH network.
Tools/Equipment	Optical power meter and fiber jumpers STM-N SONET/SDH test set Fiber cables An additional STM-N port depending on the span bandwidth at each node. These ports are required for test set connectivity. These are the ports you use as the circuit source and destination.
Prerequisite Procedures	NTP-F145 Provision a Point-to-Point Connection, page 5-3
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at one of the point-to-point nodes. The node view appears. If you are already logged in, continue with Step 2.

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

Step 3 Click the **Alarms** tab. Complete the following steps:

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 for instructions.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

c. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export alarm information.

Step 4 Click the **Conditions** tab. Complete the following steps:

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

b. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export condition data.

Step 5 On the network map, double-click the node that you logged into in Step 1.

Step 6 Create a test circuit from the login node to the other point-to-point node. Complete the "DLP-F291 Verify MS-SPRing Extension Byte Mapping" task on page 17-82. When you set the circuit state, choose **Unlocked** and check the **Apply to drop ports** check box. Choose one of the following options:

- For an STM-1 span, create a VC4 test circuit.
- For an STM-4 span, create a VC4-4c test circuit.
- For an STM-16 span, create a VC4-16c test circuit.
- For an STM-64 span, create a VC4-64c test circuit. If an STM-64 test set is not available, create a VC4-16c test circuit across an STM-64 span.

Step 7 Configure the test set for the test circuit type you created. If you are testing a VC4 circuit or a VC4-*n*c circuit on an STM-N card or port, you must have a direct optical interface to the ONS 15600 SDH. Set the test set for STM-N. For information about configuring your test set, consult your test set user guide.

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

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

Note Use an appropriately sized attenuator when connecting transmit ports to receive ports. On the long-haul optical cards such as OC48/STM16 LR/LH 16 Port 1550 and the OC192/STM64 LR/LH 4 Port 1550, use a 15-dBm attenuator; on the short-haul optical cards such as OC48/STM16 SR/SH 16 Port 1310 and OC192/STM64 SR/SH 4 Port 1310, use a 3-dBm attenuator.

Step 10 At the circuit source port:

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

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

Note Use appropriate attenuation on the test set receive connector; for more information, refer to the test set manual.

Step 11 Verify that the test set displays a clean signal. If a clean signal is not present, repeat Steps 7 through 10 to make sure the test set and cabling are configured correctly. If the problem persists, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide.*

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

Step 13 Complete the "DLP-F192 Optical 1+1 Manual Protection Switch Test" task on page 16-50.

Step 14 Set up and complete a long-term bit error rate (BER) test on the working and the protect spans. Use the existing configuration and follow your site requirements for the specified length of time. Record the test results and configuration.

Step 15 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete.

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

Step 17 Click the **Alarms** tab. Complete the following steps:

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 for instructions.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

c. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export alarm data.

Step 18 If a node fails any test, repeat the test to verify correct setup and configuration. If the test fails again, refer to the next level of support.

Step 19 Complete the "DLP-F293 Delete Circuits" task on page 17-83 to delete the test circuit.

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

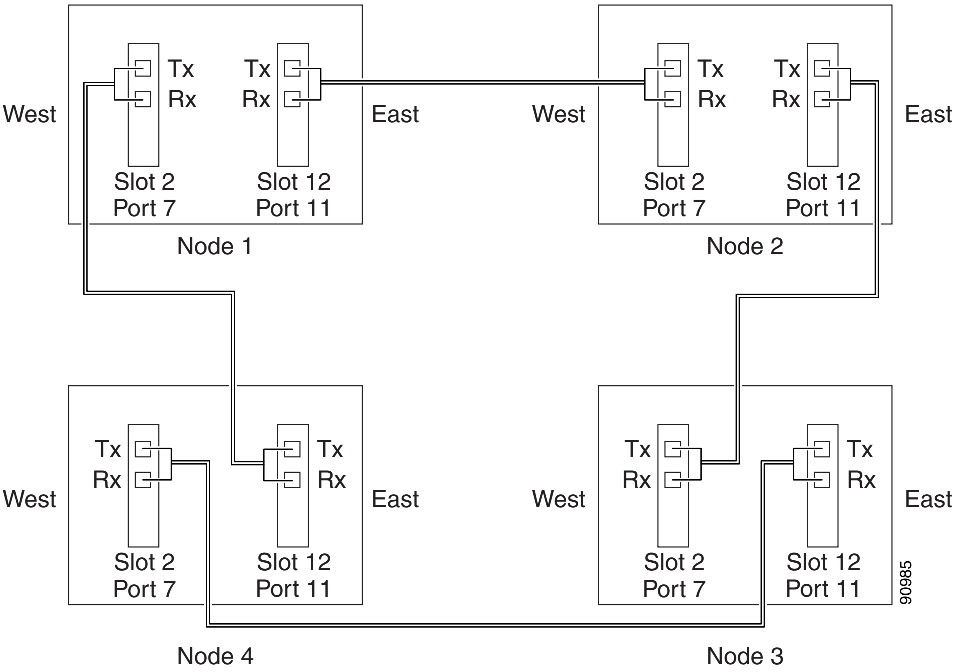
Stop. You have completed this procedure.

NTP-F147 Provision MS-SPRing Nodes

Purpose	This procedure provisions ONS 15600 SDH nodes for an MS-SPRing.
Tools/Equipment	None
Prerequisite Procedures	NTP-F144 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F349 Install Fiber-Optic Cables for MS-SPRing Configurations" task on page 18-54, verifying that the east port at one node is connected to the west port on an adjacent node, and that this east-to-west port connection is used at all MS-SPRing nodes, similar to Figure 5-1. In the figure, the STM-N drop card on the left side of the shelf is the west port, and the drop card on the right side of the shelf is considered the east port.

Figure 5-1 Four-Node, Two-Fiber MS-SPRing Fiber Connection Example



Step 2 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node that you want to configure in the MS-SPRing. If you are already logged in, continue with Step 3.

Step 3 Complete the "DLP-F253 Provision RS-DCC Terminations" task on page 17-46. Provision the two cards/ports that will serve as the MS-SPRing ports at the node.

Note If an ONS 15600 SDH is not connected to a corporate LAN, DCC provisioning must be performed through a direct (craft) connection to the node. Remote provisioning is possible only after all nodes in the network have DCCs provisioned to in-service STM-N ports.

Step 4 As needed, complete the "DLP-F315 Provision a Proxy Tunnel" task on page 18-16.

Step 5 As needed, complete the "DLP-F316 Provision a Firewall Tunnel" task on page 18-17.

Step 6 If an MS-SPRing span passes through third-party equipment that cannot transparently transport the K3 byte, complete the "DLP-F255 Remap the K3 Byte" task on page 17-49. This task is not necessary for most users.

Step 7 Repeat Steps 2 through 6 at each node that will be in the MS-SPRing. Verify that the DCC Termination Failure (EOC) and Loss of Signal (LOS) alarms are cleared after DCCs are provisioned on all nodes in the ring.

Step 8 Complete the "NTP-F148 Create an MS-SPRing" procedure on page 5-8.

Stop. You have completed this procedure.

NTP-F148 Create an MS-SPRing

Purpose	This procedure creates an MS-SPRing at each MS-SPRing-provisioned node.
Tools/Equipment	None
Prerequisite Procedures	NTP-F147 Provision MS-SPRing Nodes, page 5-6
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node on the network where you will create the MS-SPRing. If you are already logged in, continue with Step 2.

Step 2 Complete one of the following tasks:

- "DLP-F338 Create a Two-Fiber MS-SPRing Using the MS-SPRing Wizard" task on page 18-38—Use this task to create a two-fiber MS-SPRing using the CTC MS-SPRing wizard. The MS-SPRing wizard checks to see that each node is ready for MS-SPRing provisioning, then provisions all of the nodes at once. Using the MS-SPRing wizard is recommended.
- "DLP-F339 Create a Two-Fiber MS-SPRing Manually" task on page 18-40—Use this task to provision a two-fiber MS-SPRing manually at each node that will be in the MS-SPRing.

Step 3 Complete the "NTP-F149 Two-Fiber MS-SPRing Acceptance Test" procedure on page 5-8.

Stop. You have completed this procedure.

NTP-F149 Two-Fiber MS-SPRing Acceptance Test

Purpose	This procedure tests a two-fiber MS-SPRing.
Tools/Equipment	Test set and cables appropriate for the test circuit
Prerequisite Procedures	NTP-F147 Provision MS-SPRing Nodes, page 5-6 NTP-F148 Create an MS-SPRing, page 5-8
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This procedure requires that you create test circuits and perform span switches around the ring. For clarity, "Node 1" refers to the login node where you begin the procedure. "Node 2" refers to the node connected to the East STM-N trunk (span) port of Node 1. "Node 3" refers to the node connected to the East STM-N trunk port of Node 2, etc.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at one of the nodes on the MS-SPRing that you are testing. (This node will be called Node 1.) If you are already logged in, continue with Step 2.

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

Step 3 Click the **Alarms** tab. Complete the following steps:

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 for instructions.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

c. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export alarm data.

Step 4 Click the **Conditions** tab. Complete the following steps:

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

b. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export condition data.

Step 5 In network view, double-click Node 1.

Step 6 Complete the "DLP-F341 MS-SPRing Exercise Ring Test" task on page 18-42.

Step 7 Create a test circuit from Node 1 to the node connected to the east STM-N trunk port of Node 1. (This node will be called Node 2.) Complete the "DLP-F291 Verify MS-SPRing Extension Byte Mapping" task on page 17-82. When you set the circuit state, choose **Unlocked** and check the **Apply to drop ports** check box.

Step 8 Configure the test set for the test circuit type you created. If you are testing a VC4 circuit or a VC4-*nc* circuit on an STM-N card or port, you must have a direct optical interface to the ONS 15600 SDH. Set the test set for STM-N. For information about configuring your test set, consult your test set user guide.

Step 9 Verify the integrity of all patch cables that will be used in this test by connecting the test set Tx connector to the test set Rx connector. Use appropriate attenuation; for more information, refer to the test set manual. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to the next step.

Step 10 Create a physical loopback at the circuit destination port: attach one end of a patch cable to the destination port's Tx connector; attach the other end to the port's Rx connector.

Note Use an appropriately sized attenuator when connecting transmit ports to receive ports. On the long-haul optical cards such as OC48/STM16 LR/LH 16 Port 1550 and the OC192/STM64 LR/LH 4 Port 1550, use a 15-dB attenuator; on the short-haul optical cards such as OC48/STM16 SR/SH 16 Port 1310 and OC192/STM64 SR/SH 4 Port 1310, use a 3-dB attenuator.

Step 11 At the circuit source port:

a. Connect the test set Tx connector, using appropriate attenuation, to the circuit Rx connector.

b. Connect the test set Rx connector, using appropriate attenuation, to the circuit Tx connector.

Note For information about the appropriate level of attenuation, refer to the test set manual.

Step 12 Verify that the test set displays a clean signal. If a clean signal is not present, repeat Steps 7 through 11 to make sure the test set and cabling are configured correctly.

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

Step 14 Complete the "DLP-F342 MS-SPRing Switch Test" task on page 18-43 at Node 1.

Step 15 Set up and complete a BER test on the test circuit. Use the existing configuration and follow your site requirements for length of time. Record the test results and configuration.

Step 16 Complete the "DLP-F293 Delete Circuits" task on page 17-83 for the test circuit.

Step 17 Repeat Steps 5 through 16 for Nodes 2 and higher, working your way around the MS-SPRing, testing each node and span in the ring. Work your way around the MS-SPRing creating test circuits between every two consecutive nodes.

Step 18 After you test the entire ring, remove any loopbacks and test sets from the nodes.

Step 19 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application. Continue with Chapter 6, "Create Circuits."

Stop. You have completed this procedure.

NTP-F150 Provision a Traditional MS-SPRing Dual-Ring Interconnect

Purpose	This procedure provisions MS-SPRings in a traditional DRI topology. DRIs interconnect two or more MS-SPRings to provide an additional level of protection.
Tools/Equipment	None
Prerequisite Procedures	NTP-F144 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Complete the following steps if you have not provisioned the MS-SPRings that you will interconnect in an MS-SPRing DRI. If the MS-SPRings are created, go to Step 3.

a. Complete the "NTP-F147 Provision MS-SPRing Nodes" procedure on page 5-6 to provision the MS-SPRings.

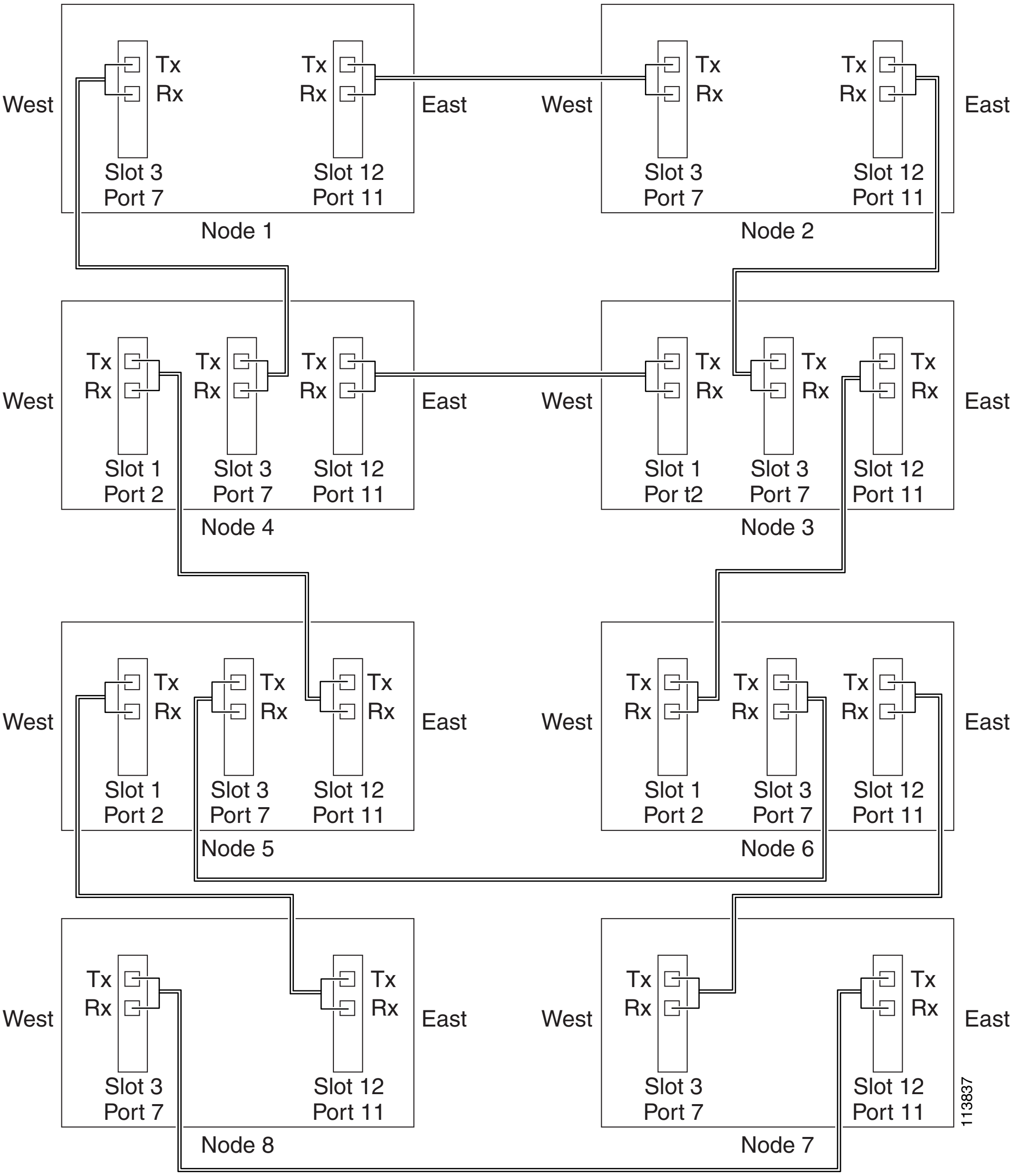
b. Complete the "NTP-F148 Create an MS-SPRing" procedure on page 5-8 to create the MS-SPRings.

c. Complete the "NTP-F149 Two-Fiber MS-SPRing Acceptance Test" procedure on page 5-8 to test two-fiber MS-SPRings.

Step 3 Verify that the MS-SPRing DRI interconnect nodes have STM-N cards installed and have fiber connections to the other interconnect nodes. The following rules apply:

- The STM-N cards that will connect the MS-SPRings must be installed at the interconnect nodes.
- The interconnect nodes must have fiber connections. Figure 5-2 shows an example of fiber connections for a traditional two-fiber MS-SPRing DRI.

Figure 5-2 Traditional Two-Fiber MS-SPRing DRI Fiber Connection Example



Stop. You have completed this procedure.

NTP-F151 Provision an Integrated MS-SPRing Dual-Ring Interconnect

Purpose	This procedure provisions MS-SPRings in an integrated DRI topology.
Tools/Equipment	None
Prerequisite Procedures	NTP-F144 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node in the MS-SPRing DRI network. If you are already logged in, continue with Step 2.

Step 2 Complete the following steps if you have not provisioned the MS-SPRings that you will interconnect in a MS-SPRing DRI. If the MS-SPRings are created, go to Step 3.

a. Complete the "NTP-F147 Provision MS-SPRing Nodes" procedure on page 5-6 to provision the MS-SPRings.

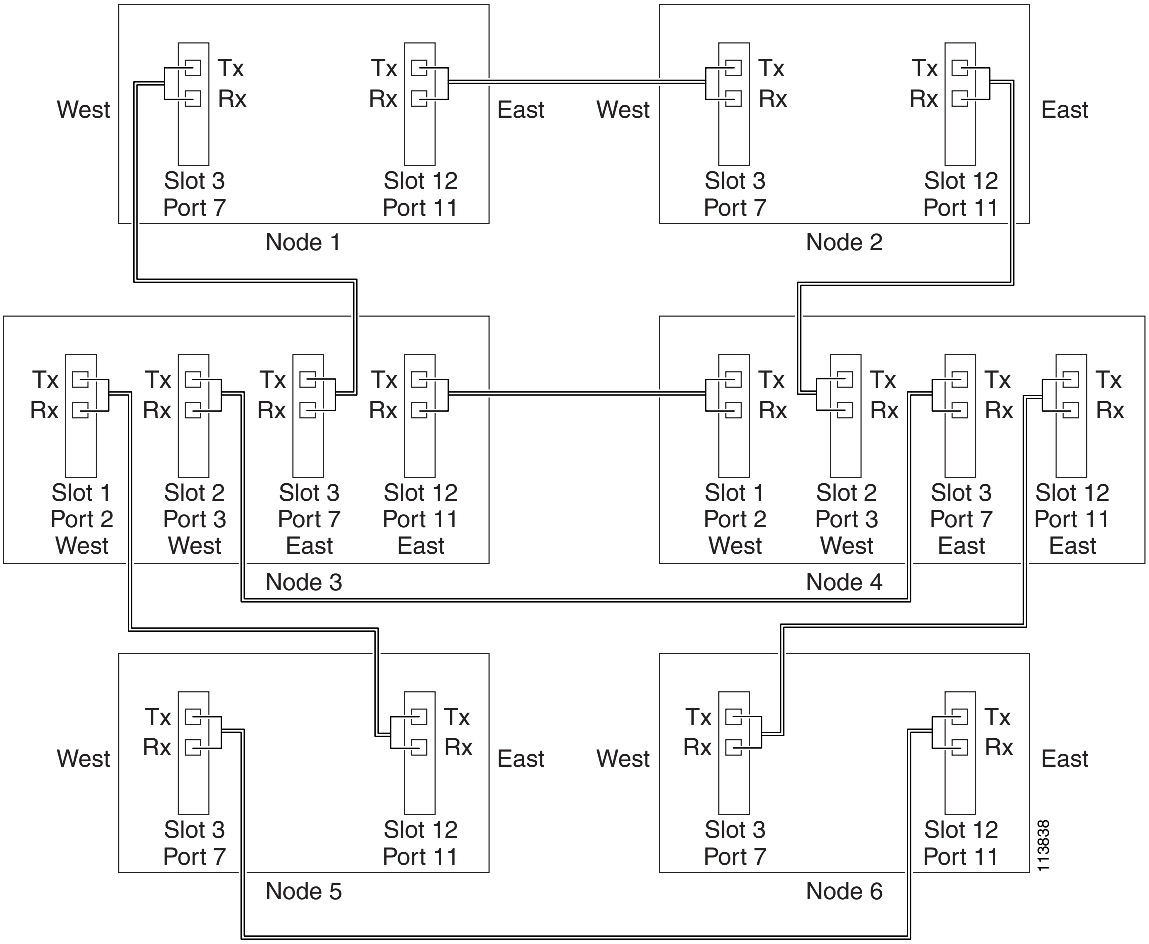
b. Complete the "NTP-F148 Create an MS-SPRing" procedure on page 5-8 to create the MS-SPRings.

c. Complete the "NTP-F149 Two-Fiber MS-SPRing Acceptance Test" procedure on page 5-8 to test two-fiber MS-SPRings.

Step 3 Verify that the MS-SPRing DRI interconnect node has STM-N cards installed and has fiber connections to the other interconnect node. The following rules apply:

- The STM-N cards that will connect the MS-SPRings must be installed at the two interconnect nodes.
- The two interconnect nodes must have the correct fiber connections. Figure 5-3 shows an example of an integrated two-fiber MS-SPRing DRI configuration.

Figure 5-3 Integrated Two-Fiber MS-SPRing DRI Example



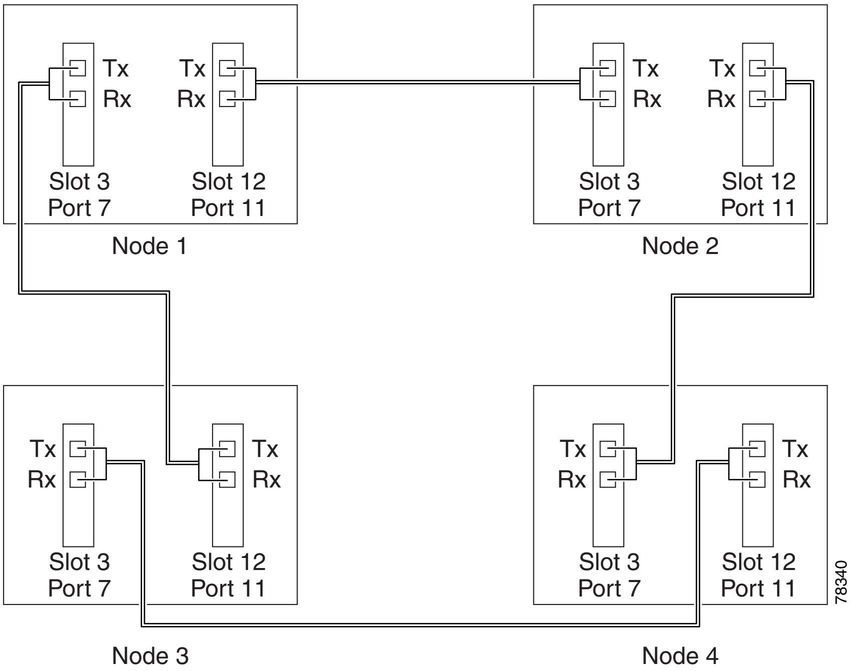
Stop. You have completed this procedure.

NTP-F152 Provision SNCP Nodes

Purpose	This procedure provisions ONS 15600 SDH nodes for an SNCP.
Tools/Equipment	None
Prerequisite Procedures	NTP-F144 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Verify that the fiber is correctly connected to the ports on the SNCP trunk (span) STM-N card. Fiber connected to an east port at one node should be connected to the west port on an adjacent node using an appropriately sized attenuator, fibered similarly to the example in Figure 5-4.

Figure 5-4 SNCP Fiber Connection Example



Step 2 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node on the SNCP that you are turning up. If you are already logged in, continue with Step 3.

Step 3 Complete the "DLP-F253 Provision RS-DCC Terminations" task on page 17-46 or the "DLP-F314 Provision MS-DCC Terminations" task on page 18-14 for the cards/ports that will host the SNCP on the node, for example, Slot 3 (STM-16)/Port 7 and Slot 12 (STM-16)/ Port 11.

Note If an ONS 15600 SDH is not connected to a corporate LAN, you must perform regenerator-section DCC (RS-DCC) or multiplex-section DCC (MS-DCC) provisioning through a local craft connection. Remote provisioning is possible only after all nodes in the network have RS-DCC or MS-DCC terminations provisioned to unlocked STM-N ports.

Step 4 Repeat Steps 2 and 3 for each node in the SNCP.

Step 5 As needed, complete the "DLP-F315 Provision a Proxy Tunnel" task on page 18-16.

Step 6 As needed, complete the "DLP-F316 Provision a Firewall Tunnel" task on page 18-17.

Step 7 If necessary, complete the "DLP-F254 Change the Service State for a Port" task on page 17-48 for all ports that you configured as RS-DCC or MS-DCC terminations. (CTC usually puts ports in service by default when you complete the DCC terminations.) Repeat this step at each node that will be in the SNCP.

Step 8 Complete the "NTP-F153 SNCP Acceptance Test" procedure on page 5-15.

Stop. You have completed this procedure.

NTP-F153 SNCP Acceptance Test

Purpose	This procedure creates drop ports at two of the nodes in the SNCP to support test set connections (source and destination ports).
Tools/Equipment	Test set and cables appropriate to the test circuit you will create.
Prerequisite Procedures	NTP-F144 Verify Node Turn-Up, page 5-2 NTP-F152 Provision SNCP Nodes, page 5-13
Required/As Needed	Required if you provisioned an SNCP
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at one of the nodes on the SNCP that you are testing. If you are already logged in, continue with Step 2.

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

Step 3 Click the **Alarms** tab. Complete the following steps:

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 for instructions.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

c. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export alarm data.

Step 4 Click the **Conditions** tab. Complete the following steps:

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

b. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export condition data.

Step 5 On the network map, double-click the node that you logged into in Step 1.

Step 6 Create a fully protected circuit as appropriate for the SNCP spans. If an STM-64 test set is not available, create an STM-16 test circuit across an STM-64 span. See the "DLP-F291 Verify MS-SPRing Extension Byte Mapping" task on page 17-82 for instructions. When you set the circuit state, choose **Unlocked** and check the **Apply to drop ports** check box.

Step 7 Configure the test set for the test circuit type you created. For information about configuring your test set, consult your test set user guide.

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

Step 9 Create a physical loopback at the circuit destination port:

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

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

Note Use an appropriately sized attenuator when connecting transmit ports to receive ports. On the long-haul optical cards such as OC48/STM16 LR/LH 16 Port 1550 and the OC192/STM64 LR/LH 4 Port 1550, use a 15-dBm attenuator; on the short-haul optical cards such as OC48/STM16 SR/SH 16 Port 1310 and OC192/STM64 SR/SH 4 Port 1310, use a 3-dBm attenuator.

Step 10 At the circuit source port:

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

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

Note Use appropriate attenuation on the test set receive connector; for more information, refer to the test set manual.

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

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

Step 13 From the View menu, choose **Go To Network View**.

Step 14 Click one of the two spans coming from the circuit source node.

Step 15 Complete the "DLP-F193 SNCP Protection Switching Test" task on page 16-51.

Although a service interruption under 60 ms might occur, the test circuit should continue to work before, during, and after the switches. If the circuit stops working, do not continue. Contact your next level of support.

Step 16 In network view, click the other circuit source span and repeat Step 15.

Step 17 Set up and complete a long-term BER test. Use the existing configuration and follow your site requirements for length of time. Record the test results and configuration.

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

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

Step 20 Click the **Alarms** tab. Complete the following steps:

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 for instructions.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

c. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export alarm data.

Step 21 Click the **Conditions** tab. Complete the following steps:

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

b. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export condition data.

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

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

Stop. You have completed this procedure.

NTP-F154 Provision a Traditional SNCP Dual-Ring Interconnect

Purpose	This procedure provisions SNCPs in a traditional DRI topology. DRIs interconnect two or more SNCPs to provide an additional level of protection.
Tools/Equipment	None
Prerequisite Procedures	NTP-F144 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Complete the following steps if you have not provisioned the SNCPs that you will interconnect in an SNCP DRI. If the SNCPs are created, go to Step 3.

a. Complete the "NTP-F152 Provision SNCP Nodes" procedure on page 5-13 to provision the SNCPs.

b. Complete the "NTP-F153 SNCP Acceptance Test" procedure on page 5-15 to test the SNCPs.

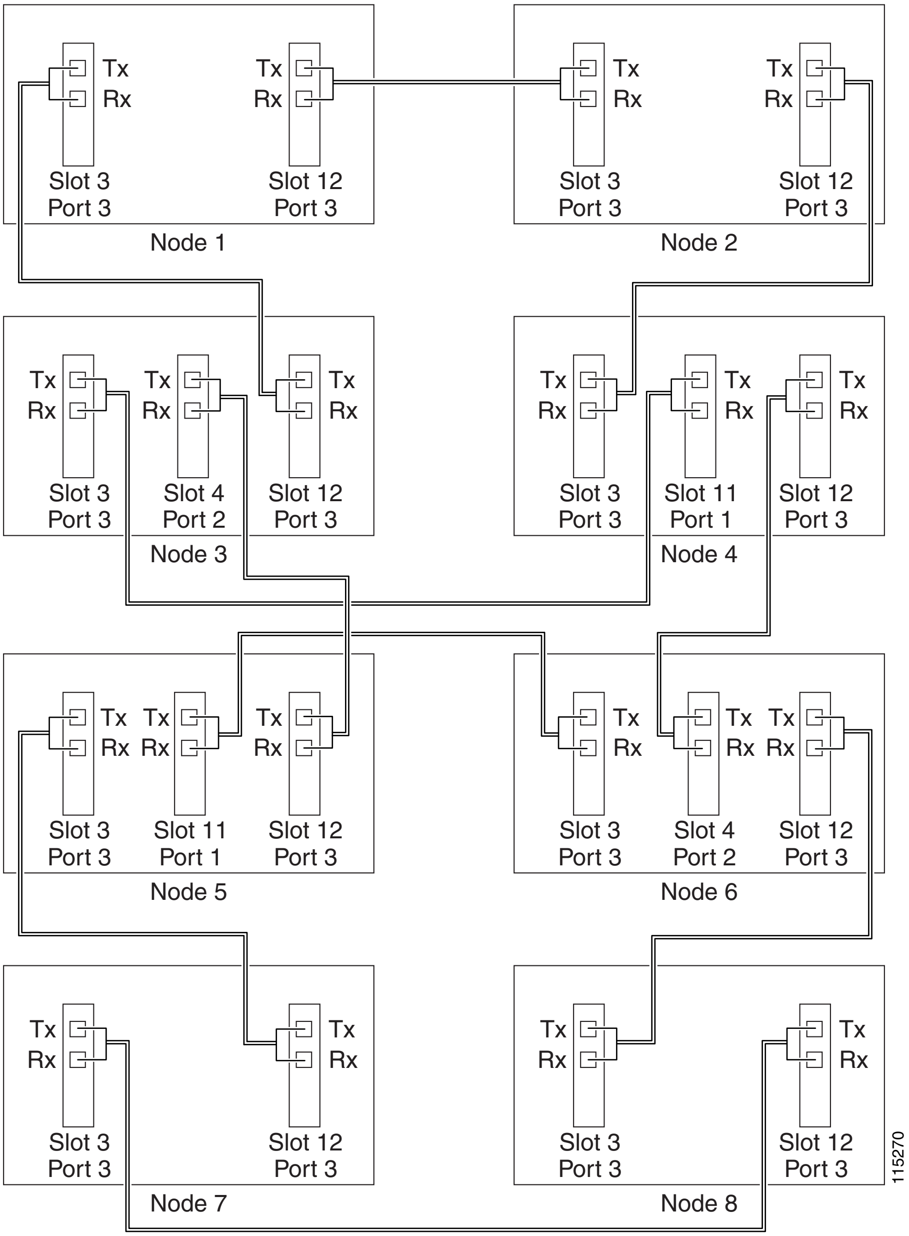
Note All SNCPs that will be interconnected must have the same STM-N rate.

Step 3 Verify that the SNCP DRI interconnect nodes have STM-N cards installed and have fiber connections to the other interconnect node. Note that:

- The STM-N cards that will connect the SNCPs must be installed at the interconnect nodes. The STM-N cards in the SNCP nodes and the interconnect nodes must be the same type.
- The interconnect nodes must have fiber connections.

An example is shown in Figure 5-5. This example shows an SNCP DRI with two rings, Nodes 1 through 4 and 5 through 8. In the example, an additional STM-N is installed in Slot 12, Port 3 at Node 4 and connected to an STM-N in Slot 4, Port 2 at Node 6. Nodes 3 and 5 are interconnected with STM-N cards in Slot 4, Port 2 (Node 3) and Slot 12, Port 3 (Node 5).

Figure 5-5 Traditional SNCP DRI Fiber Connection Example



Stop. You have completed this procedure.

NTP-F155 Provision an Integrated SNCP Dual-Ring Interconnect

Purpose	This procedure provisions SNCPs in an integrated DRI topology.
Tools/Equipment	None
Prerequisite Procedures	NTP-F144 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node in the SNCP DRI network. If you are already logged in, continue with Step 2.

Step 2 Complete the following steps if you have not provisioned the SNCPs that you will interconnect in an SNCP DRI. If the SNCPs are created, continue with Step 3.

a. Complete the "NTP-F152 Provision SNCP Nodes" procedure on page 5-13 to provision the SNCPs.

b. Complete the "NTP-F153 SNCP Acceptance Test" procedure on page 5-15 to test the SNCPs.

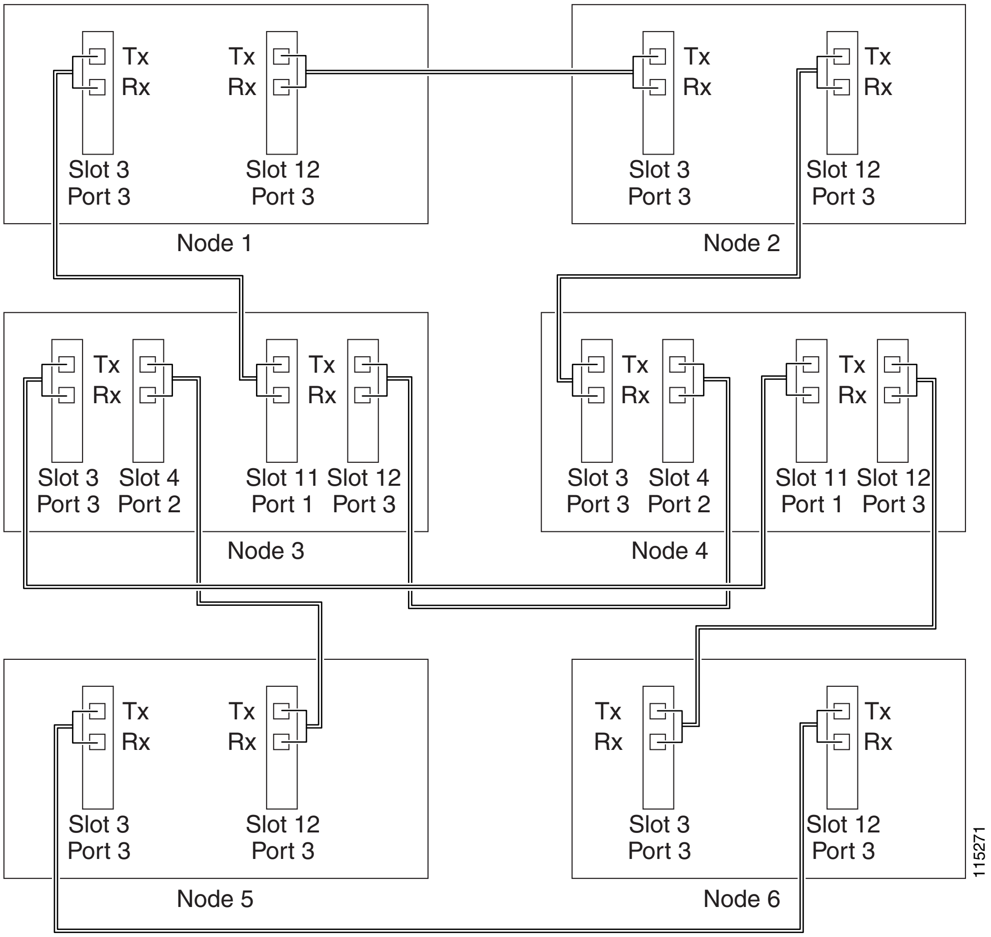
Note All SNCPs that will be interconnected must have the same STM-N rate.

Step 3 Verify that the SNCP DRI interconnect nodes have STM-N cards installed and have fiber connections to the other interconnect node. Note that:

- The STM-N cards that will connect the SNCPs must be installed at the interconnect nodes. The STM-N cards in the SNCP nodes and the interconnect nodes must be the same type.
- The interconnect nodes must have the correct fiber connections.

  An example is shown in Figure 5-6. This example shows an SNCP DRI with two rings.

Figure 5-6 Integrated SNCP DRI Example



Stop. You have completed this procedure.

NTP-F156 Provision a Traditional MS-SPRing/SNCP Dual-Ring Interconnect

Purpose	This procedure provisions an MS-SPRing and an SNCP in a traditional DRI topology. DRIs interconnect ring topologies to provide an additional level of protection.
Tools/Equipment	None
Prerequisite Procedures	NTP-F144 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Complete the following steps if you have not provisioned the MS-SPRing and SNCP that you will interconnect in a traditional DRI. If the MS-SPRing and SNCP are created, go to Step 3.

a. To provision and test the MS-SPRing, complete the following procedures:

- NTP-F147 Provision MS-SPRing Nodes, page 5-6
- NTP-F148 Create an MS-SPRing, page 5-8
- NTP-F149 Two-Fiber MS-SPRing Acceptance Test, page 5-8

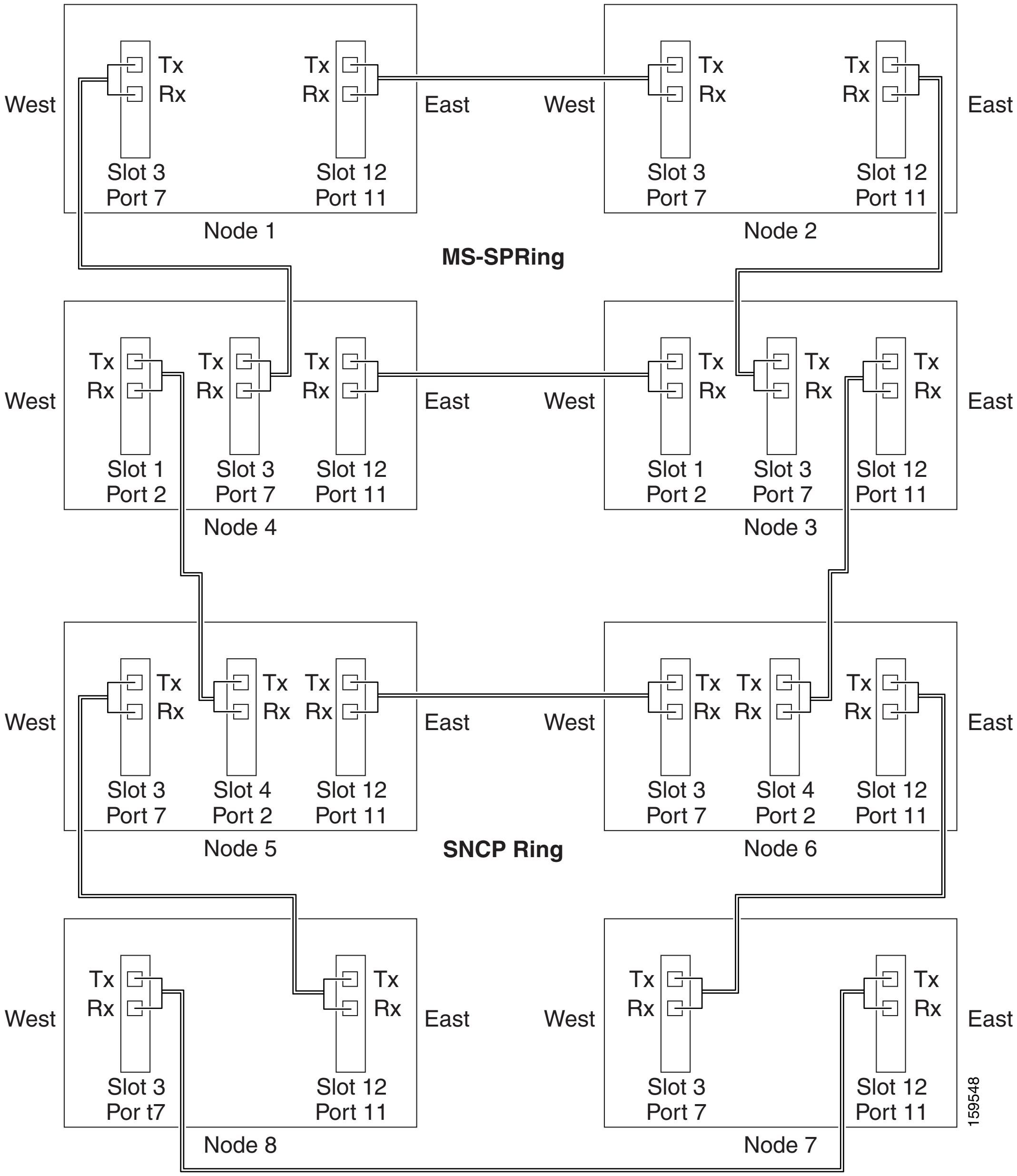
b. To provision and test the SNCP, complete the following procedures:

- NTP-F152 Provision SNCP Nodes, page 5-13
- NTP-F153 SNCP Acceptance Test, page 5-15

Step 3 Verify that the DRI interconnect nodes have STM-N cards installed and have fiber connections to the other interconnect node. Note that:

- The STM-N cards that will connect the MS-SPRing and SNCP must be installed at the interconnect nodes. The STM-N ports in the SNCP nodes and the interconnect nodes must be the same rate.
- The interconnect nodes must have fiber connections. An example is shown in Figure 5-7.

Figure 5-7 Traditional MS-SPRing to SNCP DRI Fiber Connection Example



Stop. You have completed this procedure.

NTP-F157 Provision an Integrated MS-SPRing/SNCP Dual-Ring Interconnect

Purpose	This procedure provisions an MS-SPRing and an SNCP in an integrated DRI topology.
Tools/Equipment	None
Prerequisite Procedures	NTP-F144 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node in the MS-SPRing and SNCP DRI network. If you are already logged in, continue with Step 2.

Step 2 Complete the following steps if you have not provisioned the MS-SPRing and SNCP that you will interconnect in an integrated DRI. If the MS-SPRing and SNCP are created, continue with Step 3.

a. To provision and test the MS-SPRing, complete the following procedures:

- NTP-F147 Provision MS-SPRing Nodes, page 5-6
- NTP-F148 Create an MS-SPRing, page 5-8
- NTP-F149 Two-Fiber MS-SPRing Acceptance Test, page 5-8

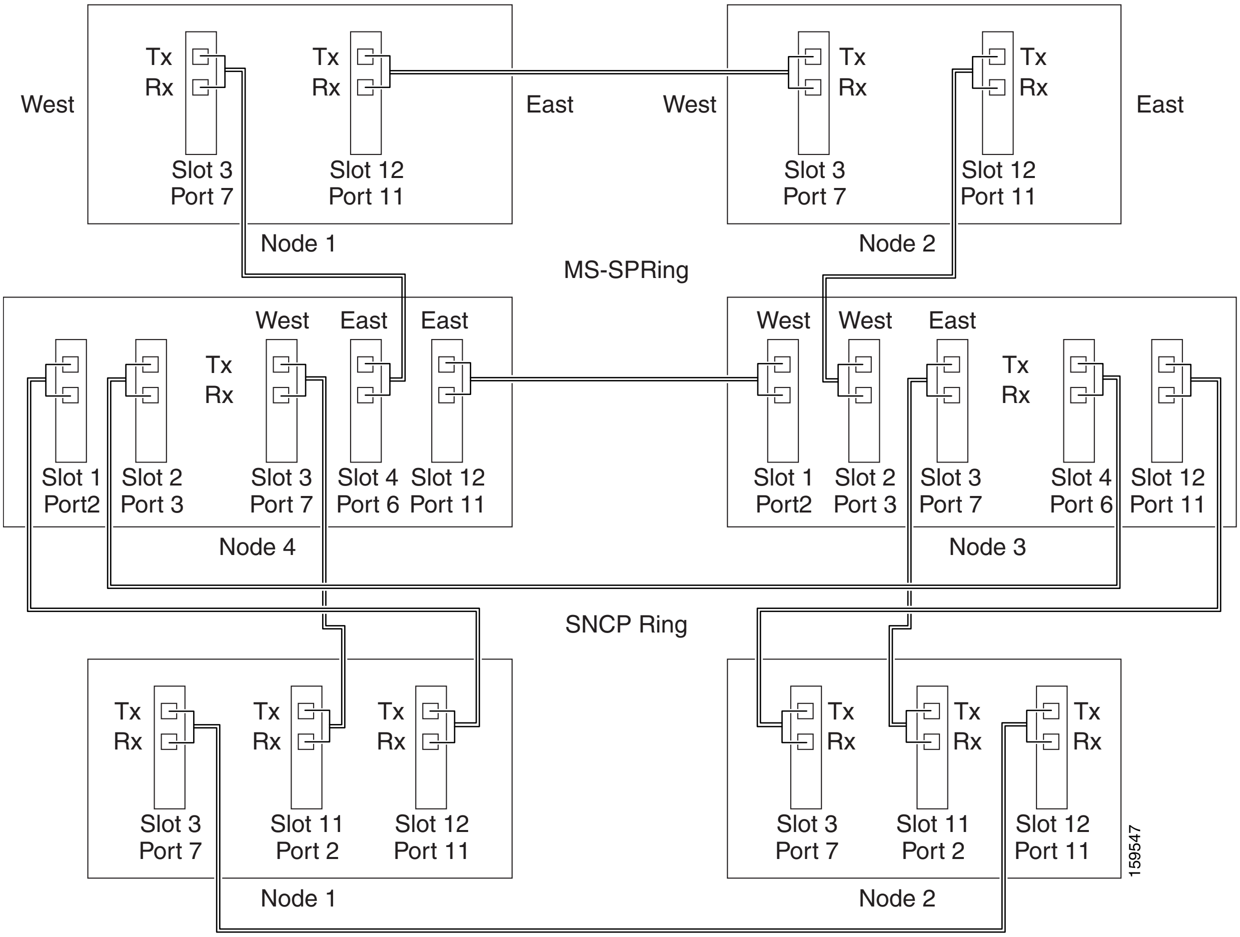
b. To provision and test the SNCP, complete the following procedures:

- NTP-F152 Provision SNCP Nodes, page 5-13
- NTP-F153 SNCP Acceptance Test, page 5-15

Step 3 Verify that the MS-SPRing and SNCP DRI interconnect nodes have STM-N cards installed and have fiber connections to the other interconnect node. Note that:

- The STM-N cards that will connect the MS-SPRing and SNCP must be installed at the interconnect nodes. The STM-N ports in the SNCP nodes and the interconnect nodes must be the same rate.
- The interconnect nodes must have the correct fiber connections. An example is shown in Figure 5-8.

Figure 5-8 Integrated MS-SPRing to SNCP DRI Example



Stop. You have completed this procedure.

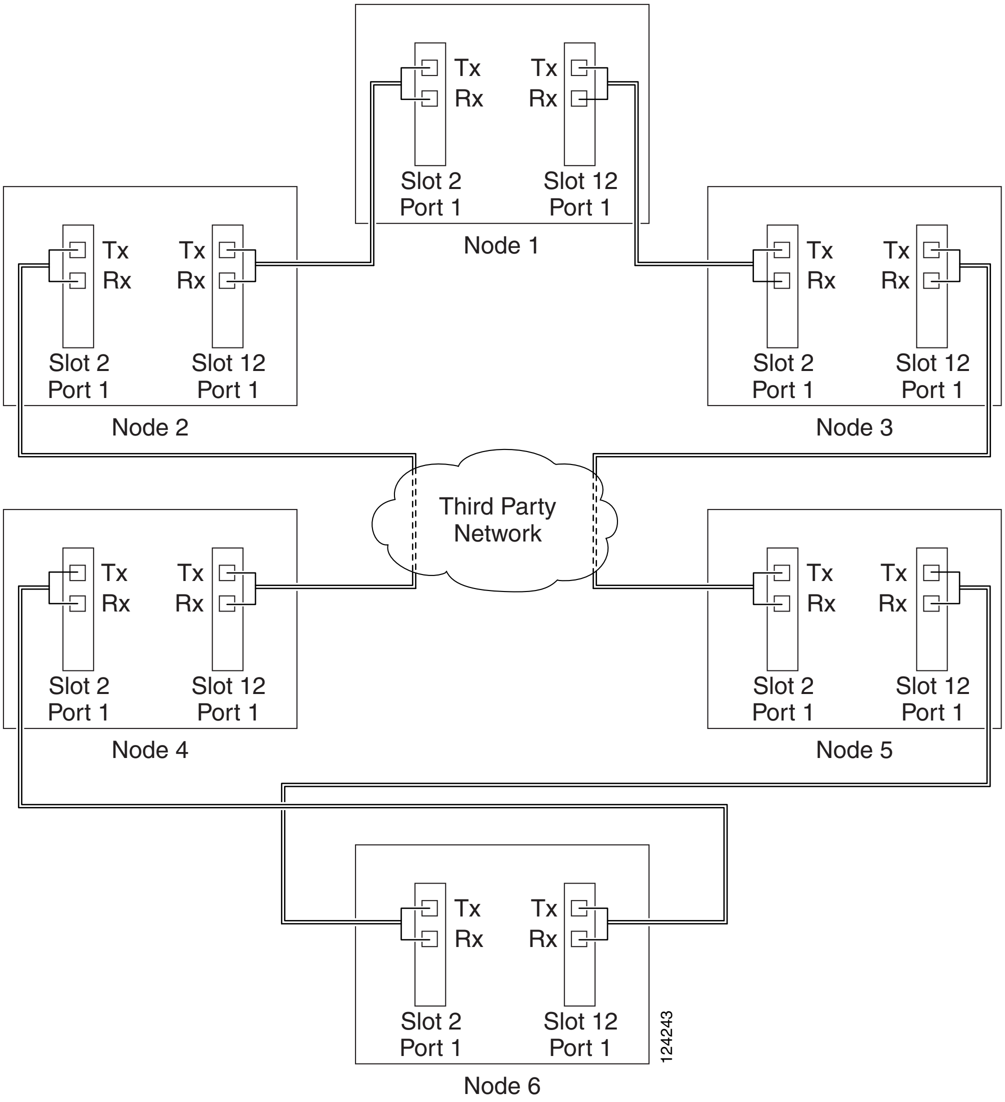
NTP-F158 Provision an Open-Ended SNCP

Purpose	This procedure provisions ONS 15600 SDHs in an open-ended SNCP connected to a third-party vendor network. This topology allows you to route a circuit from one ONS 15600 SDH network to another ONS 15600 SDH network through the third-party network. Also see the "NTP-F174 Create a Server Trail" procedure on page 6-28, which provides an alternative way to create a connection between ONS nodes through a third-party network.
Tools/Equipment	None
Prerequisite Procedures	NTP-F144 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed

Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Verify that the fiber is correctly connected to the SNCP trunk (span) STM-N cards at each open-ended SNCP node. Figure 5-9 shows an example. Node 1 is connected to ONS 15600 SDH Nodes 2 and 3 through Slots 12 and 2. Trunk cards at Nodes 2 and 3 are connected to the third-party vendor equipment.

Figure 5-9 ONS 15600 SDH Open-Ended SNCPs Fiber Connection Example



Step 2 Verify that the third-party cards or units to which the ONS 15600 SDH trunk cards are connected are the same STM-N rate as the ONS 15600 SDH trunk cards. The third-party time slots must match the ONS 15600 SDH card time slots to which they are connected. For example, if your trunk card is an STM-16, the third-party vendor card or unit must have VC4s 1 to 8 available.

Step 3 Log into an ONS 15600 SDH in the SNCP you are turning up. See the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 4.

Step 4 Complete the "DLP-F253 Provision RS-DCC Terminations" task on page 17-46 or the "DLP-F314 Provision MS-DCC Terminations" task on page 18-14 for the ONS 15600 SDH cards and ports that are connected to another ONS 15600 SDH. Do not create RS-DCC or MS-DCC terminations for the card and port that connects to the third-party equipment. For example in Figure 5-9, DCC terminations are created at the following cards and ports:

- Nodes 1 and 6: Slot 2, Port 1 and Slot 12, Port 1
- Node 2 and 5: Slot 12, Port 1
- Node 3 and 4: Slot 2, Port 1

Note If an ONS 15600 SDH is not connected to a corporate LAN, RS-DCC, or MS-DCC provisioning must be performed through a direct (craft) connection. Remote provisioning is possible only after all nodes in the network have RS-DCC or MS-DCC terminations provisioned to in-service STM-N ports.

Step 5 Repeat Steps 3 and 4 for each node in the SNCP.

Step 6 As needed, complete the "DLP-F315 Provision a Proxy Tunnel" task on page 18-16.

Step 7 As needed, complete the "DLP-F316 Provision a Firewall Tunnel" task on page 18-17.

Step 8 Following the documentation provided by the third-party vendor, provision the optical loop leading from the ONS 15600 SDH connection at one end to the ONS 15600 SDH connection at the other end. In other words, you will create an open-ended SNCP using procedures for the third-party equipment.

Step 9 Complete the "NTP-F159 Open-Ended SNCP Acceptance Test" procedure on page 5-26.

Stop. You have completed this procedure.

NTP-F159 Open-Ended SNCP Acceptance Test

Purpose	This procedure tests an open-ended SNCP.
Tools/Equipment	Test set and cables appropriate to the test circuit you will create.
Prerequisite Procedures	NTP-F158 Provision an Open-Ended SNCP, page 5-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Note Although a service interruption under 60 ms might occur, the test circuit should continue to work before, during, and after the switches. If the circuit stops working, do not continue. Contact your next level of support.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node that will be the source node for traffic traversing the third-party network. If you are already logged in, continue with Step 2.

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

Step 3 Click the **Alarms** tab. Complete the following steps:

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 for instructions.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

c. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export alarm information.

Step 4 Click the **Conditions** tab. Complete the following steps:

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

b. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export condition data.

Step 5 On the network map, double-click the node that you logged into in Step 1.

Step 6 Create a test circuit from that node to the STM-N trunk (span) cards on the nodes that connect to the third-party network. For example, in Figure 5-9 on page 5-25, a circuit is created from Node 1 to the Slot 12 STM-N card at Node 2, and a secondary circuit destination is created on the Slot 2 STM-N card at Node 3. See the "DLP-F291 Verify MS-SPRing Extension Byte Mapping" task on page 17-82 for instructions. When you set the circuit state, choose **Unlocked** and check the **Apply to drop ports** check box.

Step 7 Create a circuit within the third-party network from ONS 15600 SDH connection ports to the second set of ONS 15600 SDH connection ports on both SNCP spans. Refer to the third-party equipment documentation for circuit creation procedures.

Step 8 Repeat Step 6 to create a second circuit at the terminating node on the other side of the third-party network. In Figure 5-9, this is Node 6. However, this circuit will have two sources, one at Node 4/Slot 2, and one at Node 5/Slot 12. The destination will be a drop card on Node 6.

Step 9 Configure the test set for the test circuit type you created. For information about configuring your test set, consult your test set user guide.

Step 10 Verify the integrity of all patch cables that will be used in this test by connecting the test set Tx connector to the test set Rx connector. Use appropriate attenuation; for more information, refer to the test set manual. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to the next step.

Step 11 Create a physical loopback at the circuit destination card:

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

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

Step 12 At the circuit source card:

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

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

Step 13 Verify that the test set shows a clean signal. If a clean signal does not appear, repeat Steps 6 through 12 to make sure the test set and cabling are configured correctly.

Step 14 Inject BIT errors from the test set. To verify that you have a complete end-to-end circuit, verify that the errors appear at the test set.

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

Step 16 Click one of the two spans leaving the circuit source node.

Step 17 Complete the "DLP-F193 SNCP Protection Switching Test" task on page 16-51 to test the SNCP protection switching function on this span.

Step 18 In network view, click the other circuit source span and repeat Step 17.

Step 19 Set up and complete a BER test. Use the existing configuration and follow your site requirements for the length of time. Record the test results and configuration.

Step 20 Complete the "DLP-F293 Delete Circuits" task on page 17-83 for the test circuit.

Step 21 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete.

Step 22 Click the **Alarms** tab. Complete the following steps:

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 for instructions.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

c. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export alarm information.

Step 23 Click the **Conditions** tab. Complete the following steps:

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

b. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export condition data.

Step 24 Repeat Steps 5 through 23 for each node that will be a source or destination for circuits traversing the third-party network.

Step 25 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application. Continue with Chapter 6, "Create Circuits."

Stop. You have completed this procedure.

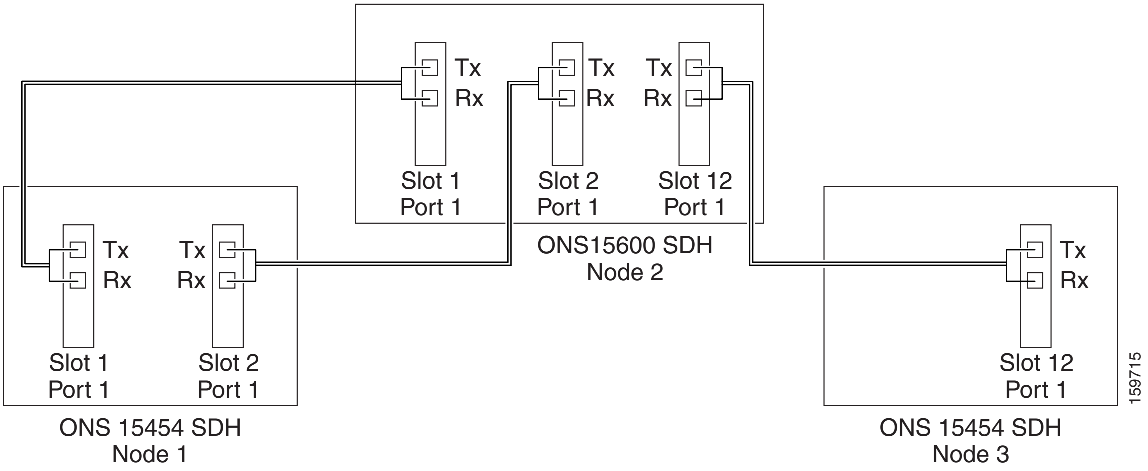
NTP-F160 Provision an ONS 15600 SDH Node as a Protection Domain Hub

Purpose	This procedure creates a network topology where the ONS 15600 SDH bridges traffic between different protection domains on ONS 15454 SDH nodes: 1+1, MS-SPRing, and SNCP. This configuration must be used when you want to create an end-to-end low-order circuit from an ONS 15454 SDH SNCP network over an ONS 15600 SDH hub node to an ONS 15454 SDH line-protected destination. For more information about routing low-order traffic over an ONS 15600 SDH hub node, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15600 SDH Reference Manual*.
Tools/Equipment	None
Prerequisite Procedures	NTP-F144 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed

Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Verify that the fiber is correctly connected to the SNCP trunk (span) STM-N cards at each open-ended SNCP node. Figure 5-10 shows a simplified example of the connections required when the ONS 15600 SDH node is set up to bridge traffic between SNCP and line-protected domains. ONS 15454 SDH Node 1 is connected to ONS 15600 SDH Node 2 through Slots 1 and 2; the fiber is set up for SNCP protection. The ONS 15600 SDH Node 2 is connected to ONS 15454 SDH Node 3 through Slots 12; the fiber is set up for 1+1 or MS-SPRing protection.

Figure 5-10 Bridging Traffic over SNCP and Line-Protected Domains Fiber Connection Example



Step 2 Log into an ONS 15600 SDH in the network you are turning up. See the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 4.

Step 3 Complete the "DLP-F253 Provision RS-DCC Terminations" task on page 17-46 or the "DLP-F314 Provision MS-DCC Terminations" task on page 18-14 for the ONS 15600 SDH cards and ports that are connected to an ONS 15454 SDH node. For example in Figure 5-10, terminations are created at the following cards and ports:

- Node 1 (SNCP): Slot 1, Port 1 and Slot 2, Port 1
- Node 2 (SNCP): Slot 1, Port 1; Slot 2, Port 1; and Slot 12, Port 1
- Node 3 (Line-protected): Slot 12, Port 1

Note If an ONS 15600 SDH is not connected to a corporate LAN, RS-DCC, or MS-DCC provisioning must be performed through a direct (craft) connection. Remote provisioning is possible only after all nodes in the network have RS-DCC or MS-DCC terminations provisioned to in-service STM-N ports.

Step 4 As needed, complete the "DLP-F315 Provision a Proxy Tunnel" task on page 18-16.

Step 5 As needed, complete the "DLP-F316 Provision a Firewall Tunnel" task on page 18-17.

Step 6 For each ONS 15600 SDH STM port in the SNCP and MS-SPRing domains and the working STM port in the 1+1 domain, complete the "DLP-F253 Provision RS-DCC Terminations" task on page 17-46. Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-F314 Provision MS-DCC Terminations" task on page 18-14.

Step 7 Complete the following steps if you have not provisioned the point-to-point network or MS-SPRing that will interconnect to the ONS 15600 SDH hub node:

a. To provision and test the point-to-point network, complete the following procedures:
   - NTP-F145 Provision a Point-to-Point Connection, page 5-3
   - NTP-F146 Point-to-Point Network Acceptance Test, page 5-4

b. To provision and test the BLSR, complete the following:
   - NTP-F147 Provision MS-SPRing Nodes, page 5-6
   - NTP-F148 Create an MS-SPRing, page 5-8
   - NTP-F149 Two-Fiber MS-SPRing Acceptance Test, page 5-8

Step 8 Complete the following to create the three circuits necessary. This step results in two circuits, a high-order open-ended circuit with a low-order circuit routed through it from the ONS 15454 SDH source to the ONS 15454 SDH destination; CTC merges the two low-order circuits created into a single circuit. Cisco recommends that you name all circuits with the same name to indicate their relationship. The circuits must be physically aligned for CTC to create the end-to-end circuit.

a. Complete the "NTP-F175 Create an Automatically Routed Open-Ended SNCP High-Order Circuit" procedure on page 6-29. You must create a TL1-like circuit.

b. Create a low-order open-ended SNCP circuit on the ONS 15454 SDH nodes that connect the ONS 15454 SDH SNCP to the ONS 15600 SDH node. You must create a TL1-like circuit. Refer to the "Create Circuits and Low-Order Tunnels" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

c. Create a two-way low-order circuit on the ONS 15454 SDH node that connects the line-protected domain to the ONS 15600 SDH node. You must create a TL1-like circuit. Refer to the "Create Circuits and Low-Order Tunnels" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Note The open-ended high-order circuit created in this step cannot be deleted if a low-order circuit traverses it.

Step 9 Complete the "NTP-F161 Mixed Protection Domain Hub Acceptance Test" procedure on page 5-30.

Stop. You have completed this procedure.

NTP-F161 Mixed Protection Domain Hub Acceptance Test

Purpose	This procedure tests whether an ONS 15600 SDH node can carry traffic across a mixed protection domain (SNCP and line-protection).
Tools/Equipment	Test set and cables appropriate to the test circuit you will create.
Prerequisite Procedures	NTP-F160 Provision an ONS 15600 SDH Node as a Protection Domain Hub, page 5-28

Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Note Although a service interruption under 60 ms might occur, the test circuit should continue to work before, during, and after the switches. If the circuit stops working, do not continue. Contact your next level of support.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node that will be the source node for the traffic traversing the mixed protection domains. If you are already logged in, continue with Step 2.

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

Step 3 Click the **Alarms** tab. Complete the following steps:

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 for instructions.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

c. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export alarm information.

Step 4 Click the **Conditions** tab. Complete the following steps:

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

b. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export condition data.

Step 5 Create a high-order test circuit from the node in the 1+1 domain to the MS-SPRing domain. For more information, see Chapter 6, "Create Circuits." Complete the following:

a. Set up two test sets or a test set and a physical loopback to verify that traffic is error free. Configure the test set for the test circuit type you created. For information about configuring your test set, consult your test set user guide.

b. Complete the "DLP-F192 Optical 1+1 Manual Protection Switch Test" task on page 16-50 to test the protection switching function on this span.

c. Complete the "DLP-F342 MS-SPRing Switch Test" task on page 18-43 to test the protection switching function on this span.

d. Complete the "DLP-F293 Delete Circuits" task on page 17-83 for the test circuit.

Step 6 Create a low-order test circuit from the node in the 1+1 domain to the MS-SPRing domain and repeat Step 5. For more information on creating low-order circuits, refer to the "Create Circuits and Low-Order Tunnels" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 7 Create a high-order test circuit from the node in the SNCP domain to the node in the 1+1 domain. For more information, see Chapter 6, "Create Circuits." Complete the following:

a. Set up two test sets or a test set and a physical loopback to verify that traffic is error free. Configure the test set for the test circuit type you created. For information about configuring your test set, consult your test set user guide.

b. Complete the "DLP-F192 Optical 1+1 Manual Protection Switch Test" task on page 16-50 to test the protection switching function on this span.

c. Complete the "DLP-F193 SNCP Protection Switching Test" task on page 16-51 to test the UPSR protection switching function on this span.

d. Complete the "DLP-F293 Delete Circuits" task on page 17-83 for the test circuit.

Step 8 Create a low-order test bidirectional circuit from the node in the SNCP domain to the to the node in the 1+1 domain and repeat Step 7. For more information about creating low-order circuits, refer to the "Create Circuits and Low-Order Tunnels" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 9 Create a high-order test circuit from the node in the SNCP domain to the node in the MS-SPRing domain. For more information, see Chapter 6, "Create Circuits." Complete the following:

a. Set up two test sets or a test set and a physical loopback to verify that traffic is error free. Configure the test set for the test circuit type you created. For information about configuring your test set, consult your test set user guide.

b. Complete the "DLP-F342 MS-SPRing Switch Test" task on page 18-43 to test the protection switching function on this span.

c. Complete the "DLP-F193 SNCP Protection Switching Test" task on page 16-51 to test the UPSR protection switching function on this span.

d. Complete the "DLP-F293 Delete Circuits" task on page 17-83 for the test circuit.

Step 10 Create a low-order test bidirectional circuit from the node in the SNCP domain to the to the node in the MS-SPRing domain and repeat Step 9. For more information about creating low-order circuits, refer to the "Create Circuits and Low-Order Tunnels" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 11 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete.

Step 12 Click the **Alarms** tab. Complete the following steps:

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 for instructions.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

c. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export alarm information.

Step 13 Click the **Conditions** tab. Complete the following steps:

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

b. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export condition data.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application. Continue with Chapter 6, "Create Circuits."

Stop. You have completed this procedure.

NTP-F162 Create a Logical Network Map

Purpose	This procedure positions nodes in the network view. This procedure allows a Superuser to create a consistent network view for all nodes on the network.
Tools	None
Prerequisite Procedures	NTP-F144 Verify Node Turn-Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

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

Step 3 Change the position of the nodes in the network view according to your site plan. To do this:

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

b. Deselect the previously selected node.

c. Repeat Step a for each node you need to position.

Step 4 On the network view map, right-click and choose **Save Node Position**.

Step 5 Click **Yes** in the **Save Node Position** dialog box.

CTC displays a progress bar and saves the new node positions.

Note Nodes on the network map can be moved by users with Retrieve, Provisioning, and Maintenance security levels, but new network views can only be saved by a Superuser. To restore the view to a previously saved version of the network map, right-click on the network view map and choose **Reset Node Position**.

Stop. You have completed this procedure.

CHAPTER 6

Create Circuits

This chapter explains how to create Cisco ONS 15600 SDH circuits and tunnels. For additional information, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* as necessary.

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

1. NTP-F163 Verify Network Turn-Up, page 6-2—Complete this procedure before you create any circuits.
2. NTP-F164 Create an Automatically Routed Optical Circuit, page 6-4—Complete as needed.
3. NTP-F165 Create a Manually Routed Optical Circuit, page 6-9—Complete as needed.
4. NTP-F166 Create a Unidirectional Optical Circuit with Multiple Drops, page 6-12—Complete as needed.
5. NTP-F167 Test Optical Circuits, page 6-16—Complete this procedure after you create circuits.
6. NTP-F168 Create a Half Circuit on an MS-SPRing or 1+1 Node, page 6-17—Complete as needed to create a half circuit using an STM-N as a destination in a multiplex section-shared protection ring (MS-SPRing) or 1+1 topology.
7. NTP-F169 Create a Half Circuit on an SNCP Node, page 6-19—Complete as needed to create a half circuit using an STM-N as a destination in a subnetwork connection protection (SNCP) ring.
8. NTP-F170 Create Overhead Circuits, page 6-21—Complete as needed.
9. NTP-F171 Create an ASAP Ethernet Circuit, page 6-22—Complete as needed.
10. NTP-F172 Test ASAP Ethernet Circuits, page 6-24—Complete as needed.
11. NTP-F173 Create a High-Order Test Circuit around the Ring, page 6-25—Complete as needed.
12. NTP-F174 Create a Server Trail, page 6-28—Complete as needed.
13. NTP-F175 Create an Automatically Routed Open-Ended SNCP High-Order Circuit, page 6-29—Complete as needed.
14. NTP-E199 Create an Overlay Ring Circuit, page 6-32—Complete as needed.

Note You cannot set up low-order circuits to terminate on an ONS 15600 SDH node. However, you can create both high-order and low-order circuits that have an ONS 15454 SDH source and destination with an ONS 15600 SDH as a pass-through node. For information on ONS 15454 SDH low-order circuit creation and tunneling, refer to the circuit chapters in the *Cisco ONS 15454 SDH Procedure Guide*. If your network includes Software Release 4.1 or earlier ONS 15454 SDH nodes, you must launch Cisco Transport Controller (CTC) from an ONS 15600 SDH node before provisioning circuits.

Note During circuit provisioning in a network that includes ONS 15600 SDHs and ONS 15454 SDHs, the ONS 15600 SDH raises a temporary unequipped path (HP-UNEQ or LP-UNEQ) alarm. The alarm clears when the circuit is complete.

Table 6-1 defines key ONS 15600 SDH circuit creation terms and options.

Table 6-1 ONS 15600 SDH Circuit Options

Circuit Option	Description
Source	The circuit source is where the circuit enters the ONS 15600 SDH network.
Destination	The circuit destination is where the circuit exits an ONS 15600 SDH network.
Automatic circuit routing	CTC routes the circuit automatically on the shortest available path based on routing parameters and bandwidth availability.
Manual circuit routing	Manual routing allows you to choose a specific path, not just the shortest path chosen by automatic routing. You can choose a specific virtual channel (VC) for each circuit segment and create circuits from work orders prepared by an operations support system (OSS) like the Telcordia Trunk Information Record Keeping System (TIRKS).

NTP-F163 Verify Network Turn-Up

Purpose	This procedure verifies that the ONS 15600 SDH network is ready for circuit provisioning.
Tools/Equipment	None
Prerequisite Procedures	Chapter 5, “Turn Up a Network”
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the “DLP-F181 Log into CTC” task on page 16-34 at a node on the network where you will create circuits. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go To Network View**. Wait for all the nodes that are part of the network to appear on the network map. (Large networks might take several minutes to display all the nodes.)

Note If this is the first time your computer has connected to this ONS 15600 SDH network, the node icons are stacked on the left side of the graphic area, possibly out of view. Use the scroll bar below the network map to display the icons. To separate the icons, press **Ctrl** and drag and drop the icon to the new location. Repeat until all the nodes are visible on the graphic area.

Step 3 Verify node accessibility. In the network view, all node icons must be either green, yellow, orange, or red.

If all network nodes do not appear after a few minutes, or if a node icon is gray with an IP address under it, do not continue. Look at the NET box in the lower right corner of the window. If it is gray, log in again, making sure not to check the Disable Network Discovery check box in the CTC Login dialog box. If problems persist, see Chapter 5, "Turn Up a Network" to review the network turn-up procedure appropriate for your network topology, or refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for troubleshooting procedures.

Step 4 Verify data communications channel (DCC) connectivity. All nodes must be connected by green lines. If lines are missing or gray, do not continue. See Chapter 5, "Turn Up a Network" and follow the network turn-up procedure appropriate for your network topology. Verify that all nodes have DCC connectivity before continuing.

Step 5 Click the **Alarms** tab to view alarm descriptions. Investigate and resolve, if necessary, all critical (red node icon) or major (orange node icon) alarms. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* to resolve alarms before continuing.

Step 6 From the View menu, choose **Go To Home View**. Verify that the node is provisioned according to your site or engineering plan:

a. View the cards in the shelf map. Verify that the ONS 15600 SDH cards appear in the specified slots.

b. Click the **Provisioning > General** tabs. Verify that the node name, contacts, date, time, and Network Time Protocol/Simple Network Time Protocol (NTP/SNTP) server IP address (if used) are correctly provisioned. If needed, make corrections using the "NTP-F133 Set Up Date, Time, and Contact Information" procedure on page 4-4.

c. Click the **Network** tab. Verify that the IP address, Subnet Mask, Default Router, and Gateway Settings are correctly provisioned. If not, make corrections using the "NTP-F135 Set Up CTC Network Access" procedure on page 4-6.

d. Click the **Protection** tab. Verify that protection groups are created as specified in your site plan. If the protection groups are not created, complete the "NTP-F138 Create a 1+1 Protection Group" procedure on page 4-10.

e. If the node is in an MS-SPRing, click the **MS-SPRing** tab. (If the node is not in an MS-SPRing, continue with Step f.) Verify that the following items are provisioned as specified in your site plan:

- MS-SPRing type (two-fiber)
- MS-SPRing ring ID and node IDs
- Ring reversion time
- East and west port assignments

If you need to make corrections, see the "NTP-F147 Provision MS-SPRing Nodes" procedure on page 5-6 for instructions.

f. Click the **Security** tab. Verify that the users and access levels are provisioned as specified. If not, see the "NTP-F132 Create Users and Assign Security" procedure on page 4-3 to correct the information.

g. If Simple Network Management Protocol (SNMP) is used, click the **SNMP** tab and verify the trap and destination information. If the information is not correct, see the "NTP-F139 Set Up SNMP" procedure on page 4-11 to correct the information.

h. Click the **Comm Channels** tab. Verify that regenerator-section DCCs (RS-DCCs) and/or multiplex-section DCCs (MS-DCCs) were created to the applicable STM-N ports. If not, go to the "DLP-F253 Provision RS-DCC Terminations" task on page 17-46 or "DLP-F314 Provision MS-DCC Terminations" task on page 18-14.

i. Click the **Timing** tab. Verify that timing is provisioned as specified. If not, go to the "NTP-F205 Change Node Timing" procedure on page 11-5 to make the changes.

j. Click the **Alarm Profiles** tab. If you provisioned optional alarm profiles, verify that the alarms are provisioned as specified. If not, see the "NTP-F194 Create, Assign, and Delete Alarm Severity Profiles" procedure on page 9-6 to change the information.

k. Verify that the network element defaults listed in the status area of the node view window are correct.

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

Step 8 Complete the appropriate circuit creation procedure from the NTP list in the "Before You Begin" section on page 6-1.

Stop. You have completed this procedure.

NTP-F164 Create an Automatically Routed Optical Circuit

Purpose	This procedure creates an automatically routed optical circuit, including VC3, VC4, or concatenated VC4-2c, VC4-3c, VC4-4c, VC4-8c, VC4-16c, or VC4-64c speed. CTC automatically routes the circuit based on the entries that you make at circuit creation and during the system load.
Tools/Equipment	None
Prerequisite Procedures	NTP-F163 Verify Network Turn-Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults, see the "Network Element Defaults" appendix in the *Cisco ONS 15600 SDH Reference Manual*.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node on the network where you will create the high-order circuit. The default (node) view appears. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-F249 Assign a Name to a Port" task on page 17-42. If not, continue with Step 3.

Step 3 If the optical ports at the source and/or destination nodes are ASAP pluggable port module (PPM) ports, complete the "NTP-F196 Manage Pluggable Port Modules on the ASAP Card" procedure on page 10-1 and set the port type to STM1, STM4, STM16, or STM 64, as necessary.

Step 4 From the View menu, choose **Go To Network View**.

Step 5 Click the **Circuits** tab, then click **Create**. In the Circuit Creation dialog box, complete the following:

- Circuit Type—Choose **VC_HO_PATH_CIRCUIT**.
- Number of Circuits—Enter the number of STM-N circuits you want to create. The default is 1. If you are creating multiple circuits with the same source and destination, you can use autoranging to create the circuits automatically.
- Auto-ranged—This check box is automatically checked when you enter more than 1 in the Number of Circuits field. Leave it checked if you are creating multiple STM-N circuits with the same source and destination and you want CTC to create the circuits automatically. Uncheck this check box if you do not want CTC to create the circuits automatically.

Step 6 Click **Next**.

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

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size: VC3, VC4, VC4-4c, VC4-8c, VC4-16c, or VC4-64c. ASAP optical ports also allow circuit sizes of VC4-2c and VC4-3c.
- Bidirectional—When checked (default), creates a two-way circuit. Leave checked for this circuit.
- Create cross-connects only (TL1-like)—Check this check box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. Also, low-order tunnels and Ethergroup sources and destinations are unavailable.
- Diagnostic—Leave unchecked.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - **Unlocked**—Puts the circuit cross-connects in the Unlocked-enabled service state.
  - **Locked,disabled**—Puts the circuit cross-connects in the Locked-enabled,disabled service state. Traffic is not passed on the circuit.
  - **Unlocked,automaticInService**—Puts the circuit cross-connects in the Unlocked-disabled,automaticInService service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to Unlocked-enabled.
  - **Locked,maintenance**—Puts the circuit cross-connects in the Locked-enabled,maintenance service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use Locked,maintenance for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to Unlocked; Unlocked,automaticInService or Locked,disabled when testing is complete. See the "DLP-F313 Change a Circuit Service State" task on page 18-13.

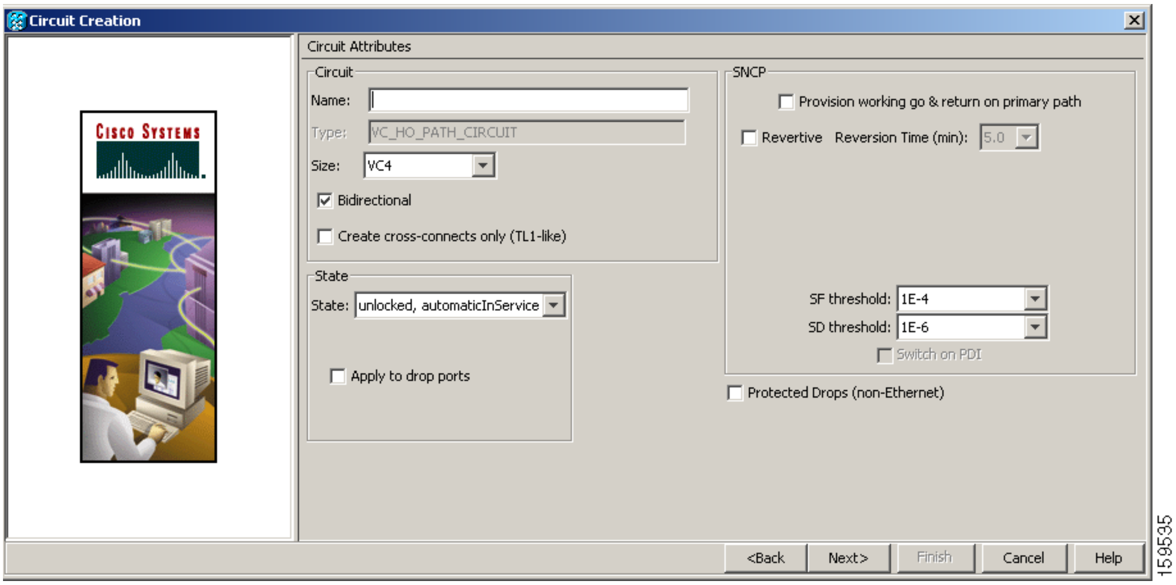
  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15600 SDH Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is

larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state of the source and destination ports.

Note If ports managed into the Unlocked administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to Unlocked-disabled,failed.

- Protected Drops—Check this check box if you want CTC to display only protected cards and ports (1+1 protection) as choices for the circuit source and destination.

Figure 6-1 Defining Circuit Attributes


Circuit Creation

Circuit Attributes

Circuit
Name:
Type: VC_HO_PATH_CIRCUIT
Size: VC4
☑ Bidirectional
□ Create cross-connects only (TL1-like)

State
State: unlocked, automaticInService
□ Apply to drop ports

SNCP
□ Provision working go & return on primary path
□ Revertive Reversion Time (min): 5.0
SF threshold: 1E-4
SD threshold: 1E-6
□ Switch on PDI

□ Protected Drops (non-Ethernet)

Step 8 If the circuit will be routed on an SNCP ring, complete the "DLP-F250 Provision SNCP Selectors During Circuit Creation" task on page 17-43.

Step 9 Click **Next**.

Step 10 Complete the "DLP-F194 Provision an Optical Circuit Source and Destination" task on page 16-52 for the optical circuit that you are creating.

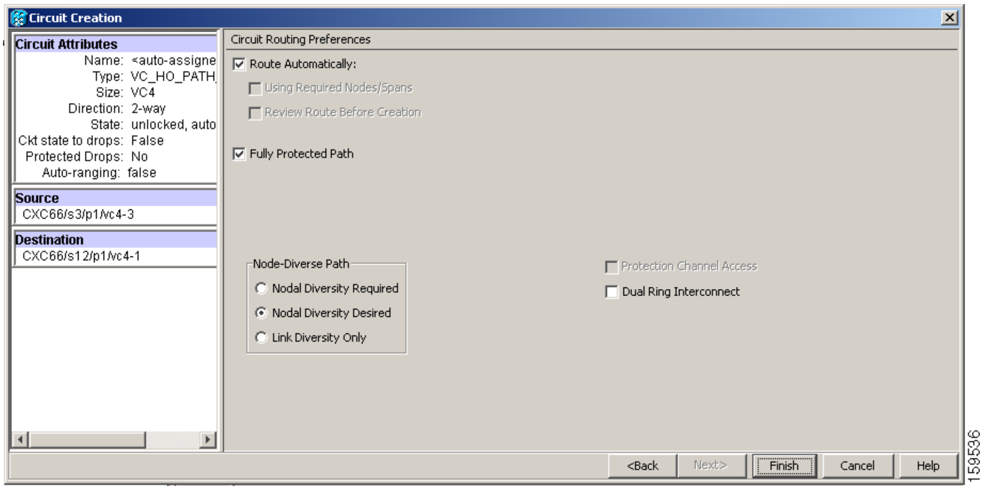
Step 11 In the Circuit Routing Preferences area (Figure 6-2), check **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- Using Required Nodes/Spans—Check this box to specify nodes and spans to include or exclude in the CTC-generated circuit route.

  Including nodes and spans for a circuit ensures that those nodes and spans are in the working path of the circuit (but not the protect path). Excluding nodes and spans ensures that the nodes and spans are not in the working or protect path of the circuit.

- Review Route Before Creation—Check this box to review and edit the circuit route before the circuit is created.

Figure 6-2 Setting Circuit Routing Preferences



Circuit Attributes
Name: <auto-assigne
Type: VC_HO_PATH
Size: VC4
Direction: 2-way
State: unlocked, auto
Ckt state to drops: False
Protected Drops: No
Auto-ranging: false

Source
CXC66/s3/p1/vc4-3

Destination
CXC66/s12/p1/vc4-1

Circuit Routing Preferences
☑ Route Automatically:
□ Using Required Nodes/Spans
□ Review Route Before Creation
☑ Fully Protected Path

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

□ Protection Channel Access
□ Dual Ring Interconnect

Step 12 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. CTC creates a fully protected circuit route based on the path diversity option you choose. Fully protected paths might or might not have SNCP path segments (with primary and alternate paths), and the path diversity options apply only to SNCP path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 17.
- To route the circuit on an MS-SPRing protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, and then continue with Step 17.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on an SNCP ring, choose one of the following:

- **Nodal Diversity Required**—Ensures that the primary and alternate paths within SNCP portions of the complete circuit path are nodally diverse.
- **Nodal Diversity Desired**—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the SNCP portion of the complete circuit path.
- **Link Diversity Only**—Specifies that only fiber-diverse primary and alternate paths for SNCP portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on an MS-SPRing DRI or SNCP DRI, check the **Dual Ring Interconnect** check box. If not, continue with Step 17.

Step 15 If you checked Dual Ring Interconnect for an SNCP ring in Step 14, complete the following substeps. If you checked Dual Ring Interconnect for an MS-SPRing, skip this step and continue with Step 16.

a. Click **Next**.

b. In the Circuit Route Constraints area, click a node or span on the circuit map.

c. Click **Include** to include the node or span in the circuit, or click **Exclude** to exclude the node/span from the circuit. The order in which you select included nodes and spans sets the circuit sequence. Click spans twice to change the circuit direction.

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

e. Review the circuit route. To change the circuit routing order, select a node beneath the Required Nodes/Lines or Excluded Nodes Links lists, then click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 16 If you checked Dual Ring Interconnect for an MS-SPRing in Step 14, complete the following substeps to assign primary and secondary nodes and ring type:

a. In the Circuit Constraints for Automatic Routing area, click **Add MS-SPRing DRI**.

b. In the confirmation dialog box, click **OK**.

c. In the Node options area of the MS-SPRing DRI Options dialog box, complete the following:

- Primary Node—For a traditional or integrated MS-SPRing-DRI, choose the node where the circuit interconnects the rings.
- Secondary Node—For a traditional or integrated MS-SPRing-DRI, choose the secondary node for the circuit to interconnect the rings. This route is used if the route on the primary node fails.
- Primary Node #2—For a traditional MS-SPRing-DRI where two primary nodes are required to interconnect rings, choose the second primary node.
- Secondary Node #2—For a traditional MS-SPRing-DRI where two secondary nodes are required, choose the second secondary node.

d. In the Ring and Path Options area, complete the following:

- The first ring is—Choose SNCP or MS-SPRing from the drop-down list.
- The second ring is—Choose SNCP or MS-SPRing from the drop-down list.
- Use ring interworking protection (RIP) on secondary path—Check this box to carry the secondary spans on the protection channels. These spans will be preempted during a ring/span switch.

e. Click **OK**. The node information appears in the Required Nodes/Lines list, and the map graphic indicates which nodes are primary and secondary.

f. In the Circuit Constraints for Automatic Routing area, click a node or span on the circuit map.

g. Click **Include** to include the node or span in the circuit, or click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans is the order in which the circuit will be routed. Click spans twice to change the circuit direction. If you are creating an SNCP to MS-SPRing traditional handoff, exclude the unprotected links from the primary node towards the secondary node. If you are creating an SNCP to MS-SPRing integrated handoff, exclude unnecessary DRIs on the SNCP segments.

h. Review the circuit constraints. To change the circuit routing order, choose a node in the Required Nodes/Lines lists and click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 17 If you selected Review Route Before Creation in Step 11, complete the following substeps; otherwise, continue with Step 18:

a. Click **Next**.

b. Review the circuit route. To add or delete a circuit span, select a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the "NTP-F165 Create a Manually Routed Optical Circuit" procedure on page 6-9 to assign the circuit route yourself.

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

- If you entered more than 1 in Number of Circuits and checked Auto-ranged, CTC automatically creates the number of circuits entered in Number of Circuits. If autoranging cannot complete all the circuits (for example, not enough bandwidth is available on the source or destination), a dialog box appears. Set the new source or destination for the remaining circuits, then click **Finish** to continue autoranging. After completing the circuit(s), the Circuits window appears.
- If you entered more than 1 in Number of Circuits and did not check Auto-ranged, the Circuit Creation dialog box appears for you to create the remaining circuits. Repeat Steps 7 through 17 for each additional circuit. After completing the circuit(s), the Circuits window appears.

Step 19 In the Circuits window, verify that the circuit(s) you created appear in the circuits list.

Step 20 Complete the "NTP-F167 Test Optical Circuits" procedure on page 6-16. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-F165 Create a Manually Routed Optical Circuit

Purpose	This procedure creates a manually routed, bidirectional or unidirectional STM-N circuit, including VC3, VC4, or concatenated VC4-2c, VC4-3c, VC4-4c, VC4-8c, VC4-16c, or VC4-64c.
Tools/Equipment	None
Prerequisite Procedures	NTP-F163 Verify Network Turn-Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node on the network where you want to create an optical circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-F249 Assign a Name to a Port" task on page 17-42. If not, continue with Step 3.

Step 3 If the optical ports at the source and/or destination nodes are ASAP PPM ports, complete the "NTP-F196 Manage Pluggable Port Modules on the ASAP Card" task on page 10-1 and set the port type to STM1, STM4, STM16 , or STM64, as necessary.

Step 4 From the View menu, choose **Go To Network View**.

Step 5 Click the **Circuits** tab, then click **Create**.

Step 6 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **VC_HO_PATH_CIRCUIT**.
- Number of Circuits—Enter the number of STM-N circuits you want to create. The default is 1.
- Auto-ranged—Applies to automatically routed circuits only. If you entered more than 1 in the Number of Circuits field, uncheck this box. (The box is unavailable if only one circuit is entered in Number of Circuits.)

Step 7 Click **Next**.

Step 8 Define the circuit attributes (Figure 6-1 on page 6-6):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size: VC3, VC4, VC4-4c, VC4-8c, VC4-16c, or VC4-64c. ASAP optical ports also allow circuit sizes of VC4-2c and VC4-3c.
- Bidirectional—Leave checked (default) for this circuit. When checked, CTC creates a two-way circuit.
- Create cross-connects only (TL1-like)—Check this check box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. Also, low-order tunnels and Ethergroup sources and destinations are unavailable.
- Diagnostic—Leave unchecked.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - **Unlocked**—Puts the circuit cross-connects in the Unlocked-enabled service state.
  - **Locked,disabled**—Puts the circuit cross-connects in the Locked-enabled,disabled service state. Traffic is not passed on the circuit.
  - **Unlocked,automaticInService**—Puts the circuit cross-connects in the Unlocked-disabled,automaticInService service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to Unlocked-enabled.
  - **Locked,maintenance**—Puts the circuit cross-connects in the Locked-enabled,maintenance service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use Locked,maintenance for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to Unlocked; Unlocked,automaticInService; or Locked,disabled when testing is complete. See the "DLP-F313 Change a Circuit Service State" task on page 18-13. For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15600 SDH Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state of the source and destination ports.

  Note If ports managed into the Unlocked administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to Unlocked-disabled,failed.

- Protected Drops—If selected, CTC displays only protected cards and ports (1+1 protection) as choices for the circuit source and destination.

Step 9 If the circuit will be routed on an SNCP ring, complete the "DLP-F250 Provision SNCP Selectors During Circuit Creation" task on page 17-43.

Step 10 Click **Next**.

Step 11 Complete the "DLP-F194 Provision an Optical Circuit Source and Destination" task on page 16-52 for the STM-N circuit you are creating.

Step 12 In the Circuit Routing Preferences area (Figure 6-2 on page 6-7), uncheck **Route Automatically**.

Step 13 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 14.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 18.
- To route the circuit on an MS-SPRing protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, and then continue with Step 18.

Caution Circuits routed on MS-SPRing protection channels are not protected and are preempted during MS-SPRing switches.

Step 14 If you selected Fully Protected Path in Step 13 and the circuit will be routed on an SNCP ring, choose one of the following:

- **Nodal Diversity Required**—Ensures that the primary and alternate paths within the SNCP ring portions of the complete circuit path are nodally diverse.
- **Nodal Diversity Desired**—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the SNCP ring portion of the complete circuit path.
- **Link Diversity Only**—Specifies that only fiber-diverse primary and alternate paths for SNCP ring portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 15 If you selected Fully Protected Path in Step 13 and the circuit will be routed on an MS-SPRing DRI or SNCP DRI, check the **Dual Ring Interconnect** check box.

Step 16 Click **Next**. In the Route Review/Edit area, node icons appear for you to route the circuit manually. The green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit. If you checked Dual Ring Interconnect for MS-SPRing, continue with Step 17. If you did not check Dual Ring Interconnect, continue with Step 18.

Step 17 If you checked Dual Ring Interconnect in Step 15 for an MS-SPRing DRI, complete the following substeps to assign primary and secondary nodes and ring type.

a. In the Route/Review Edit area, click the **MS-SPRing-DRI Nodes** tab.

b. Click **Add MS-SPRing DRI**.

c. In the Node options area of the MS-SPRing DRI Options dialog box, complete the following:

- Primary Node—For a traditional or integrated MS-SPRing-DRI, choose the node where the circuit interconnects the rings.
- Secondary Node—For a traditional or integrated MS-SPRing-DRI, choose the secondary node for the circuit to interconnect the rings. This route is used if the route on the primary node fails.
- Primary Node #2—For a traditional MS-SPRing-DRI where two primary nodes are required to interconnect rings, choose the second primary node.
- Secondary Node #2—For a traditional MS-SPRing-DRI where two secondary nodes are required, choose the second secondary node.

d. Click **OK**.

e. Review the circuit constraints. To change the circuit routing order, choose a node in the Required Nodes/Lines lists and click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

f. Click the **Included Spans** tab, and continue with Step 18.

Step 18 Complete the "DLP-F343 Provision an STM-N Circuit Route" task on page 18-47.

Step 19 Click **Finish**. If the path does not meet the specified path diversity requirement, an error message appears and allows you to change the circuit path. If you entered more than 1 in the Number of circuits field, the Circuit Creation dialog box appears after the circuit is created so you can create the remaining circuits. Repeat Steps 8 through 18 for each additional circuit.

When provisioning a protected circuit, you only need to select one path of 1+1 spans from the source to the drop. If you select unprotected spans as part of the path, select two different paths for the unprotected segment of the path.

Step 20 When all the circuits are created, the main Circuits window appears. Verify that the circuit(s) you created appear in the window.

Step 21 Complete the "NTP-F167 Test Optical Circuits" procedure on page 6-16.

Stop. You have completed this procedure.

NTP-F166 Create a Unidirectional Optical Circuit with Multiple Drops

Purpose	This procedure creates a unidirectional STM-N circuit with multiple traffic drops (circuit destinations). The ONS 15600 SDH supports up to 2048 1:2 nonblocking broadcast connections or up to 682 1:*n* (where *n* is less than or equal to 8) nonblocking broadcast connections.
Tools/Equipment	None
Prerequisite Procedures	NTP-F163 Verify Network Turn-Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node on the network where you will create the optical circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-F249 Assign a Name to a Port" task on page 17-42. If not, continue with Step 3.

Step 3 If the optical ports at the source and/or destination nodes are ASAP PPM ports, complete the "NTP-F196 Manage Pluggable Port Modules on the ASAP Card" procedure on page 10-1 and set the port type to STM1, STM4, STM16, or STM 64 as necessary.

Step 4 From the View menu, choose **Go To Network View**.

Step 5 Click the **Circuits** tab, then click **Create**.

Step 6 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **VC_HO_PATH_CIRCUIT**.

- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable when the Number of Circuits field is 1.

Step 7 Click **Next**.

Step 8 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size: VC3, VC4, VC4-4c, VC4-8c, VC4-16c, or VC4-64c. ASAP optical ports also allow circuit sizes of VC4-2c and VC4-3c.
- Bidirectional—Uncheck this box for this circuit.
- Create cross-connects only (TL1-like)—Check this check box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. Also, low-order tunnels and Ethergroup sources and destinations are unavailable.
- Diagnostic—Leave unchecked.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - **Unlocked**—Puts the circuit cross-connects in the Unlocked-enabled service state.
  - **Locked,disabled**—Puts the circuit cross-connects in the Locked-enabled,disabled service state. Traffic is not passed on the circuit.
  - **Unlocked,automaticInService**—Puts the circuit cross-connects in the Unlocked-disabled,automaticInService service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to Unlocked-enabled.
  - **Locked,maintenance**—Puts the circuit cross-connects in the Locked-enabled,maintenance service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use Locked,maintenance for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to Unlocked; Unlocked,automaticInService; or Locked,disabled when testing is complete. See the "DLP-F313 Change a Circuit Service State" task on page 18-13. For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15600 SDH Reference Manual.*
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state of the source and destination ports.

  Note If ports managed into the Unlocked administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to Unlocked-disabled,failed.

- Protected Drops—Check this box if you want the circuit routed to only protect drops. If you check this box, CTC displays only protected cards as source and destination choices.

Step 9 If the circuit will be routed on an SNCP ring, complete the "DLP-F250 Provision SNCP Selectors During Circuit Creation" task on page 17-43.

Step 10 Click **Next**.

Step 11 Complete the "DLP-F194 Provision an Optical Circuit Source and Destination" task on page 16-52 for the circuit you are creating.

Step 12 In the Circuit Routing Preferences area, uncheck **Route Automatically**. When unchecked, the Using Required Nodes/Spans and Review Route Before Circuit Creation check boxes are not available.

Step 13 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 14. Fully protected paths might or might not have SNCP ring path segments (with primary and alternate paths), and the path diversity options apply only to SNCP ring path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 16.
- To route the circuit on an MS-SPRing protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, and then continue with Step 16.

Caution Circuits routed on MS-SPRing protection channels are not protected and are preempted during MS-SPRing switches.

Step 14 If you selected Fully Protected Path in Step 13, choose one of the following:

- **Nodal Diversity Required**—Ensures that the primary and alternate paths within the SNCP ring portions of the complete circuit path are nodally diverse.
- **Nodal Diversity Desired**—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the SNCP ring portion of the complete circuit path.
- **Link Diversity Only**—Specifies that only fiber-diverse primary and alternate paths for SNCP ring portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Note For manually routed circuits, CTC checks your manually provisioned path against the path diversity option you choose. If the path does not meet the path diversity requirement that is specified, CTC displays an error message.

Step 15 If you selected Fully Protected Path in Step 13 and the circuit will be routed on an SNCP DRI, check the **Dual Ring Interconnect** check box.

Step 16 Click **Next**. In the Route Review and Edit area, node icons appear so you can route the circuit manually. The green arrows pointing from the selected node to other network nodes indicate spans that are available for routing the circuit.

Step 17 Complete the "DLP-F343 Provision an STM-N Circuit Route" task on page 18-47.

Note When provisioning a protected circuit, you only need to select one 1+1 span paths from the source to the drop. If you select unprotected spans as part of the path, you must provision both the working and protect paths.

Step 18 Click **Finish**. After completing the circuit, the Circuits window appears.

Step 19 In the Circuits window, click the circuit that you want to route to multiple drops. The Delete, Edit, and Search radio buttons become active.

Step 20 Click **Edit**. The Edit Circuit window appears with the General tab selected. All nodes in the DCC network appear on the network. Circuit source and destination information appears under the source and destination nodes. To display a detailed view of the circuit, click **Show Detailed Map**. You can rearrange the node icons by selecting the node with the left mouse button, pressing **Ctrl**, and dragging the icon to the new location.

Step 21 In the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops appears.

Step 22 Click **Create**.

Step 23 In the Define New Drop dialog box, define the new drop:

a. Node—Choose the target node for the circuit drop.

b. Slot—Choose the target card and slot.

c. Port, VC—Choose the port and/or VC from the Port and VC drop-down lists. The choice in these lists depends on the card selected in Step b.

d. The routing preferences for the new drop will match those of the original circuit. However, you can modify the following:

- If the original circuit was routed on a protected path, you can change the nodal diversity options: Nodal Diversity Required, Nodal Diversity Desired, or Link Diversity Only. See Step 14 for options descriptions.
- If the original circuit was not routed on a protected path, the Protection Channel Access option is available. See Step 13 for a description of the PCA option.

e. Click **OK**. The new drop appears in the Drops list.

Step 24 If you need to create additional drops on the circuit, repeat Steps 21 through 23.

Step 25 Click **Close**. The Circuits window appears.

Step 26 Verify that the new drops appear under the Destination column for the circuit you edited. If they do not appear, repeat Steps 21 through 25 while verifying that all options are provisioned correctly.

Step 27 Complete the "NTP-F167 Test Optical Circuits" procedure on page 6-16.

Stop. You have completed this procedure.

NTP-F167 Test Optical Circuits

Purpose	This procedure tests the first optical circuit created on the source or destination port.
Tools/Equipment	Test set capable of optical speeds, appropriate fibers, and attenuators
Prerequisite Procedures	This procedure assumes you completed facility loopback tests to test the fibers and cables from the source and destination ONS 15600 SDHs to the fiber distribution panel or the DSX. If this has not been done, do so now. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*. In addition, you must complete one of the following procedures: • NTP-F164 Create an Automatically Routed Optical Circuit, page 6-4 • NTP-F165 Create a Manually Routed Optical Circuit, page 6-9
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution You cannot disconnect fibers and connect test sets if the circuit is carrying traffic.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the source node. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-F313 Change a Circuit Service State" task on page 18-13 to set the circuit and circuit ports to the Locked-enabled,maintenance service state.

Step 3 Set up the loopback cable at the destination node:

a. Test the loopback cable by connecting one end to the test set transmit (Tx) port and the other end to the test set receive (Rx) port. Use appropriate attenuation; for information on attenuation, refer to the test set manual. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly.

b. Install the loopback cable on the port you are testing. Connect the Tx connector to the Rx connector of the port being tested.

Note Use an appropriately sized attenuator when connecting transmit ports to receive ports. On the long-reach optical cards, use a 15 dB attenuator; on the short-reach optical cards, use a 3 dB attenuator.

Step 4 Set up the loopback cable at the source node:

a. Test the loopback cable by connecting one end to the test set Tx port and the other end to the test set Rx port. Use appropriate attenuation; for more information, refer to the test set manual. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly.

b. At the source node, attach the loopback cable to the port you are testing. Connect the Tx port of the test set to the circuit Rx port, and the test set Rx port to the circuit Tx port.

Note Use an appropriately sized attenuator when connecting transmit ports to receive ports. On the long-reach optical cards (OC48/STM16 LR/LH 16 Port 1550 and the OC192/STM64 LR/LH 4 Port 1550), use a 15 dB attenuator; on the short-reach optical cards (OC48/STM16 SR/SH 16 Port 1310 and OC192/STM64 SR/SH 4 Port 1310), use a 3 dB attenuator.

Step 5 Configure the test set for the source STM-16 or STM-64 ONS 15600 SDH card. For information about configuring your test set, consult your test set user guide.

Step 6 Verify that the test set displays a clean signal. If a clean signal is not present, repeat Steps 2 through 5 to make sure you have configured the test set and cabling correctly.

Step 7 Inject errors from the test set. Verify that the errors appear at the source and destination nodes.

Step 8 Clear the performance monitoring (PM) parameters for the ports that you tested. See the "DLP-F213 Clear Selected PM Counts" task on page 17-12 for instructions.

Step 9 Perform protection switch testing appropriate to the SDH topology:

- For MS-SPRings, see the "DLP-F342 MS-SPRing Switch Test" task on page 18-43.
- For SNCP rings, see the "DLP-F193 SNCP Protection Switching Test" task on page 16-51.

Step 10 Perform a bit error rate (BER) test for 12 hours or according to site specification. For information about configuring your test set for BER testing, see your test set user guide.

Step 11 After the BER test is complete, print the results or save them to a disk for future reference. For information about printing or saving test results, see your test set user guide.

Step 12 Complete the "DLP-F313 Change a Circuit Service State" task on page 18-13 to change the circuit and circuit ports from the Locked-enabled,maintenance service state to their previous service states.

Stop. You have completed this procedure.

NTP-F168 Create a Half Circuit on an MS-SPRing or 1+1 Node

Purpose	This procedure creates an STM-N circuit from a drop card to an STM-N trunk card on the same node in an MS-SPRing or 1+1 topology.
Tools/Equipment	None
Prerequisite Procedures	NTP-F163 Verify Network Turn-Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node on the network where you will create the half circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-F249 Assign a Name to a Port" task on page 17-42. If not, continue with Step 3.

Step 3 If the ports at the source and/or destination nodes are ASAP PPM ports, complete the "NTP-F196 Manage Pluggable Port Modules on the ASAP Card" procedure on page 10-1.

Step 4 From the View menu, choose **Go To Network View**.

Step 5 Click the **Circuits** tab, then click **Create**.

Step 6 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **VC_HO_PATH_CIRCUIT**.
- Number of circuits—Enter the number of circuits you want to create. The default is 1.
- Auto-ranged—Uncheck this check box; it is automatically selected if you enter more than 1 in the Number of Circuits field.

Step 7 Click **Next**.

Step 8 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose **VC4**.
- Bidirectional—Leave checked for this circuit (default).
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. Also, low-order tunnels and Ethergroup sources and destinations are unavailable.
- Diagnostic—Leave unchecked.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - **Unlocked**—Puts the circuit cross-connects in the Unlocked-enabled service state.
  - **Locked,disabled**—Puts the circuit cross-connects in the Locked-enabled,disabled service state. Traffic is not passed on the circuit.
  - **Unlocked,automaticInService**—Puts the circuit cross-connects in the Unlocked-disabled,automaticInService service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to Unlocked-enabled.
  - **Locked,maintenance**—Puts the circuit cross-connects in the Locked-enabled,maintenance service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use Locked,maintenance for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to Unlocked; Unlocked,automaticInService or Locked,disabled when testing is complete. See the "DLP-F313 Change a Circuit Service State" task on page 18-13. For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15600 SDH Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state of the source and destination ports.

Note If ports managed into the Unlocked administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to Unlocked-disabled,failed.

- Protected Drops—Uncheck this box.

Step 9 Click **Next**.

Step 10 Complete the "DLP-F251 Provision a Half Circuit Source and Destination on an MS-SPRing or 1+1 Protection Group" task on page 17-44.

Step 11 Click **Finish**. One of the following results occurs, depending on the circuit properties you chose in the Circuit Creation dialog box:

- If you entered more than 1 in the Number of circuits field and checked Auto-ranged, CTC automatically creates the number of circuits entered in Number of circuits. If autoranging cannot complete all the circuits, for example, because sequential ports are unavailable at the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click **Finish** to continue autoranging. After completing the circuit(s), the Circuits window appears.
- If you entered more than 1 in the Number of circuits field and did not check Auto-ranged, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 6 through 10 for each additional circuit. After completing the circuit(s), the Circuits window appears.

Step 12 In the Circuits window, verify that the new circuits appear in the circuits list.

Step 13 Complete the "NTP-F167 Test Optical Circuits" procedure on page 6-16. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-F169 Create a Half Circuit on an SNCP Node

Purpose	This procedure creates an STM-N circuit from a drop card to an STM-N line card on the same SNCP node.
Tools/Equipment	None
Prerequisite Procedures	NTP-F163 Verify Network Turn-Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-F249 Assign a Name to a Port" task on page 17-42. If not, continue with Step 3.

Step 3 If the ports at the source and/or destination nodes are ASAP PPM ports, complete the "NTP-F196 Manage Pluggable Port Modules on the ASAP Card" procedure on page 10-1.

Step 4 From the View menu, choose **Go To Network View**.

Step 5 Click the **Circuits** tab, then click **Create**.

Step 6 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **VC_HO_PATH_CIRCUIT**.
- Number of Circuits—Enter the number of circuits you want to create. The default is 1.

- Auto-ranged—Uncheck this check box; it is automatically selected if you enter more than 1 in the Number of Circuits field.

Step 7 Click **Next**.

Step 8 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose VC3, VC4, VC4-4c, VC4-8c, VC4-16c, or VC4-64c. ASAP optical ports also allow circuit sizes of VC4-2c and VC4-3c.
- Bidirectional—Leave checked for this circuit (default).
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits.
- Diagnostic—Leave unchecked.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - **Unlocked**—Puts the circuit cross-connects in the Unlocked-enabled service state.
  - **Locked,disabled**—Puts the circuit cross-connects in the Locked-enabled,disabled service state. Traffic is not passed on the circuit.
  - **Unlocked,automaticInService**—Puts the circuit cross-connects in the Unlocked-disabled,automaticInService service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to Unlocked-enabled.
  - **Locked,maintenance**—Puts the circuit cross-connects in the Locked-enabled,maintenance service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use Locked,maintenance for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to Unlocked; Unlocked,automaticInService; or Locked,disabled when testing is complete. See the "DLP-F313 Change a Circuit Service State" task on page 18-13. For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15600 SDH Reference Manual*.
- Apply to drop ports—Check this box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC will apply the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the box is unchecked, CTC will not change the state of the source and destination ports.

  Note If ports managed into the Unlocked administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to Unlocked-disabled,failed.

- Protected Drops—Leave this box unchecked.

Step 9 Complete the "DLP-F250 Provision SNCP Selectors During Circuit Creation" task on page 17-43.

Step 10 Click **Next**.

Step 11 Complete the "DLP-F252 Provision a Half Circuit Source and Destination on an SNCP" task on page 17-45.

Step 12 Click **Finish**. One of the following results occurs, depending on the circuit properties you chose in the Circuit Creation dialog box:

- If you entered more than 1 in the Number of circuits field and checked Auto-ranged, CTC automatically creates the number of circuits entered in Number of circuits. If autoranging cannot complete all the circuits, for example, because sequential ports are unavailable at the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click Finish to continue autoranging. After completing the circuit(s), the Circuits window appears.
- If you entered more than 1 in the Number of circuits field and did not check Auto-ranged, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 6 through 11 for each additional circuit. After completing the circuit(s), the Circuits window appears.

Step 13 In the Circuits window, verify that the new circuits appear in the circuits list.

Step 14 Complete the "NTP-F167 Test Optical Circuits" procedure on page 6-16. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-F170 Create Overhead Circuits

Purpose	This procedure creates overhead circuits on an ONS 15600 SDH network. ONS 15600 SDH overhead circuits include DCC tunnels and IP-encapsulated tunnels.
Tools/Equipment	None
Prerequisite Procedures	NTP-F163 Verify Network Turn-Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you will create the overhead circuit. If you are already logged in, continue with Step 2.

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

Step 3 As needed, complete the "DLP-F244 Create a DCC Tunnel" task on page 17-36.

Step 4 As needed, complete the "DLP-F166 Create an IP-Encapsulated Tunnel" task on page 16-9.

Stop. You have completed this procedure.

NTP-F171 Create an ASAP Ethernet Circuit

Purpose	This procedure creates an Ethernet circuit using ASAP PPM ports.
Tools/Equipment	An ASAP card must be installed.
Prerequisite Procedures	NTP-F163 Verify Network Turn-Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure requires the use of automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see Appendix C, "Network Element Defaults," in the *Cisco ONS 15600 SDH Reference Manual*.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-F196 Manage Pluggable Port Modules on the ASAP Card" procedure on page 10-1 and set the port type to **ETHR**.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab and click **Create**.

Step 5 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **VC_HO_PATH_CIRCUIT**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.

Step 6 Click **Next**.

Step 7 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size. Valid circuit sizes for an ASAP circuit are VC3, VC4, VC4-2c, VC4-3c, VC4-4c, and VC4-8c.
- Bidirectional—Leave the default unchanged (checked).
- Create cross-connects only (TL1-like)—Uncheck this box.
- Diagnostic—Leave unchecked.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - **Unlocked**—Puts the circuit cross-connects in the Unlocked-enabled service state.
  - **Locked,disabled**—Puts the circuit cross-connects in the Locked-enabled,disabled service state. Traffic is not passed on the circuit.

  - **Unlocked,automaticInService**—Puts the circuit cross-connects in the Unlocked-disabled,automaticInService service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to Unlocked-enabled.
  - **Locked,maintenance**—Puts the circuit cross-connects in the Locked-enabled,maintenance service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use Locked,maintenance for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to Unlocked; Unlocked,automaticInService; or Locked,disabled when testing is complete. See the "DLP-F313 Change a Circuit Service State" task on page 18-13. For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

- Apply to drop ports—Leave this box at the default (unchecked).

Note If ports managed into the Unlocked administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to Unlocked-disabled,failed.

- Protected Drops—Leave the default unchanged (unchecked).

Step 8 If the circuit will be routed on an SNCP ring, complete the "DLP-F250 Provision SNCP Selectors During Circuit Creation" task on page 17-43.

Step 9 Click **Next**.

Step 10 Provision the circuit source:

a. From the Node drop-down list, choose the circuit source node. Either end node can be the point-to-point circuit source.

b. From the Slot drop-down list, choose the slot containing the ASAP card that you will use for one end of the point-to-point circuit.

c. From the Port drop-down list, choose a port.

Step 11 Click **Next**.

Step 12 Provision the circuit destination:

a. From the Node drop-down list, choose the circuit destination node.

b. From the Slot drop-down list, choose the slot containing the card that you will use for other end of the point-to-point circuit.

c. From the Port drop-down list, choose a port, if applicable.

Step 13 Click **Next**.

Step 14 In the left pane of the Circuit Routing Preferences window, confirm that the following information is correct:

- Circuit name
- Circuit type
- Circuit size
- ONS nodes

Step 15 If the information is not correct, click the **Back** button and repeat Steps 5 through 14 with the correct information. If the information is correct, check **Route Automatically**.

Step 16 Click **Finish**.

Note To change the capacity of an ASAP circuit, you must delete the original circuit and reprovision a new larger circuit.

Step 17 Complete the "DLP-F324 Provision ASAP Ethernet Ports" task on page 18-22, as necessary.

Step 18 Complete the "DLP-F325 Provision ASAP POS Ports" task on page 18-23, as necessary.

Step 19 Complete the "NTP-F172 Test ASAP Ethernet Circuits" procedure on page 6-24.

Stop. You have completed this procedure.

NTP-F172 Test ASAP Ethernet Circuits

Purpose	This procedure tests circuits created on ASAP Ethernet ports.
Tools/Equipment	Ethernet test set and appropriate fibers
Prerequisite Procedures	This procedure assumes you completed facility loopback tests to test the fibers and cables from the source and destination ONS 15600 SDHs to the fiber distribution panel or the DSX, and "NTP-F171 Create an ASAP Ethernet Circuit" procedure on page 6-22. For more information on facility loopback tests, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you will create the circuit.

Step 2 Complete the "DLP-F313 Change a Circuit Service State" task on page 18-13 to change the circuit and circuit ports to the Locked-enabled,maintenance service state.

Step 3 On the shelf graphic, double-click the circuit source card.

Step 4 Click the **Provisioning > Ethernet > Port** tabs.

Step 5 Verify the following settings:

- Admin State—Locked,maintenance
- Flow Control Neg—Checked or unchecked as indicated by the circuit or site plan
- Max Size—Checked or unchecked as indicated by the circuit or site plan

Step 6 Repeat Steps 1 through 5 for the destination node.

Step 7 At the destination node, connect the Ethernet test to the destination port and configure the test set to send and receive the appropriate Ethernet traffic.

Note At this point, you are not able to send and receive Ethernet traffic.

Step 8 At the source node, connect an Ethernet test set to the source port and configure the test set to send and receive the appropriate Ethernet traffic.

Step 9 Transmit Ethernet frames between both test sets. If you cannot transmit and receive Ethernet traffic between the nodes, repeat Steps 1 through 8 to make sure you configured the Ethernet ports and test set correctly.

Step 10 Perform protection switch testing appropriate to the SDH topology:

- For SNCP rings, complete the "DLP-F193 SNCP Protection Switching Test" task on page 16-51.
- For MS-SPRings, complete the "DLP-F342 MS-SPRing Switch Test" task on page 18-43.

Configure your test set according to local site practice. For information about configuring your test set, see your test set user guide.

Step 11 Complete the "DLP-F313 Change a Circuit Service State" task on page 18-13 to change the circuit and circuit ports to the Unlocked-enabled service state.

Step 12 After the circuit test is complete, print the results or save them to a disk for future reference. For information about printing or saving test results, see your test set user guide.

Stop. You have completed this procedure.

NTP-F173 Create a High-Order Test Circuit around the Ring

Purpose	This procedure creates a high-order test circuit that routes traffic around a ring with the source and destination located on different ports of the same node.
Tools/Equipment	None
Prerequisite Procedures	NTP-F163 Verify Network Turn-Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node on the network where you want to create an optical circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-F249 Assign a Name to a Port" task on page 17-42. If not, continue with Step 3.

Step 3 If the optical ports at the source and/or destination nodes are ASAP PPM ports, complete the "NTP-F196 Manage Pluggable Port Modules on the ASAP Card" procedure on page 10-1 and set the port type to STM1, STM4, or STM16, as necessary.

Step 4 From the View menu, choose **Go To Network View**.

Step 5 Click the **Circuits** tab, then click **Create**.

Step 6 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **VC_HO_PATH_CIRCUIT**.
- Number of Circuits—Enter the number of STM-N circuits you want to create. The default is 1.

- Auto-ranged—Applies to automatically routed circuits only. If you entered more than 1 in the Number of Circuits field, uncheck this box. (The box is unavailable if only one circuit is entered in Number of Circuits.)

Step 7 Click **Next**.

Step 8 Define the circuit attributes (Figure 6-1 on page 6-6):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size: VC3, VC4, VC4-4c, VC4-8c, VC4-16c, or VC4-64c. ASAP optical ports also allow circuit sizes of VC4-2c and VC4-3c.
- Bidirectional—Leave checked (default) for this circuit. When checked, CTC creates a two-way circuit.
- Create cross-connects only (TL1-like)—Check this check box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. Also, low-order tunnels and Ethergroup sources and destinations are unavailable.
- Diagnostic—Leave unchecked.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - **Unlocked**—Puts the circuit cross-connects in the Unlocked-enabled service state.
  - **Locked,disabled**—Puts the circuit cross-connects in the Locked-enabled,disabled service state. Traffic is not passed on the circuit.
  - **Unlocked,automaticInService**—Puts the circuit cross-connects in the Unlocked-disabled,automaticInService service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to Unlocked-enabled.
  - **Locked,maintenance**—Puts the circuit cross-connects in the Locked-enabled,maintenance service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use Locked,maintenance for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to Unlocked; Unlocked,automaticInService; or Locked,disabled when testing is complete. See the "DLP-F313 Change a Circuit Service State" task on page 18-13. For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15600 SDH Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state of the source and destination ports.

  Note If ports managed into the Unlocked administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to Unlocked-disabled,failed.

- Protected Drops—If selected, CTC displays only protected cards and ports (1+1 protection) as choices for the circuit source and destination.

Step 9 Click **Next**.

Step 10 Choose the circuit source:

a. From the Node drop-down list, choose the node where the circuit will originate.

b. From the Slot drop-down list, choose the slot containing the card where the circuit originates. (If card capacity is fully utilized, it does not appear in the list.)

c. Depending on the circuit origination card, choose the source port and/or VC from the Port and VC drop-down list. The Port drop-down list is only available if the card has multiple ports. VCs do not appear if they are already in use by other circuits.

Note The VCs that appear depend on the card, circuit size, and protection scheme.

Step 11 Click **Next**.

Step 12 Choose the circuit destination:

Note The destination port must be located on the same node as the circuit source port.

a. From the Node drop-down list, choose the node selected in Step 10a.

b. From the Slot drop-down list, choose the slot containing the card where the circuit will terminate (destination card). (If a card’s capacity is fully utilized, the card does not appear in the drop-down list.)

c. Depending on the card selected in Step b, choose the destination port and/or VC from the Port and VC drop-down lists. The Port drop-down list is available only if the card has multiple ports. The VCs that appear depend on the card, circuit size, and protection scheme.

Step 13 Click **Next**.

Step 14 In the Circuit Routing Preferences area (Figure 6-2 on page 6-7), uncheck **Route Automatically**.

Step 15 When routing a test circuit with source and destination ports on the same node, the Fully Protected Path check box is automatically disabled. Choose one of the following options:

- To leave the test circuit unprotected, skip this step and continue with Step 16.
- To route the test circuit on an MS-SPRing protection channel, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 16.

Caution Circuits routed on MS-SPRing protection channels are not protected and are preempted during MS-SPRing switches.

Step 16 Click **Next**. In the Route Review/Edit area, node icons appear for you to route the circuit manually. The green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit.

Step 17 Complete the “DLP-F343 Provision an STM-N Circuit Route” task on page 18-47.

Step 18 Click **Finish**. If the path does not meet the specified path diversity requirement, an error message appears and allows you to change the circuit path. If you entered more than 1 in the Number of circuits field, the Circuit Creation dialog box appears after the circuit is created so you can create the remaining circuits. Repeat Steps 8 through 17 for each additional circuit.

Step 19 When all the circuits are created, the main Circuits window appears. Verify that the circuit(s) you created appear in the window.

Stop. You have completed this procedure.

NTP-F174 Create a Server Trail

Purpose	This procedure creates a server trail, which provides a connection between ONS nodes through a third-party network. You can create server trails between any two any two STM-N or EC1 ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-F163 Verify Network Turn-Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You cannot create server trails on ports with DCC links.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

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

Step 3 Click the **Provisioning > Server Trails** tabs.

Step 4 Click **Create**.

Step 5 In the Server Trail Creation dialog box, complete the following fields:

- Type—Choose **VC_HO_PATH_CIRCUIT**.
- Size—Depending on the type selected, choose the server trail size. For VC_HO_PATH_CIRCUIT, choose **VC4-2c**, **VC4-3c**, **VC4-4c**, **VC4-6c**, **VC4-8c**, **VC4-12c**, **VC4-16c**, **VC4-64c**, or **VC4**. For VC_LO_PATH_CIRCUIT, choose **VC3**, **VC12**, or **VC11**.
- Protection Type—Choose one of the following protection types: Preemptible, Unprotected, or Fully Protected. The server trail protection sets the protection type for any circuit that traverses it.
  - Preemptible— PCA circuits will use server trails with the Preemptible attribute.
  - Unprotected—In Unprotected Server Trail, CTC assumes that the circuits going out from that specific port will not be protected by provider network and will look for a secondary path from source to destination if you are creating a protected circuit.
  - Fully Protected—In Fully Protected Server Trail, CTC assumes that the circuits going out from that specific port will be protected by provider network and will not look for a secondary path from source to destination.
- Number of Trails—Enter the number of server trails. Number of trails determine the number of circuits that can be created on server trail. You can create a maximum of 3744 server trails on a node. You can create multiple server trails from the same port. This is determined by how many circuits of a particular server trail size can be supported on the port (for example, you can create one VC4 server trail from one STM-1 port or 3 VC3 and 63 VC12 server trails from one STM-1 port).

Step 6 Click **Next**.

Step 7 In the Source area, complete the following:

a. From the Node drop-down list, choose the node where the source will originate.

b. From the Slot drop-down list, choose the slot containing the card where the server trail originates. (If a card's capacity is fully utilized, the card does not appear in the list.)

c. Depending on the card selected, choose the destination port and/or VC3, VC4, VC11, or VC12 from the Port and VC3, VC4, VC11, or VC12 lists. The Port list is only available if the card has multiple ports. VC3, VC4, VC11, or VC12 do not appear if they are already in use by other circuits.

Step 8 Click **Next**.

Step 9 In the Destination area, complete the following:

a. From the Node drop-down list, choose the destination node.

b. From the Slot drop-down list, choose the slot containing the card where the server trail will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the list.)

c. Depending on the card selected, choose the destination port and/or VC3, VC4, VC11, or VC12 from the Port and VC3, VC4, VC11, or VC12 lists. The Port list is only available if the card has multiple ports. VC3, VC4, VC11, or VC12 do not appear if they are already in use by other circuits.

Step 10 Click **Finish**.

Stop. You have completed this procedure.

NTP-F175 Create an Automatically Routed Open-Ended SNCP High-Order Circuit

Purpose	This procedure creates an open-ended high-order SNCP. Use this procedure when it is necessary to route low-order traffic across an ONS 15600 SDH hub.
Tools/Equipment	None
Prerequisite Procedures	NTP-F160 Provision an ONS 15600 SDH Node as a Protection Domain Hub, page 5-28 NTP-F163 Verify Network Turn-Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node on the network where you want to create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-F249 Assign a Name to a Port" task on page 17-42. If not, continue with Step 3.

Step 3 If the optical ports at the source and/or destination nodes are ASAP PPM ports, complete the "NTP-F196 Manage Pluggable Port Modules on the ASAP Card" procedure on page 10-1 and set the port type to STM1, STM4, STM16, or STM 64, as necessary.

Step 4 From the View menu, choose **Go To Network View**.

Step 5 Click the **Circuits** tab, then click **Create**.

Step 6 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **VC_HO_PATH_CIRCUIT**.
- Number of Circuits—Leave set to 1.
- Auto-ranged—Leave unchecked.

Step 7 Click **Next**.

Step 8 Define the circuit attributes (Figure 6-1 on page 6-6):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose **VC-4**.
- Bidirectional—As desired. When checked, CTC creates a two-way circuit.
- Create cross-connects only (TL1-like)—Check this check box to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you are creating an open-ended high-order SNCP circuit to bridge low-order traffic, you must check this check box.
- Diagnostic—Leave unchecked.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - **Unlocked**—Puts the circuit cross-connects in the Unlocked-enabled service state.
  - **Locked,disabled**—Puts the circuit cross-connects in the Locked-enabled,disabled service state. Traffic is not passed on the circuit.
  - **Unlocked,automaticInService**—Puts the circuit cross-connects in the Unlocked-disabled,automaticInService service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to Unlocked-enabled.
  - **Locked,maintenance**—Puts the circuit cross-connects in the Locked-enabled,maintenance service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use Locked,maintenance for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to Unlocked; Unlocked,automaticInService; or Locked,disabled when testing is complete. See the "DLP-F313 Change a Circuit Service State" task on page 18-13. For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15600 SDH Reference Manual*.
- Apply to drop ports—Check this check box if you want to apply the administrative state chosen in the State field to the circuit source and destination ports. CTC applies the administrative state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the port. If not, a Warning dialog box displays the ports where the administrative state could not be applied. If the check box is unchecked, CTC does not apply the administrative state of the source and destination ports.

  Note If ports managed into the Unlocked administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to Unlocked-disabled,failed.

- Protected Drops—If selected, CTC displays only protected cards and ports (1+1 protection) as choices for the circuit source and destination.

Step 9 If the circuit will be routed on an SNCP ring, complete the "DLP-F250 Provision SNCP Selectors During Circuit Creation" task on page 17-43.

Step 10 Click **Next**.

Step 11 Complete the "DLP-F194 Provision an Optical Circuit Source and Destination" task on page 16-52 for the optical circuit that you are creating. Choose a single source and secondary destinations to create the open-ended SNCP circuit.

Step 12 In the Circuit Routing Preferences area (Figure 6-2 on page 6-7), check **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- Using Required Nodes/Spans—Check this box to specify nodes and spans to include or exclude in the CTC-generated circuit route.

  Including nodes and spans for a circuit ensures that those nodes and spans are in the working path of the circuit (but not the protect path). Excluding nodes and spans ensures that the nodes and spans are not in the working or protect path of the circuit.

- Review Route Before Creation—Check this box to review and edit the circuit route before the circuit is created.

Step 13 Leave **Fully Protected Path** checked.

Step 14 Choose one of the following:

- **Nodal Diversity Required**—Ensures that the primary and alternate paths within the SNCP ring portions of the complete circuit path are nodally diverse.
- **Nodal Diversity Desired**—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the SNCP ring portion of the complete circuit path.
- **Link Diversity Only**—Specifies that only fiber-diverse primary and alternate paths for SNCP ring portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 15 Click **Next**. If you selected Review Route Before Creation in Step 12, complete the following substeps; otherwise, continue with Step 16:

a. Click **Next**.

b. Review the circuit route. To add or delete a circuit span, select a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the "NTP-F165 Create a Manually Routed Optical Circuit" procedure on page 6-9 to assign the circuit route yourself.

Step 16 Click **Finish**. If the path does not meet the specified path diversity requirement, an error message appears and allows you to change the circuit path. If you entered more than 1 in the Number of circuits field, the Circuit Creation dialog box appears after the circuit is created so you can create the remaining circuits. Repeat Steps 6 through 15 for each additional circuit.

Step 17 When all the circuits are created, the main Circuits window appears. Verify that the circuit(s) you created appear in the window.

Step 18 Complete the "NTP-F167 Test Optical Circuits" procedure on page 6-16.

Stop. You have completed this procedure.

NTP-E199 Create an Overlay Ring Circuit

Purpose	This procedure creates an overlay ring circuit that routes traffic around multiple rings, passing through one or more nodes more than once.
Tools/Equipment	None
Prerequisite Procedures	NTP-F163 Verify Network Turn-Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or HIGHER

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at an ONS 15600 SDH on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-F249 Assign a Name to a Port" task on page 17-42. If you want CTC to assign a name automatically based on circuit type, node name, and sequence number, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **VC_HO_PATH_CIRCUIT**.
- Number of Circuits—Enter the number of circuits that you want to create. The default is 1.
- Auto-ranged—Uncheck this checkbox.

Note If specify the number of circuits as more than 1 and if the auto-ranged check box is selected, the Route Automatically check box in the Circuit Routing Preferences area is automatically checked; this prevents you from creating an overlay ring circuit.

Step 5 Click **Next**.

Step 6 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the high-order circuit size: **VC4**, V**C4-2c**, **VC4-3c**, **VC4-4c**, **VC4-8c**, **VC4-16c**, or **VC4-64c**.
- Bidirectional—Leave checked for this circuit.
- Create cross-connects only (TL1-like)—Check this check box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If you check this box, low-order tunnels and Ethergroup sources and destinations are unavailable.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - **Unlocked**—Puts the circuit cross-connects in the Unlocked-enabled service state.

  - **Locked,disabled**—Puts the circuit cross-connects in the Locked-enabled,disabled service state. Traffic is not passed on the circuit.
  - **Unlocked,automaticInService**—Puts the circuit cross-connects in the Unlocked-disabled,automaticInService service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to Unlocked-enabled.
  - **Locked,maintenance**—Puts the circuit cross-connects in the Locked-enabled,maintenance service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use Locked,maintenance for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to Unlocked; Unlocked,automaticInService; or Locked,disabled when testing is complete. See the "DLP-F313 Change a Circuit Service State" task on page 18-13.

  For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 SDH Reference Manual*.

- Apply to drop ports—Check this box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC applies the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. If the box is unchecked, CTC does not change the state of the source and destination ports.

  Note If ports managed into the Unlocked administrative state are not receiving signals, loss of signal alarms are generated and the port service state transitions to Unlocked-disabled,failed.

- Protected Drops—Select this check box if you want the circuit routed to protect drops only, that is, to ONS 15454 SDH cards that are in 1:1, 1:N, or 1+1 protection. If you select this check box, CTC shows only protected cards as source and destination choices.

Step 7 Click **Next**.

Step 8 Choose the circuit source:

a. From the Node drop-down list, choose the node where the circuit will originate.

b. From the Slot drop-down list, choose the slot containing the high-order card where the circuit originates. (If a card's capacity is fully utilized, it does not appear in the drop-down list.)

c. Depending on the circuit origination card, choose the source port and/or VC-4 from the Port and VC-4 drop-down lists. The Port drop-down list is only available if the card has multiple ports. VC-4s are not shown if they are already in use by other circuits.

Note The VC4s that appear depend on the card, circuit size, and protection scheme.

Step 9 Click **Next**.

Step 10 Choose the circuit destination:

a. From the Node drop-down list, choose the node selected in Step 8a.

b. From the Slot drop-down list, choose the slot containing the optical card where the circuit will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the drop-down list.)

c. Depending on the card selected in Step b, choose the destination port and/or VC-4 from the Port and VC-4 drop-down lists. The Port drop-down list is available only if the card has multiple ports. The VC-4s that appear depend on the card, circuit size, and protection scheme.

Step 11 Click **Next**.

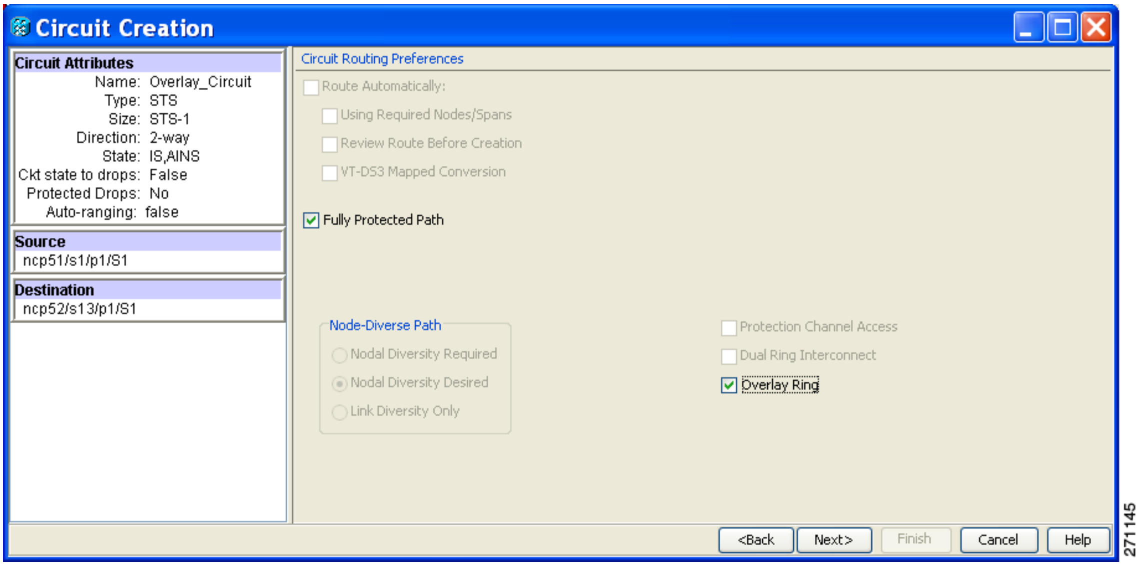
Step 12 In the Circuit Routing Preferences area, uncheck **Route Automatically** to enable the **Overlay Ring** check box.

Step 13 To set the circuit path protection, complete one of the following:

- To create an unprotected circuit, uncheck the **Fully Protected Path** check box.
- To create a protected circuit, check the **Fully Protected Path** check box.

Step 14 Check the **Overlay Ring** check box (Figure 6-3).

Figure 6-3 Overlay Ring Check Box



Circuit Creation

Circuit Attributes
Name: Overlay_Circuit
Type: STS
Size: STS-1
Direction: 2-way
State: IS,AINS
Ckt state to drops: False
Protected Drops: No
Auto-ranging: false

Source
ncp51/s1/p1/S1

Destination
ncp52/s13/p1/S1

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

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

□ Protection Channel Access
□ Dual Ring Interconnect
☑ Overlay Ring

Step 15 Click **Next**. In the Route Review/Edit area, node icons appear for circuit routing. The circuit source node is selected. Green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit.

Note During manual routing, while creating an overlay ring circuit, you can create loops. Creating loops allows you to return to the same node more than once while selecting the spans.

Step 16 Click **Finish**.

Step 17 When all the circuits are created, the main Circuits window appears. Verify that the circuits you created appear in the window.

Stop. You have completed this procedure.

CHAPTER 7

Manage Circuits

This chapter explains how to manage Cisco ONS 15600 SDH optical and overhead circuits.

Before You Begin

To create circuits, see Chapter 6, "Create Circuits."

To clear any alarm or trouble conditions, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

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

1. NTP-F176 Locate and View Circuits, page 7-2—Complete as needed.
2. NTP-F177 Modify and Delete Circuits, page 7-2—Complete as needed to edit a circuit name, change a circuit service state, change the active and standby colors of spans, or change signal fail (SF) and signal degrade (SD) thresholds, reversion time, and payload defect indication-path (PDI-P) settings for subnetwork connection protection (SNCP) circuits.
3. NTP-F178 Modify and Delete Overhead Circuits and Server Trails, page 7-3—Complete as needed to change a tunnel type, repair an IP circuit, or delete overhead circuits.
4. NTP-F179 Create a J0 Section Trace, page 7-3—Complete as needed to monitor interruptions or changes to circuit traffic.
5. NTP-F180 Create a J1 Path Trace, page 7-4—Complete as needed to monitor interruptions or changes to circuit traffic.
6. NTP-F181 Bridge and Roll Traffic, page 7-5—Complete as needed to reroute circuits without interrupting service.
7. NTP-F182 Reconfigure Circuits, page 7-6—Complete as needed to reconfigure circuits.
8. NTP-F183 Merge Circuits, page 7-7—Complete as needed to merge circuits.

Note To provision ONS 15600 SDH circuits from an ONS 15454 SDH node, the Cisco Transport Controller (CTC) version launched from the ONS 15454 SDH must be Software R4.1 or later. Cisco recommends launching CTC from the ONS 15600 SDH node before provisioning circuits.

Note During circuit provisioning in a network that includes ONS 15600 SDH nodes and ONS 15454 SDH nodes, the ONS 15600 SDH raises a temporary HP-UNEQ or LP-UNEQ alarm. The alarm clears when the circuit is complete.

NTP-F176 Locate and View Circuits

Purpose	This procedure locates and displays ONS 15600 SDH circuits. You can also export circuit data from the Circuit and Edit Circuits windows.
Tools/Equipment	None
Prerequisite Procedures	Circuits must exist on the network. See Chapter 6, "Create Circuits."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at any node on the network where you want to view the circuits. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-F348 View Circuit Information" task on page 18-51.

Step 3 As needed, complete the "DLP-F214 Search for Circuits" task on page 17-13.

Step 4 As needed, complete the "DLP-F215 Filter the Display of Circuits" task on page 17-14.

Step 5 As needed, complete the "DLP-F216 View Circuits on a Span" task on page 17-15.

Step 6 As needed, complete the "DLP-F379 Export CTC Data" task on page 18-88.

Stop. You have completed this procedure.

NTP-F177 Modify and Delete Circuits

Purpose	This procedure edits or changes the properties of ONS 15600 SDH circuits.
Tools/Equipment	None
Prerequisite Procedures	Circuits must exist on the network. See Chapter 6, "Create Circuits."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the network containing the circuit you want to modify. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-F217 Edit a Circuit Name" task on page 17-16.

Step 3 As needed, complete the "DLP-F313 Change a Circuit Service State" task on page 18-13.

Step 4 As needed, complete the "DLP-F218 Change Active and Standby Span Color" task on page 17-17.

Step 5 As needed, complete the "DLP-F264 Edit SNCP Circuit Path Selectors" task on page 17-55.

Step 6 As needed, complete the "DLP-F301 Edit SNCP Dual-Ring Interconnect Circuit Hold-Off Timer" task on page 18-2.

Step 7 As needed, complete the "DLP-F293 Delete Circuits" task on page 17-83.

Stop. You have completed this procedure.

NTP-F178 Modify and Delete Overhead Circuits and Server Trails

Purpose	This procedure changes the tunnel type, repairs IP circuits, and deletes overhead circuits and server trails.
Tools/Equipment	None
Prerequisite Procedures	Overhead circuits must exist on the network. See Chapter 6, "Create Circuits."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

⚠ **Caution** Deleting circuits can be service affecting and should be performed during a maintenance window.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 for a node on the network where you want to delete the circuit. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-F302 Change Tunnel Type" task on page 18-2.

Step 3 As needed, complete the "DLP-F304 Repair an IP Tunnel" task on page 18-4.

Step 4 As needed, complete the "DLP-F303 Delete Overhead Circuits" task on page 18-3.

Step 5 As needed, complete the "DLP-F382 Delete a Server Trail" task on page 18-95.

Stop. You have completed this procedure.

NTP-F179 Create a J0 Section Trace

Purpose	This procedure creates a repeated, fixed-length string of characters used to monitor interruptions or changes to traffic between nodes.
Tools/Equipment	Any optical card
Prerequisite Procedures	None
Required/As Needed	As needed (optional if path trace is set)
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node on the network where you will create the section trace. If you are already logged in, continue with Step 2.

Step 2 In node view, double-click the the card.

Step 3 Click the **Provisioning > Line > Section Trace** tabs.

Step 4 From the Port drop-down list, choose the port for the section trace.

Step 5 From the Trace Mode drop-down list, enable the section trace expected string by choosing **Auto** or **Manual**:

- Auto—The first string received from the source port is automatically provisioned as the current expected string. An alarm is raised when a string that differs from the baseline is received.
- Manual—The string entered in the Current Expected String field is the baseline. An alarm is raised when a string that differs from the Current Expected String is received.

Step 6 In the Section Trace String Size area, click **1 byte**, **16 byte,** or **64 byte**. In the New Transmit String field, enter the string that you want to transmit. Enter a string that makes the destination port easy to identify, such as the node IP address, node name, or another string. If the New Transmit String field is left blank, the J0 transmits a string of null characters.

Step 7 If you set the Section Trace Mode field to Manual, enter the string that the destination port should receive from the source port in the New Expected String field. If you set Section Trace Mode to Auto, skip this step.

Step 8 Click **Apply**.

Step 9 After you set up the section trace, the received string appears in the Received field. The following options are available:

- Click **Hex Mode** to display section trace in hexadecimal format. The button name changes to ASCII Mode. Click it to return the section trace to ASCII format.
- Click the **Reset** button to reread values from the port.
- Click **Default** to return to the section trace default settings (Section Trace Mode is set to Off and the New Transmit and New Expected Strings are null).

Caution Clicking Default will generate alarms if the port on the other end is provisioned with a different string.

The expect and receive strings are updated every few seconds if the Section Trace Mode field is set to Auto or Manual.

Stop. You have completed this procedure.

NTP-F180 Create a J1 Path Trace

Purpose	This procedure creates a repeated, fixed-length string of characters used to monitor interruptions or changes to circuit traffic.
Tools/Equipment	ONS 15600 SDH cards capable of transmitting and/or receiving path trace must be installed. See Table 18-1 on page 18-5 for a list of cards.
Prerequisite Procedures	Circuits must exist on the network. See Chapter 6, "Create Circuits."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You cannot create a J1 path trace on a TL1-like circuit.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node on the network where you will create the path trace. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-F305 Provision Path Trace on Circuit Source and Destination Ports" task on page 18-4.

Step 3 As needed, complete the "DLP-F306 Provision Path Trace on STM-N Ports" task on page 18-8.

Stop. You have completed this procedure.

NTP-F181 Bridge and Roll Traffic

Purpose	This procedure reroutes live traffic without interrupting service. You can use the Bridge and Roll wizard for maintenance functions such as card replacement or load balancing. A circuit consists of a source facility, destination facility(s), and intermediate facilities (path).
Tools/Equipment	None
Prerequisite Procedures	• Circuits must exist on the network. See Chapter 6, "Create Circuits." for circuit creation procedures. • To route circuits on protected ports, you must create a protection group using the "NTP-F138 Create a 1+1 Protection Group" procedure on page 4-10 or the "NTP-F148 Create an MS-SPRing" procedure on page 5-8. • When a roll involves two circuits, a data communications channel (DCC) connection must exist. See the "DLP-F253 Provision RS-DCC Terminations" task on page 17-46. • Use the "NTP-F176 Locate and View Circuits" procedure on page 7-2 to verify that the planned Roll To paths are in service. Verify that the planned Roll To and Roll From paths are not in the Roll Pending status, used in test access, used in a loopback, used in a hairpin circuit, used in a monitor circuit, or have ports in protection group switching. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* to clear any alarms.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

Note Using the bridge and roll feature, you can upgrade an unprotected circuit to a fully protected circuit or downgrade a fully protected circuit to an unprotected circuit.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the ONS 15600 SDH circuit source node. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-F351 Roll the Source or Destination of One Optical Circuit" task on page 18-56.

Step 3 As needed, complete the "DLP-F352 Roll One Cross-Connect from an Optical Circuit to a Second Optical Circuit" task on page 18-60.

Step 4 As needed, complete the "DLP-F353 Roll Two Cross-Connects on One Optical Circuit Using Automatic Routing" task on page 18-62 or the "DLP-F354 Roll Two Cross-Connects on One Optical Circuit Using Manual Routing" task on page 18-66.

Step 5 As needed, complete the "DLP-F355 Roll Two Cross-Connects from One Optical Circuit to a Second Optical Circuit" task on page 18-68.

Step 6 As needed, complete the "DLP-F357 Cancel a Roll" task on page 18-70.

Step 7 As needed, complete the "DLP-F356 Delete a Roll" task on page 18-69. Use caution when selecting this option. Delete a roll only if it cannot be completed or cancelled. Circuits may have a PARTIAL status when this option is selected.

Stop. You have completed this procedure.

NTP-F182 Reconfigure Circuits

Purpose	This procedure rebuilds circuits, which might be necessary when a large number of circuits are in the PARTIAL status.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Click the **Circuits** tab.

Step 3 Choose the circuits that you want to reconfigure.

Step 4 From the Tools menu, choose **Circuits > Reconfigure Circuits**.

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

Step 6 In the notification box, view the reconfiguration result. Click **Ok**.

Stop. You have completed this procedure.

NTP-F183 Merge Circuits

Purpose	This procedure merges two circuits that create a single, contiguous path but are separate circuits because of different circuit IDs or conflicting parameters. A merge combines a single master circuit with one or more circuits.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Click the **Circuits** tab.

Step 3 Click the circuit that you want to use as the master circuit for a merge.

Step 4 Click **Edit**.

Step 5 In the Edit Circuits window, click the **Merge** tab.

Step 6 Choose the circuits that you want to merge with the master circuit.

Step 7 Click **Merge**.

Step 8 In the confirmation dialog box, click **Yes** to continue.

Step 9 In the notification box, view the merge result. Click **Ok**.

Stop. You have completed this procedure.

CHAPTER 8

Monitor Performance

This chapter explains how to enable and view performance monitoring statistics for the Cisco ONS 15600 SDH. Performance monitoring (PM) parameters are used by service providers to gather, store, threshold, and report performance data for early detection of problems. For more PM information, details, and definitions, refer to the *Cisco ONS 15600 SDH Reference Manual*.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* as necessary.

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

1. NTP-F184 Change the PM Display, page 8-2—Complete as needed.
2. NTP-F185 Enable Intermediate-Path Performance Monitoring, page 8-3—Complete as needed.
3. NTP-F186 Monitor Optical Performance, page 8-5—Complete as needed after enabling performance monitoring.
4. NTP-F187 Monitor Ethernet Performance, page 8-6—Complete as needed.

Note For additional information regarding PM parameters, refer to ITU G.826, Telcordia GR-820-CORE, Telcordia GR-499-CORE, and Telcordia GR-253-CORE.

NTP-F184 Change the PM Display

Purpose	This procedure changes the display of PM counts by selecting drop-down list or radio button options in the Performance window.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits." and Chapter 10, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node that you want to monitor. If you are already logged in, continue with Step 2.

Step 2 As needed, use the following tasks to change the display of PM counts:

- DLP-F208 Refresh PM Counts at Fifteen-Minute Intervals, page 17-9
- DLP-F209 Refresh PM Counts at One-Day Intervals, page 17-10
- DLP-F210 Monitor Near-End PM Counts, page 17-10
- DLP-F211 Monitor Far-End PM Counts, page 17-11
- DLP-F212 Reset Current PM Counts, page 17-11
- DLP-F213 Clear Selected PM Counts, page 17-12
- DLP-F397 Clear All PM Thresholds, page 18-120
- DLP-F256 Set Auto-Refresh Interval for Displayed PM Counts, page 17-49
- DLP-F207 Refresh PM Counts for a Selected Port and VC, page 17-8

Stop. You have completed this procedure.

NTP-F185 Enable Intermediate-Path Performance Monitoring

Purpose	This procedure enables intermediate path performance monitoring (IPPM), which allows you to monitor virtual container (VC) traffic through intermediate nodes in a circuit path.
Tools/Equipment	None
Prerequisite Procedures	NTP-F164 Create an Automatically Routed Optical Circuit, page 6-4 or NTP-F165 Create a Manually Routed Optical Circuit, page 6-9 or NTP-F166 Create a Unidirectional Optical Circuit with Multiple Drops, page 6-12
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Section and line performance monitoring is enabled when the ports are in the Unlocked administrative state. To enable VC traffic performance monitoring through the nodes, you must enable IPPM for the paths being monitored.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node you want to monitor. If you are already logged in, continue with Step 2.

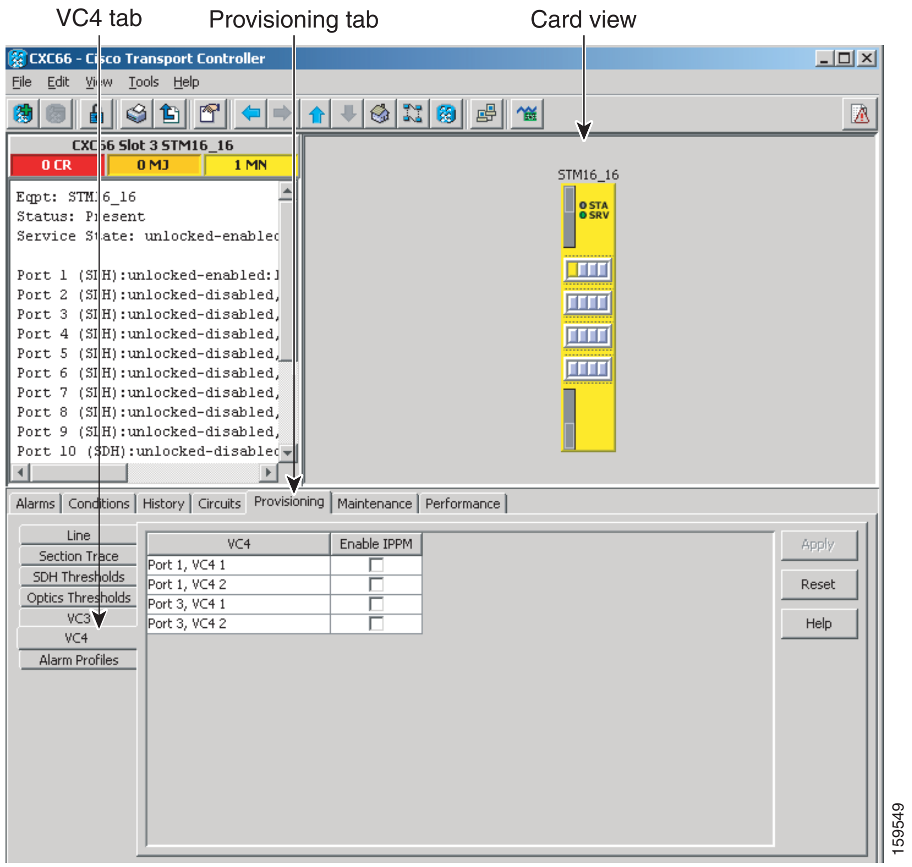
Step 2 In node view, double-click an optical (STM-N) card. The card view appears. The Cisco ONS 15600 SDH has the following optical cards:

- OC48/STM16 LR/LH 16 Port 1550
- OC48/STM16 SR/SH 16 Port 1310
- OC192/STM64 LR/LH 4 Port 1550
- OC192/STM64 SR/SH 4 Port 1310
- OC192/STM64 LH ITU C-band

Note STM-N ports on the ASAP card can be provisioned for IPPM.

Step 3 Click the **Provisioning > VC3** or **VC4** tabs. Figure 8-1 shows the VC4 tab in the Provisioning window.

Figure 8-1 SDH VC Tab for Enabling IPPM



```
Eqpt: STM16_16
Status: Present
Service State: unlocked-enablec

Port 1 (SDH):unlocked-enabled:I
Port 2 (SDH):unlocked-disabled,
Port 3 (SDH):unlocked-disabled,
Port 4 (SDH):unlocked-disabled,
Port 5 (SDH):unlocked-disabled,
Port 6 (SDH):unlocked-disabled,
Port 7 (SDH):unlocked-disabled,
Port 8 (SDH):unlocked-disabled,
Port 9 (SDH):unlocked-disabled,
Port 10 (SDH):unlocked-disablec
```

VC4	Enable IPPM
Port 1, VC4 1	□
Port 1, VC4 2	□
Port 3, VC4 1	□
Port 3, VC4 2	□

Step 4 Check the check box in the Enable IPPM column for the VC you want to monitor.

Step 5 Click **Apply**.

Step 6 Click the **Performance** tab to view the PM parameters. For IPPM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Stop. You have completed this procedure.

NTP-F186 Monitor Optical Performance

Purpose	The Performance tab window allows you to view node near-end or far-end performance on a selected card and port at specified time intervals to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	NTP-F164 Create an Automatically Routed Optical Circuit, page 6-4 or NTP-F165 Create a Manually Routed Optical Circuit, page 6-9 or NTP-F166 Create a Unidirectional Optical Circuit with Multiple Drops, page 6-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node you want to monitor. If you are already logged in, continue with Step 2.

Note To monitor an AU3 path, first create a V3 optical circuit and then choose V3 when configuring IPPM.

Step 2 To view optical PMs on STM-16 or STM-64 cards, complete the "DLP-F206 View Optical STM-N PM Parameters" task on page 17-7.

Step 3 To view optical PMs on the ASAP card, refer to the "DLP-F326 View ASAP STM-N PM Parameters" task on page 18-24 for instructions.

Note To refresh, reset, or clear PM counts, see the "NTP-F184 Change the PM Display" procedure on page 8-2 for instructions.

Stop. You have completed this procedure.

NTP-F187 Monitor Ethernet Performance

Purpose	This procedure views near-end or far-end node performance during selected time intervals on ASAP card Ethernet ports. It also enables you to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits." and Chapter 10, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node you want to monitor. If you are already logged in, continue with Step 2.

Step 2 Complete the following tasks as needed:

- DLP-F327 View ASAP Ether Ports Statistics PM Parameters, page 18-25.
- DLP-F328 View ASAP Ether Ports Utilization PM Parameters, page 18-27.
- DLP-F337 View ASAP Ether Ports History PM Parameters, page 18-37.
- DLP-F329 View ASAP POS Ports Statistics PM Parameters, page 18-28.
- DLP-F330 View ASAP POS Ports Utilization PM Parameters, page 18-29.
- DLP-F331 View ASAP POS Ports History PM Parameters, page 18-30.

Note To refresh, reset, or clear PM counts, refer to the "NTP-F184 Change the PM Display" procedure on page 8-2 for instructions.

Stop. You have completed this procedure.

CHAPTER 9

Manage Alarms

This chapter provides procedures required to view and manage Cisco ONS 15600 SDH alarms and conditions.

Cisco Transport Controller (CTC) detects and reports SDH alarms generated by the ONS 15600 SDH and the larger SDH network. You can use CTC to monitor and manage alarms at a card, node, or network level. Default alarm severities conform to the Telcordia GR-474-CORE standard, but you can reset severities to customized alarm profiles or suppress CTC alarm reporting. For alarm troubleshooting information, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Before You Begin

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

1. NTP-F188 Document Existing Provisioning, page 9-1—Complete this procedure before performing any other procedures in this chapter.
2. NTP-F189 View Alarms, Alarm History, Events, and Conditions, page 9-2—Complete as needed.
3. NTP-F190 Enable, Modify, or Disable Alarm Severity Filtering, page 9-3—Complete as needed.
4. NTP-F191 Synchronize Alarms, page 9-3—Complete as needed.
5. NTP-F192 Delete Cleared Alarms from the Display, page 9-4—Complete as needed.
6. NTP-F193 View Alarm-Affected Circuits, page 9-4—Complete as needed.
7. NTP-F194 Create, Assign, and Delete Alarm Severity Profiles, page 9-6—As needed, complete these tasks to change the default severity for certain alarms, to assign the new severities to a port, card, or node, and to delete alarm profiles.
8. NTP-F195 Suppress and Restore Alarm Reporting, page 9-7—As needed, complete these tasks to suppress reported alarms at the port, card, or node level and to disable the suppress command to resume normal alarm reporting.

NTP-F188 Document Existing Provisioning

Purpose	This procedure records, copies, prints, and exports CTC information.
Tools/Equipment	A printer must be connected to the CTC computer.
Prerequisite Procedures	Chapter 4, “Turn Up a Node”

Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node with the information where you want to record, print, or export. If you are already logged in, continue with Step 2.

Step 2 As needed, manually record CTC information (typically to document existing provisioning before upgrading or troubleshooting).

Step 3 As needed, you can copy and paste CTC text into other applications using the Microsoft Windows Copy (Ctrl+C), Cut (Ctrl+X), and Paste (Ctrl+V) commands.

Step 4 If you want to print information within a single tab, complete the "DLP-F336 Print CTC Data" task on page 18-36.

Step 5 If you want to save information to a word processing application such as a spreadsheet, complete the "DLP-F379 Export CTC Data" task on page 18-88.

Stop. You have completed this procedure.

NTP-F189 View Alarms, Alarm History, Events, and Conditions

Purpose	This procedure views ONS 15600 SDH alarms at the card, node, or network level; view the alarm history for cleared and uncleared alarms; and view conditions at the card, node, or network level.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-F195 View Alarms" task on page 16-54 to review alarms for the current session.

Step 3 Troubleshoot the alarms using the procedures in the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Step 4 Complete the "DLP-F196 View Alarm History" task on page 16-55 or the "DLP-F197 View Conditions" task on page 16-57 as needed.

Step 5 Complete the "DLP-F198 Display Events Using Each Node's Time Zone" task on page 16-58 as needed.

Stop. You have completed this procedure.

NTP-F190 Enable, Modify, or Disable Alarm Severity Filtering

Purpose	This procedure starts, stops, or changes alarm filtering for one or more severities in the Alarms, Conditions, and History windows in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to enable, modify, or disable alarm filtering. If you are already logged in, continue with Step 2.

Step 2 As necessary, complete the "DLP-F286 Enable Alarm Filtering" task on page 17-77. This task enables alarm filtering at the card, node, and network views for all nodes in the network. Alarm filtering can be enabled for alarms, conditions, or events.

Step 3 As necessary, complete the "DLP-F287 Modify Alarm and Condition Filtering Parameters" task on page 17-79 to modify the alarm filtering for network nodes to show or hide particular alarms or conditions.

Step 4 As necessary, complete the "DLP-F288 Disable Alarm Filtering" task on page 17-80 to disable alarm profile filtering for all network nodes.

Stop. You have completed this procedure.

NTP-F191 Synchronize Alarms

Purpose	This procedure manually refreshes the CTC alarm display in the card, node, or network view so that it is aligned with the most current ONS 15600 SDH alarms.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Click the **Alarms** tab in the node view, card view, or network view.

Step 3 Click **Synchronize**.

Note Alarms that have been raised during the session will have a check mark in the Alarms window New column. When you click Synchronize, the check mark disappears.

Although CTC displays alarms and events in real time, the Synchronize button allows you to verify the alarm display. This is particularly useful during provisioning or troubleshooting.

Stop. You have completed this procedure.

NTP-F192 Delete Cleared Alarms from the Display

Purpose	This procedure deletes Cleared (C) status ONS 15600 SDH alarms from the alarms window. This procedure can be used to delete transient messages from the CTC History window.
Tools/Equipment	None
Prerequisite procedures	None
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Click the **Alarms** tab and then click **Delete Cleared Alarms** to delete node-level alarms.

This action will remove any cleared ONS 15600 SDH alarms from the Alarms display. The rows of cleared alarms appear white and their status is C.

Step 3 To delete the cleared alarms for one card at one node:

a. In node view, double-click the card graphic for the card you want to open.

b. Click the **Alarms** tab and then click **Delete Cleared Alarms**.

Step 4 To delete the cleared alarms for all the nodes in a network:

a. From the View menu, choose **Go to Network View**.

b. Click the **Alarms** tab and then click **Delete Cleared Alarms**.

Stop. You have completed this procedure.

NTP-F193 View Alarm-Affected Circuits

Purpose	This procedure displays ONS 15600 SDH circuits that are affected by a specific alarm.
Tools/Equipment	None

Prerequisite Procedures	Chapter 6, "Create Circuits."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, go to Step 2.

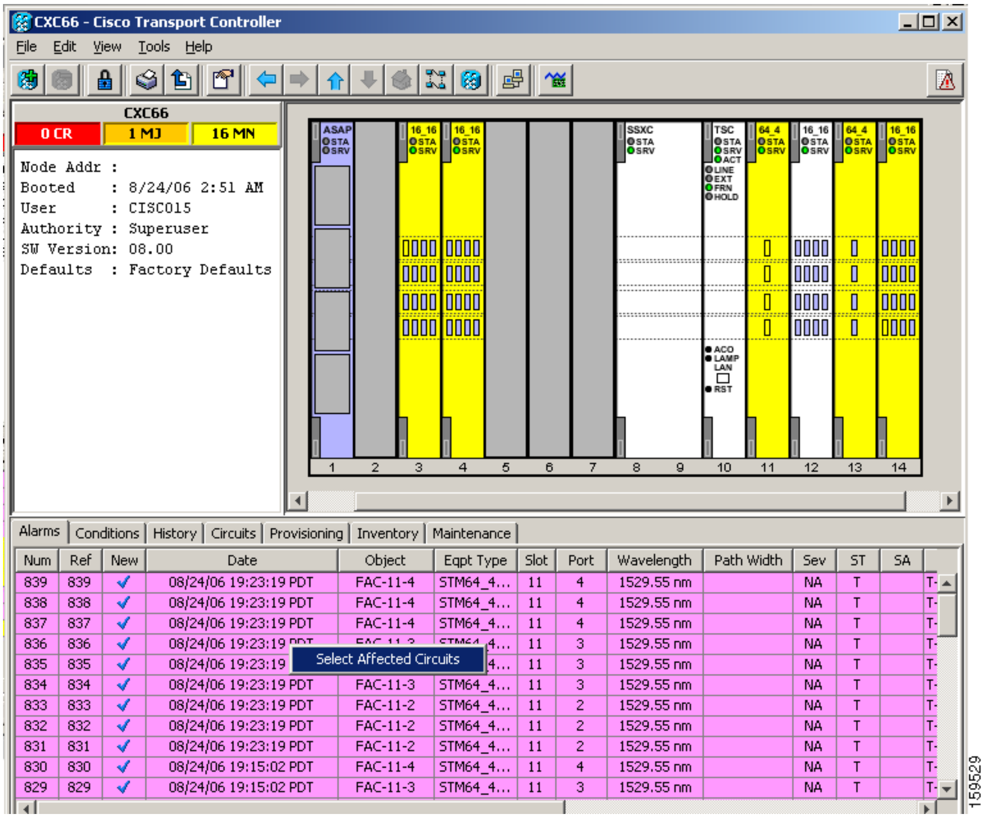
Step 2 Click the **Alarms** or **Conditions** tab and then right-click anywhere on the row of an active alarm or condition.

Note The node view is the default, but you can also navigate to the Alarms tab in the network view or card view to perform Step 2.

Note The card view is not available for the TSC or SSXC cards.

The Select Affected Circuit option shortcut menu appears (Figure 9-1).

Figure 9-1 Selecting the Affected Circuits Shortcut Menu



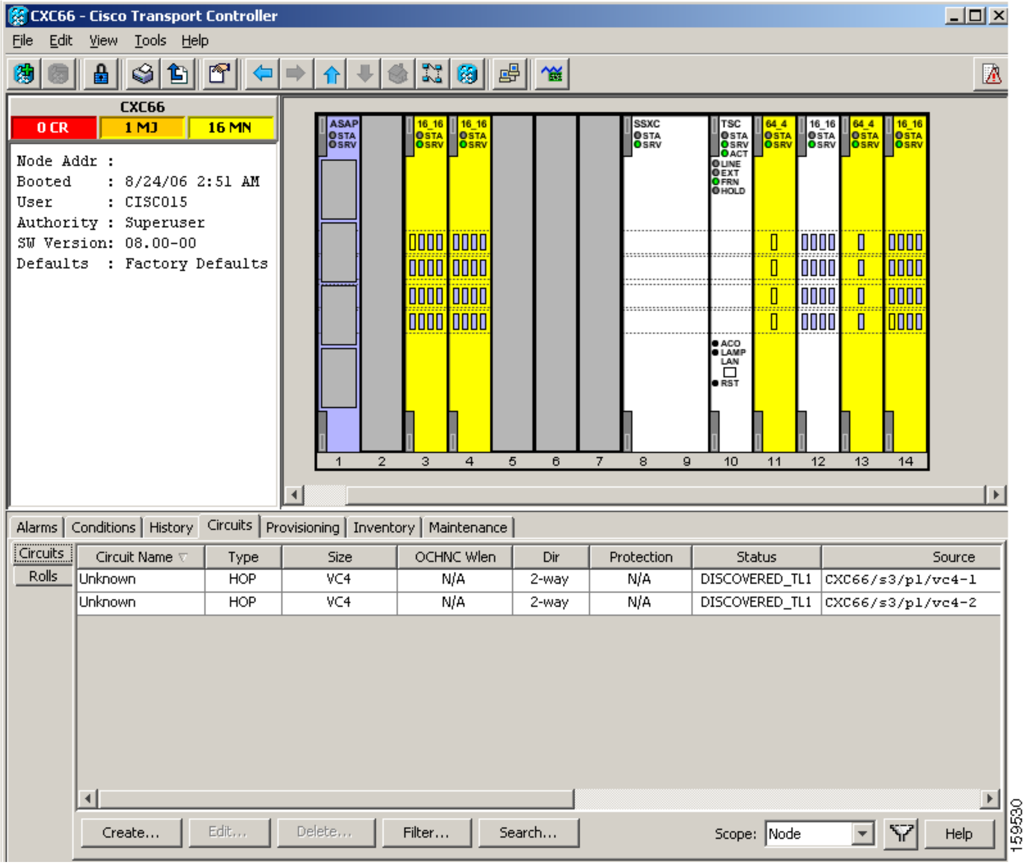
```
Node Addr :
Booted    : 8/24/06 2:51 AM
User      : CISCO15
Authority : Superuser
SW Version: 08.00
Defaults  : Factory Defaults
```

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Wavelength	Path Width	Sev	ST	SA	
839	839	✓	08/24/06 19:23:19 PDT	FAC-11-4	STM64_4...	11	4	1529.55 nm		NA	T		T-
838	838	✓	08/24/06 19:23:19 PDT	FAC-11-4	STM64_4...	11	4	1529.55 nm		NA	T		T-
837	837	✓	08/24/06 19:23:19 PDT	FAC-11-4	STM64_4...	11	4	1529.55 nm		NA	T		T-
836	836	✓	08/24/06 19:23:19 PDT	FAC-11-3	STM64_4...	11	3	1529.55 nm		NA	T		T-
835	835	✓	08/24/06 19:23:19		4...	11	3	1529.55 nm		NA	T		T-
834	834	✓	08/24/06 19:23:19 PDT	FAC-11-3	STM64_4...	11	3	1529.55 nm		NA	T		T-
833	833	✓	08/24/06 19:23:19 PDT	FAC-11-2	STM64_4...	11	2	1529.55 nm		NA	T		T-
832	832	✓	08/24/06 19:23:19 PDT	FAC-11-2	STM64_4...	11	2	1529.55 nm		NA	T		T-
831	831	✓	08/24/06 19:23:19 PDT	FAC-11-2	STM64_4...	11	2	1529.55 nm		NA	T		T-
830	830	✓	08/24/06 19:15:02 PDT	FAC-11-4	STM64_4...	11	4	1529.55 nm		NA	T		T-
829	829	✓	08/24/06 19:15:02 PDT	FAC-11-3	STM64_4...	11	3	1529.55 nm		NA	T		T-

Step 3 Click **Select Affected Circuits**.

The Circuits window appears with affected circuits highlighted (Figure 9-2).

Figure 9-2 Affected Circuit Appears for Alarm


CXC66 - Cisco Transport Controller
File Edit View Tools Help
CXC66
0 CR
1 MJ
16 MN
ASAP
16_16
SSXC
TSC
64_4
STA
SRV
ACT
LINE
EXT
FRN
HOLD
ACO
LAMP
LAN
RST
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Alarms Conditions History Circuits Provisioning Inventory Maintenance
Circuits
Rolls
Create... Edit... Delete... Filter... Search...
Scope: Node
Help
159530

```
Node Addr :
Booted    : 8/24/06 2:51 AM
User      : CISCO15
Authority : Superuser
SW Version: 08.00-00
Defaults  : Factory Defaults
```

Circuit Name	Type	Size	OCHNC Wlen	Dir	Protection	Status	Source
Unknown	HOP	VC4	N/A	2-way	N/A	DISCOVERED_TL1	CXC66/s3/p1/vc4-1
Unknown	HOP	VC4	N/A	2-way	N/A	DISCOVERED_TL1	CXC66/s3/p1/vc4-2

Stop. You have completed this procedure.

NTP-F194 Create, Assign, and Delete Alarm Severity Profiles

Purpose	This procedure changes the default severity for certain alarms (or creates, assigns, or deletes an alarm profile).
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to create an alarm profile. If you are already logged in, continue with Step 2 to create, clone, or modify an alarm profile, or go to STEP 3 to download an alarm profile.

Step 2 Complete the "DLP-F199 Create Alarm Severity Profiles" task on page 16-59 task. This tasks clones a current alarm profile, renames the profile, and customize the new profile.

Step 3 Complete the "DLP-F384 Download an Alarm Severity Profile" task on page 18-97. This task downloads an alarm severity profile from a CD or a node.

Note After storing a created or downloaded alarm profile, you must go to the node (either by logging into it or clicking on it from the network view) and activate the profile by applying it to the shelf, one or more cards, or one or more ports.

Step 4 As necessary, complete the "DLP-F200 Apply Alarm Profiles for Ports and Cards" task on page 17-1 or the "DLP-F201 Apply Alarm Profiles to Cards and Nodes" task on page 17-3.

Step 5 As necessary, complete the "DLP-F285 Delete Alarm Severity Profiles" task on page 17-76.

Stop. You have completed this procedure.

NTP-F195 Suppress and Restore Alarm Reporting

Purpose	This procedure prevents alarms from being reported on ONS 15600 SDH ports, cards, or nodes when an alarm or condition exists but you do not want it to appear in the Alarms or History windows. Also use this procedure to discontinue alarm suppression.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-F202 Suppress Alarm Reporting" task on page 17-3 to provision the node to send out autonomous messages to clear any raised alarms.

Step 3 Complete the "DLP-F203 Restore Alarm Reporting" task on page 17-5 to remove the suppress-alarms command and provision the node to send out autonomous messages to raise any actively suppressed alarms.

Stop. You have completed this procedure.

CHAPTER 10

Change Card Settings

This chapter explains how to change transmission settings on cards in a Cisco ONS 15600 SDH.

Before You Begin

As necessary, complete the "NTP-F188 Document Existing Provisioning" procedure on page 9-1.

Before performing the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* as necessary.

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

1. NTP-F196 Manage Pluggable Port Modules on the ASAP Card, page 10-1—Complete this procedure to provision a multirate pluggable port module (PPM), provision or change the line rate or wavelength on a PPM, or delete a PPM.
2. NTP-F197 Modify Line and Status Thresholds for Optical Ports, page 10-2—As needed, complete this procedure to change line (drop) and threshold settings for all STM-N cards.
3. NTP-F198 Change an Optical Port to SONET, page 10-3—As needed, complete this procedure to change an optical port from SDH to SONET.
4. NTP-F199 Change the Card Service State, page 10-4—As needed, complete this procedure to change the card service state.

NTP-F196 Manage Pluggable Port Modules on the ASAP Card

Purpose	The ASAP card hosts a total of four 4PIO or 1PIO modules. Small-form factor pluggables (SFPs) provide a fiber interface to 4PIO modules, and XFPs provide a fiber interface to 1PIO modules. A line rate (STM-1, STM-4, STM-16, STM-64, or Gigabit Ethernet) must be assigned to each SFP/XFP. In CTC, SFPs and XFPs are known as PPMs.Use this procedure to provision multirate PPMs, provision or change the optical line rate on a multirate PPM, or delete PPMs. PPMs
Tools/Equipment	None

Prerequisite Procedures	NTP-F120 Install the ASAP Card, page 2-6 DLP-F385 Install the ASAP 1PIO and 4PIO (PIM) Modules, page 18-98 DLP-F388 Install an SFP/XFP, page 18-104 or DLP-F335 Preprovision an SFP, page 18-35
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 to log into an ONS 15600 SDH on the network. If you are already logged in, continue with Step 2.

Step 2 In network view, click the **Alarms** tab:

a. Verify that the alarm filter is not turned on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 as necessary.

b. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

c. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export alarm and condition information.

Step 3 Complete the DLP-F358 Provision a Multirate PPM, page 18-70 if you installed a multirate SFP on a 4PIO module. If you preprovisioned the SFP, skip this step and continue with Step 4.

Step 4 Complete the "DLP-F391 Provision an Optical Line Rate and Wavelength" task on page 18-107 to assign an STM-1, STM-4, STM-16, or Gigabit Ethernet line rate on an SFP installed on a 4PIO module, or to assign an STM-64 line rate on an XFP installed on a 1PIO module.

Step 5 Complete the "DLP-F359 Change the Optical Line Rate" task on page 18-71 as needed.

Step 6 Complete the "DLP-F360 Delete a PPM" task on page 18-72 as needed.

Stop. You have completed this procedure.

NTP-F197 Modify Line and Status Thresholds for Optical Ports

Purpose	This procedure changes line settings, line status (in service or out of service), and performance monitoring (PM) thresholds for STM-16 cards, STM-64 cards, and STM-N ports on the ASAP card.
Tools/Equipment	None
Prerequisite Procedures	NTP-F119 Install the STM-N Cards, page 2-4 or NTP-F120 Install the ASAP Card, page 2-6
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to change the settings. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Step 3 Perform any of the following tasks as needed:

- DLP-F393 Change Line Transmission Settings for STM-N Cards, page 18-111
- DLP-F394 Change Threshold Settings for STM-N Ports, page 18-115
- DLP-F395 Change Optics Threshold Settings for STM-N Ports, page 18-117
- DLP-F396 Change the STM-N Port ALS Maintenance Settings, page 18-119

Step 4 As needed, complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Note See Chapter 9, "Manage Alarms" for information about the Alarm Behavior tab, including alarm profiles and alarm suppression.

Stop. You have completed this procedure.

NTP-F198 Change an Optical Port to SONET

Purpose	This procedure provisions a port on an STM-N card for SONET. The port must be in the Locked,maintenance administrative state before you change the port from SDH to SONET.
Tools/Equipment	None
Prerequisite Procedures	NTP-F199 Change the Card Service State, page 10-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to change the settings. If you are already logged in, continue with Step 2.

Step 2 Double-click the STM-N card where you want to provision a port for SONET.

Step 3 Click the **Provisioning > Line** tabs. (Click the **Provisioning > Optical > Line** tabs for the ASAP card.)

Step 4 In the Type field, specify the port and choose SDH.

Note Before you can change the port type from SDH to SONET, ensure the following: the EnableSyncMsg and SendDoNotUse fields are unchecked, the card is not part of an MS-SPRing or 1+1 protection group, the card is not part of an orderwire channel, and the card is not an SDH data communications channel/generic communications channel (DCC/GCC) termination point.

Step 5 Click **Apply**.

Step 6 You can repeat Steps 4 and 5 for any other ports on that card.

Stop. You have completed this procedure.

NTP-F199 Change the Card Service State

Purpose	This procedure changes a card or port's service state. The service state is an autonomously generated state that gives the overall condition of the port.
Tools/Equipment	None
Prerequisite Procedures	NTP-F120 Install the ASAP Card, page 2-6 or
	NTP-F119 Install the STM-N Cards, page 2-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to change the card service state.

Step 2 Click the **Inventory** tab.

Step 3 Click **Admin State** for the card you want to change, and choose an Admin state from the drop-down list: **Unlocked** (In service) or **Locked,maintenance** (Out of service and in maintenance).

Step 4 Click **Apply**.

Step 5 If an error message appears indicating that the card state cannot be changed from its current state, click **OK**.

Depending on the Admin State you choose, the card or port/PPM transitions to a different service state. For more information about the service states and card state transitions, refer to the "Administrative and Service States" appendix of the *Cisco ONS 15600 SDH Reference Manual*.

Stop. You have completed this procedure.

CHAPTER 11

Change Node Settings

This chapter explains how to modify provisioning for the Cisco ONS 15600 SDH. To provision a new node, see Chapter 4, "Turn Up a Node."

Before You Begin

Before performing the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* as needed.

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

1. NTP-F200 Change Node Management Information, page 11-2—Complete as needed to change node name, contact information, latitude, longitude, date, and time.
2. NTP-F201 Change CTC Network Access, page 11-2—Complete as needed to change the IP address, default router, subnet mask, and network configuration settings, and to modify static routes.
3. NTP-F202 Modify OSI Provisioning, page 11-3—Complete this procedure as needed to modify Open System Interconnection (OSI) parameters including the OSI routing mode, Target Identifier Address Resolution Protocol (TARP), routers, subnets, and IP-over-OSI tunnels.
4. NTP-F203 Customize the CTC Network View, page 11-4—Complete as needed to customize the appearance of the network map.
5. NTP-F204 Modify or Delete Optical 1+1 Port Protection Settings, page 11-4—Complete as needed to modify and delete 1+1 protection groups.
6. NTP-F205 Change Node Timing, page 11-5—Complete as needed to make changes to the ONS 15600 SDH timing parameters.
7. NTP-F206 Modify Users and Change Security, page 11-6—Complete as needed to make changes to user settings and to delete users.
8. NTP-F207 Change SNMP Settings, page 11-6—Complete as needed to modify or delete Simple Network Management Protocol (SNMP) properties.
9. NTP-F208 Change the Internal IP Addresses for the TSC Cards Using CTC, page 11-7—Complete as needed to change the internal subnet address on the TSC cards.
10. NTP-F209 Modify or Delete Communications Channel Terminations, page 11-8—Complete this procedure as needed to modify or delete regenerator-section (RS-DCC) and multiplex-section (MS-DCC) data communication channel (DCC) terminations or provisionable patchcords.

NTP-F200 Change Node Management Information

Purpose	This procedure changes node name, date, time, contact information, and the login legal disclaimer.
Tools/Equipment	None
Prerequisite Procedures	NTP-F133 Set Up Date, Time, and Contact Information, page 4-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Step 3 Complete the "DLP-F265 Change the Node Name, Date, Time, and Contact Information" task on page 17-56.

Step 4 As needed, complete the "DLP-F184 Change the Login Legal Disclaimer" task on page 16-37.

Step 5 After you confirm the changes, complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Stop. You have completed this procedure.

NTP-F201 Change CTC Network Access

Purpose	This procedure changes essential network information, including IP settings, static routes, and Open Shortest Path First (OSPF) options.
Tools/Equipment	None
Prerequisite Procedures	NTP-F135 Set Up CTC Network Access, page 4-6
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Additional ONS 15600 SDH networking information and procedures, including IP addressing examples, static route scenarios, OSPF protocol, and routing information protocol (RIP) options are provided in the *Cisco ONS 15600 SDH Reference Manual*.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Step 3 As needed, complete the following tasks:

- DLP-F219 Change IP Settings, page 17-18

- DLP-F186 Create a Static Route, page 16-41
- DLP-F221 Delete a Static Route, page 17-19
- DLP-F222 Disable OSPF, page 17-20
- DLP-F317 Delete a Proxy Tunnel, page 18-18
- DLP-F318 Delete a Firewall Tunnel, page 18-18

Step 4 Complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Stop. You have completed this procedure.

NTP-F202 Modify OSI Provisioning

Purpose	This procedure modifies the ONS 15600 SDH OSI parameters including the OSI routing mode, TARP, routers, subnets, and IP-over-CLNS tunnels. CLNS stands for connectionless network layer service.
Tools/Equipment	None
Prerequisite Procedures	NTP-F143 Provision OSI, page 4-14
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Additional information about the ONS 15600 SDH implementation of OSI is provided in the "Management Network Connectivity" chapter of the *Cisco ONS 15600 SDH Reference Manual.*

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Step 3 Perform any of the following tasks as needed:

- DLP-F362 Provision or Modify TARP Operating Parameters, page 18-74
- DLP-F363 Add a Static TID-to-NSAP Entry to the TARP Data Cache, page 18-76
- DLP-F364 Remove a Static TID-to-NSAP Entry from the TARP Data Cache, page 18-77
- DLP-F365 Add a TARP Manual Adjacency Table Entry, page 18-77
- DLP-F370 Remove a TARP Manual Adjacency Table Entry, page 18-81
- DLP-F371 Change the OSI Routing Mode, page 18-82
- DLP-F372 Edit the OSI Router Configuration, page 18-83
- DLP-F373 Edit the OSI Subnetwork Point of Attachment, page 18-84
- DLP-F374 Edit an IP-Over-CLNS Tunnel, page 18-84
- DLP-F375 Delete an IP-Over-CLNS Tunnel, page 18-85

Step 4 Complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Stop. You have completed this procedure.

NTP-F203 Customize the CTC Network View

Purpose	This procedure modifies the Cisco Transport Controller (CTC) network view, including grouping nodes into domains for a neater display, changing the network view background color, and using a custom image for the network view background.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 for instructions. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the following tasks:

- DLP-F223 Change the Network View Background Color, page 17-21
- DLP-F224 Change the Default Network View Background Map, page 17-21
- DLP-F225 Apply a Custom Network View Background, page 17-22
- DLP-F226 Create Domain Icons, page 17-23
- DLP-F227 Manage Domain Icons, page 17-23
- DLP-F266 Enable Dialog Box Do-Not-Display Option, page 17-57
- DLP-F386 Consolidate Links in Network View, page 18-100

Stop. You have completed this procedure.

NTP-F204 Modify or Delete Optical 1+1 Port Protection Settings

Purpose	This procedure modifies or deletes port protection settings on optical cards.
Tools/Equipment	None
Prerequisite Procedures	NTP-F138 Create a 1+1 Protection Group, page 4-10
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Modifying and deleting protection groups can be service affecting.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged into the correct node, continue with Step 2.

Step 2 Complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Step 3 As needed, complete any of the following tasks or procedures:

- DLP-F228 Modify a 1+1 Protection Group, page 17-25
- DLP-F229 Delete a 1+1 Protection Group, page 17-25
- NTP-F209 Modify or Delete Communications Channel Terminations, page 11-8

Step 4 Complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Stop. You have completed this procedure.

NTP-F205 Change Node Timing

Purpose	This procedure changes the SDH timing settings for the ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	NTP-F137 Set Up Timing, page 4-9
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Step 3 As needed, complete the "DLP-F230 Change the Node Timing Source" task on page 17-26.

Step 4 If you need to change any internal timing settings, follow the "DLP-F189 Set Up Internal Timing" task on page 16-47 for the settings you need to modify. For more information about each field, see the "DLP-F188 Set Up External or Line Timing" task on page 16-45.

Caution Internal timing is Stratum 3E and not intended for permanent use. All ONS 15600 SDHs should be timed to a Stratum 2 or better primary reference source.

Step 5 As needed, complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Stop. You have completed this procedure.

NTP-F206 Modify Users and Change Security

Purpose	This procedure modifies user and security properties for the ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	NTP-F132 Create Users and Assign Security, page 4-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Step 3 To view logged-on users, click the **Provisioning > Security > Active Logins** tabs.

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

- DLP-F267 Change Security Policy on a Single Node, page 17-58
- DLP-F268 Change Security Policy on Multiple Nodes, page 17-59
- DLP-F269 Change User Password and Security Levels for a Single Node, page 17-61
- DLP-F270 Change User and Security Settings for Multiple Nodes, page 17-62
- DLP-F383 Grant Superuser Privileges to a Provisioning User, page 18-96
- DLP-F289 Manually Lock or Unlock a User on a Single Node, page 17-80
- DLP-F290 Manually Lock or Unlock a User on Multiple Nodes, page 17-81
- DLP-F271 Log Out a User on a Single Node, page 17-62
- DLP-F272 Log Out a User on Multiple Nodes, page 17-63
- DLP-F231 Delete a User from a Single Node, page 17-27
- DLP-F232 Delete a User From Multiple Nodes, page 17-27
- DLP-F381 Configure the Node for RADIUS Authentication, page 18-93

Step 5 As needed, complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Stop. You have completed this procedure.

NTP-F207 Change SNMP Settings

Purpose	This task modifies SNMP properties for the ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	NTP-F139 Set Up SNMP, page 4-11
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Step 3 As needed, complete the following tasks:

- DLP-F233 Modify SNMP Trap Destinations, page 17-28
- DLP-F234 Delete SNMP Trap Destination, page 17-29

Step 4 As needed, complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Stop. You have completed this procedure.

NTP-F208 Change the Internal IP Addresses for the TSC Cards Using CTC

Purpose	This procedure changes the class B subnet address for the TSC cards. You should change the class B subnet address if your internal network uses the same address range as the default subnet addresses to avoid IP address conflict.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2 DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution All network changes should be approved by your network or LAN administrator.

Note This procedure causes the node to reboot.

Step 1 From node view, click the **Provisioning** > **Network > Internal Subnet** tabs.

Step 2 Complete the following information in the fields listed:

- TSC A—Enter the class B subnet address for the first TSC.
- TSC B—If two TSC cards are installed, enter the class B subnet address for the second TSC card.

Step 3 Click **Apply**. A confirmation dialog box appears.

Step 4 Verify that the information is correct and click **Yes**.

Stop. You have completed this procedure.

NTP-F209 Modify or Delete Communications Channel Terminations

Purpose	This procedure changes or deletes RS-DCC and MS-DCC terminations.
Tools/Equipment	None
Prerequisite Procedures	"DLP-F253 Provision RS-DCC Terminations" task on page 17-46 or "DLP-F314 Provision MS-DCC Terminations" task on page 18-14
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

⚠ **Caution** Deleting a DCC termination can cause you to lose visibility of nodes that do not have other DCCs or network connections to the CTC computer.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the following tasks to modify DCC settings:

- To modify an RS-DCC termination, complete the "DLP-F319 Change an RS-DCC Termination" task on page 18-19.
- To modify an MS-DCC termination, complete the "DLP-F320 Change an MS-DCC Termination" task on page 18-19.

Step 3 As needed, complete the following tasks to delete DCC terminations:

- To delete a RS-DCC termination, complete the "DLP-F321 Delete an RS-DCC Termination" task on page 18-20.
- To delete an MS-DCC termination, complete the "DLP-F322 Delete an MS-DCC Termination" task on page 18-20.

Stop. You have completed this procedure.

CHAPTER 12

Convert Network Configurations

This chapter explains how to convert from one SDH topology to another in a Cisco ONS 15600 SDH network. For initial network turn-up, see "Turn Up a Network."

Before You Begin

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

1. "NTP-F210 Convert a Point-to-Point to a Linear ADM Automatically" task on page 12-1—Complete as needed.
2. "NTP-F211 Convert a Point-to-Point to a Linear ADM Manually" task on page 12-3—Complete as needed if the in-service topology upgrade wizard is not available or you need to back out of the wizard.
3. "NTP-F212 Convert a Point-to-Point or Linear ADM to a Two-Fiber MS-SPRing Manually" task on page 12-5—Complete as needed.
4. "NTP-F213 Modify an MS-SPRing" task on page 12-7—Complete as needed.

NTP-F210 Convert a Point-to-Point to a Linear ADM Automatically

Purpose	This procedure upgrades a 1+1 point-to-point configuration (two nodes) to a linear add/drop multiplexing (ADM) configuration (three or more nodes) without disrupting traffic.
Tools/Equipment	Compatible hardware necessary for the upgrade (for example, ASAP cards) Attenuators might be needed for some applications.

Prerequisite Procedures	NTP-F145 Provision a Point-to-Point Connection **Note** This procedure requires that the node to be added is reachable (has IP connectivity with Cisco Transport Controller [CTC]).Two technicians who can communicate with each other during the upgrade might be needed if the PC running CTC and the ONS 15600 SDH nodes are not at the same location.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note STM-N transmit and receive levels should be in their acceptable range as shown in the specifications for each card in Table 2-2 on page 2-10.

Note If overhead circuits exist on the network, an in-service topology upgrade is service-affecting. The overhead circuits will drop traffic and have a status of PARTIAL after the upgrade is complete.

Step 1 Complete the "“DLP-F181 Log into CTC” task on page 16-34 at either of the point-to-point nodes. If you are already logged in, continue with Step 2.

Step 2 In network view, right-click the span between the two nodes where you want to add the new node. A dialog box appears.

Step 3 Choose **Upgrade Protection**. A drop-down list appears.

Step 4 Choose **Terminal to Linear** and the first page of the wizard, Upgrade Protection: Terminal to Linear, appears. The dialog box lists the following conditions for adding a new node:

- The terminal network has no critical or major alarms.
- The node that you will add has no critical or major alarms.
- The node has a compatible software version with that of the terminal nodes.
- The node has four unused optical ports matching the speed of the 1+1 protection and no communications channel has been provisioned on these four ports.
- Fiber is available to connect the added node to the terminal nodes.

Step 5 If all conditions listed in Step 4 are met, click **Next**.

Note If you are attempting to add an unreachable node, you must first log into the unreachable node using a separate CTC session and configure that node. Delete any existing protection groups as described in the "“DLP-F229 Delete a 1+1 Protection Group” task on page 17-25. Delete any existing data communications channel (DCC) terminations as described in the "“DLP-F321 Delete an RS-DCC Termination” task on page 18-20 or the "“DLP-F322 Delete an MS-DCC Termination” task on page 18-20.

Step 6 Enter the node host name or IP address or choose the name of the new node from the drop-down list. If you type in the name, make sure it is identical to the actual node name. The node name is case sensitive.

Step 7 Click **Next**. The Select Protection Group Ports page appears.

Step 8 From the drop-down lists, select the working and protect ports on the new node that you want to connect to each terminal node.

Step 9 Click **Next**. The Re-fiber the Protected Path page appears. Follow the instructions on the page for connecting the fibers between the nodes.

Step 10 When the fibers are connected properly, click **Next**. The Update Circuit(s) on Node-Name page appears.

Note The Back button is not enabled in the wizard. You can click the **Cancel** button at this point and click **Yes** if you want to cancel the Upgrade Protection procedure. If the procedure fails after you have physically moved the fiber-optic cables, you must restore the fiber-optic cables to their original positions and verify (through CTC) that traffic is on the working path of the nodes before restarting the process. To check the traffic status, go to node view and click the **Maintenance > Protection** tabs. In the Protection Groups area, click the 1+1 protection group. You can see the status of the traffic in the Selected Group area.

Step 11 Click **Next**. The Force Traffic to Protect Path page appears, stating that it is about to force the traffic from the working path to the protect path for the terminal nodes.

Step 12 Click **Next**.

Step 13 Follow each step as instructed by the wizard as it guides you through the process of refibering the working path between nodes and forcing the traffic back to the working path. The final page informs you when you have completed the procedure of upgrading from terminal to linear protection.

Step 14 Click **Finish**.

Stop. You have completed this procedure.

NTP-F211 Convert a Point-to-Point to a Linear ADM Manually

Purpose	This procedure converts a 1+1 point-to-point configuration (two nodes) to a linear ADM configuration (three or more nodes) manually, that is, without using the in-service topology upgrade wizard. Use this procedure if the wizard is unavailable or if you need to back out of the wizard.
Tools/Equipment	None
Prerequisite Procedures	NTP-F145 Provision a Point-to-Point Connection
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution This procedure is service-affecting.

Note Optical transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in Table 2-2 on page 2-10.

Note In a point-to-point configuration, two STM-N cards are connected to two STM-N cards on a second node.

Step 1 Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at either of the point-to-point nodes. If you are already logged in, continue with Step 2.

Step 2 Complete the ""DLP-F273 Check the Network for Alarms and Conditions" task on page 17-64.

Step 3 Log into the node that will be added to the point-to-point configuration (the new node).

Note If you are attempting to add an unreachable node, you must first log into the unreachable node using a separate CTC session and configure that node. Delete any existing protection groups as described in the ""DLP-F229 Delete a 1+1 Protection Group" task on page 17-25. Delete any existing data communications channel (DCC) terminations as described in the ""DLP-F321 Delete an RS-DCC Termination" task on page 18-20 or the ""DLP-F322 Delete an MS-DCC Termination" task on page 18-20.

Step 4 Verify that the new node has four STM-N ports at the same rate as the point-to-point node.

Step 5 Complete the "F144 Verify Node Turn-Up" procedure for the new node.

Step 6 Physically connect the fibers between the point-to-point node you are logged into and the new node.

Step 7 On the new node, create a 1+1 protection group for the STM-N cards that will connect to the point-to-point node. See the "NTP-F138 Create a 1+1 Protection Group" procedure on page 4-8 for instructions.

Step 8 Complete the "DLP-F253 Provision RS-DCC Terminations" task on page 17-46 for the working STM-N ports in the new node that will connect to the linear ADM network. (Alternatively, if additional bandwidth is needed for CTC management, complete the "DLP-F314 Provision MS-DCC Terminations" task on page 18-14.) Make sure to set the port state in the Create RS-DCC Termination dialog box to **Unlocked**.

Note DCC failure alarms appear until you create DCC terminations in the point-to-point node during Step 13.

Step 9 From the View menu, choose **Go To Network View**.

Step 10 Double-click the point-to-point node that will connect to the other side of the new node.

Step 11 Ensure that this point-to-point node has STM-N cards installed that can connect to the new node.

Step 12 Create a 1+1 protection group for the STM-N ports that will connect to the new node. See the "NTP-F138 Create a 1+1 Protection Group" procedure on page 4-8 for instructions.

Step 13 Create DCC terminations on the working STM-N port that will connect the new node. See the "DLP-F253 Provision RS-DCC Terminations" task on page 17-46 or the "DLP-F314 Provision MS-DCC Terminations" task on page 18-14. In the Create RS-DCC Termination dialog box, set the port state to Unlocked.

Step 14 From the View menu, choose**Go To Network View**.

Step 15 Double-click the new node.

Step 16 Complete the "NTP-F137 Set Up Timing" task on page 4-9 for the new node. If the new node is using line timing, make the working STM-N card the timing source.

Step 17 Display the network view to verify that the newly created linear ADM configuration is correct. A single green span line should appear between each linear node.

Step 18 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 for instructions.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Step 19 Repeat the procedure for each node that you want to add to the linear ADM. To create circuits, see Chapter 6, "Create Circuits."

Stop. You have completed this procedure.

NTP-F212 Convert a Point-to-Point or Linear ADM to a Two-Fiber MS-SPRing Manually

Purpose	This procedure upgrades a point-to-point configuration to a two-fiber multiplex section-shared protection ring (MS-SPRing).
Tools/Equipment	None
Prerequisite Procedures	NTP-F145 Provision a Point-to-Point Connection
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution This procedure is potentially service-affecting.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at one of the nodes that you want to convert from a point-to-point or ADM configuration to an MS-SPRing. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-F273 Check the Network for Alarms and Conditions" task on page 17-64.

Step 3 Right-click a span adjacent to the node you are logged into.

Step 4 From the shortcut menu, choose **Circuits**. The Circuits on Span window appears.

Step 5 Verify that the total number of active virtual container (VC) circuits does not exceed 50 percent of the span bandwidth. In the Circuits column there is a block titled "Unused." This number should exceed 50 percent of the span bandwidth.

Note For AU4, if the span is an STM-16, no more than 8 VCs can be provisioned on the span. For AU4, if the span is an STM-64, no more than 32 VCs can be provisioned on the span. For AU3, if the span is STM-16 no more than 24 VCs can be provisioned on the span. For AU3, if the span is an STM-64, no more than 64 VCs can be provisioned on the span.

Caution If the first half of the capacity is exceeded, this procedure cannot be completed. Bandwidth must be 50 percent unassigned to convert to an MS-SPRing. Refer to local procedures for relocating circuits if these requirements are not met.

Step 6 Repeat Steps 3 through 5 at each node in the point-to-point or linear ADM that you will convert to the MS-SPRing. If all nodes comply with Step 5, continue with Step 7.

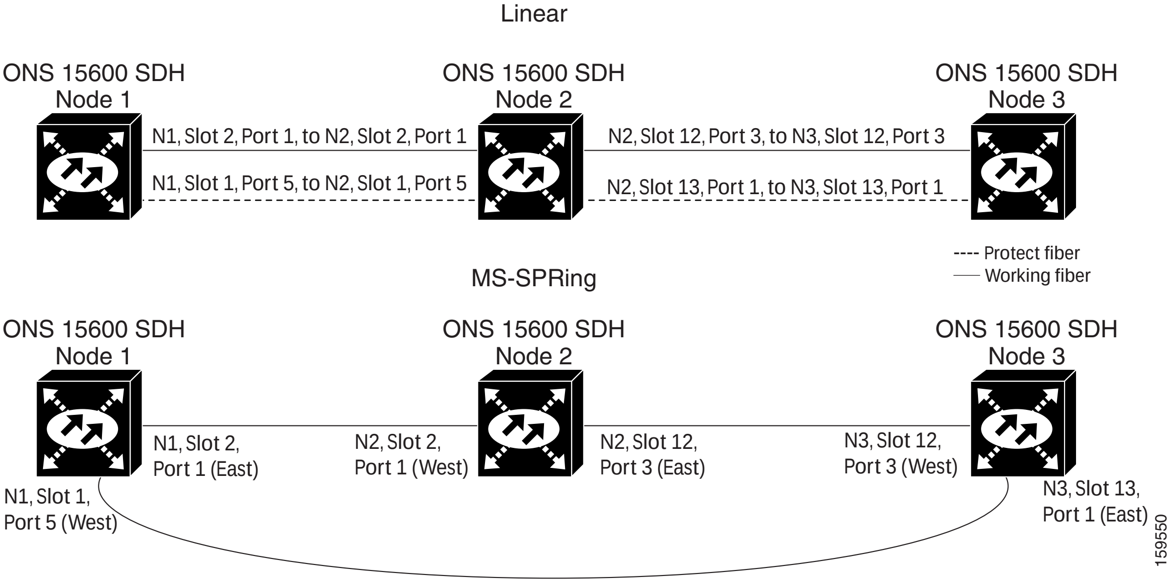
Step 7 Complete the Chapter 17, "F247 Verify that a 1+1 Working Port is Active." for every 1+1 protection group that supports a span in the point-to-point or linear ADM network.

Step 8 Complete the Chapter 17, "F229 Delete a 1+1 Protection Group."at each node that supports the point-to-point or linear ADM span.

Step 9 Complete the Chapter 17, "F254 Change the Service State for a Port." to put the protect ports out of service at each node that supports the point-to-point or linear ADM span.

Step 10 For linear ADMs, physically remove the protect fibers from all nodes in the linear ADM network. For example, in Figure 12-1 you could remove the fiber running from Node 2/Slot 13/Port 1 to Node 3/Slot 13/Port 1.

Figure 12-1 Linear ADM to MS-SPRing Conversion


Linear
ONS 15600 SDH Node 1
ONS 15600 SDH Node 2
ONS 15600 SDH Node 3
N1, Slot 2, Port 1, to N2, Slot 2, Port 1
N1, Slot 1, Port 5, to N2, Slot 1, Port 5
N2, Slot 12, Port 3, to N3, Slot 12, Port 3
N2, Slot 13, Port 1, to N3, Slot 13, Port 1
---- Protect fiber
—— Working fiber
MS-SPRing
ONS 15600 SDH Node 1
ONS 15600 SDH Node 2
ONS 15600 SDH Node 3
N1, Slot 2, Port 1 (East)
N2, Slot 2, Port 1 (West)
N2, Slot 12, Port 3 (East)
N3, Slot 12, Port 3 (West)
N1, Slot 1, Port 5 (West)
N3, Slot 13, Port 1 (East)
159550

Step 11 Create the ring by connecting the protect fiber from one end node to the protect port on the other end node. For example, the fiber between Node 1/Slot 1/Port 5 and Node 2/Slot 1/Port 5 (Figure 12-1) can be rerouted to connect Node 1/Slot 1/Port 5 to Node 3/Slot 13/Port 1.

Note If you need to physically remove any STM-N cards, do so now. In this example, cards in Node 2/Slots 1 and 13 can be removed. See the .

Step 12 In network view, click the **Circuits** tab and complete the "DLP-F379 Export CTC Data" task on page 18-88 to save the circuit data to a file on your hard drive.

Step 13 Complete the "DLP-F253 Provision RS-DCC Terminations" task on page 17-46at the end nodes to provision the slot in each node that is not already in the RS-DCC Terminations list.

Step 14 For circuits provisioned on an AU4 VC that is now part of the protection bandwidth (VCs 9 to 16 for an STM-16 MS-SPRing, and VCs 33 to 64 for an STM-64 MS-SPRing), delete and recreate each circuit:

Note Deleting circuits is service-affecting.

a. Complete the "DLP-F293 Delete Circuits" task on page 17-83 for one circuit.

b. Create the AU4 circuit on VCs 1 to 8 for an STM-16 MS-SPRing, or 1 to 32 for an STM-64 MS-SPRing on the fiber that served as the protect fiber in the linear ADM. See the "DLP-F165 Connect the Office Ground to the ONS 15600 SDH" task on page 16-7 procedure for instructions.

c. Repeat Steps a and b for each circuit residing on an MS-SPRing protect VC.

Step 15 Complete the NTP-F148 Create an MS-SPRing procedure to put the nodes into an MS-SPRing.

Stop. You have completed this procedure.

NTP-F213 Modify an MS-SPRing

Purpose	This procedure changes an MS-SPRing ring ID, node ID, or ring and span reversion times.
Tools/Equipment	None
Prerequisite Procedures	NTP-F148 Create an MS-SPRing
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node in the MS-SPRing you want to modify. If you are already logged in, continue with Step 2.

Step 2 Check the MS-SPRing for outstanding alarms and conditions. See the "DLP-F273 Check the Network for Alarms and Conditions" task on page 17-64 for instructions.

Note Some or all of the following alarms appear during MS-SPRing setup: E-W-MISMATCH, RING-MISMATCH, APSC-IMP, APSCDFLTK, and MSSP-OOSYNC. The alarms clear after you configure all the nodes in the MS-SPRing. For definitions of these alarms, refer to the Cisco ONS 15600 SDH Troubleshooting Guide.

Step 3 To change the MS-SPRing ring ID or the ring or span reversion times, complete the following steps. If you want to change a node ID, continue with Step 4.

a. In network view, click the **Provisioning > MS-SPRing** tabs.

b. Click the MS-SPRing that you want to modify and click **Edit**.

c. In the MS-SPRing window, change any of the following:

- Ring ID—If needed, change the MS-SPRing ring ID (an MS-SPRing ring ID is a 6-character string that includes letters and numbers). Do not choose an ID that is already assigned to another MS-SPRing.
- Reversion time—If needed, change the amount of time that will pass before the traffic reverts to the original working path after a ring switch.

d. Click **Apply**.

If you changed the ring ID, the MS-SPRing window closes automatically. If you only changed a reversion time, close the window by choosing Close from the File menu.

Step 4 To change an MS-SPRing node ID, complete the following steps; otherwise, continue with Step 5.

a. On the network map, double-click the node with the node ID you want to change.

b. Click the **Provisioning > MS-SPRing** tabs.

c. Choose a Node ID number. Do not choose a number already assigned to another node in the same MS-SPRing.

d. Click **Apply**.

Step 5 Verify the following:

- A green span line appears between all MS-SPRing nodes.
- All E-W-MISMATCH, RING-MISMATCH, APSC-IMP, APSCDFLTK, MSSP-OOSYNC, and APSCNMIS alarms are cleared.

Note For definitions of these alarms, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Stop. You have completed this procedure.

CHAPTER 13

Add and Remove Nodes

This chapter explains how to add and remove Cisco ONS 15600 SDH nodes from multiplex section-shared protection ring (MS-SPRing), subnetwork connection protection (SNCP) ring, and linear add/drop multiplexing (ADM) networks.

Before You Begin

See Chapter 9, "Manage Alarms" to investigate all alarms, and manually document existing provisioning. To clear trouble conditions, refer to *Cisco ONS 15600 SDH Procedure Guide, R9.0*.

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

1. NTP-F214 Add an MS-SPRing Node, page 13-1—Complete as needed.
2. NTP-F215 Remove an MS-SPRing Node, page 13-5—Complete as needed.
3. NTP-F216 Add an SNCP Node, page 13-8—Complete as needed.
4. NTP-F217 Remove an SNCP Node, page 13-11—Complete as needed.
5. NTP-F218 Add a Node to a Linear ADM, page 13-12—Complete as needed to add an ONS 15600 SDH node between two nodes in a 1+1 configuration.
6. NTP-F219 Remove an In-Service Node from a Linear ADM, page 13-14—Complete as needed to remove an ONS 15600 SDH from a linear ADM without disrupting traffic.

NTP-F214 Add an MS-SPRing Node

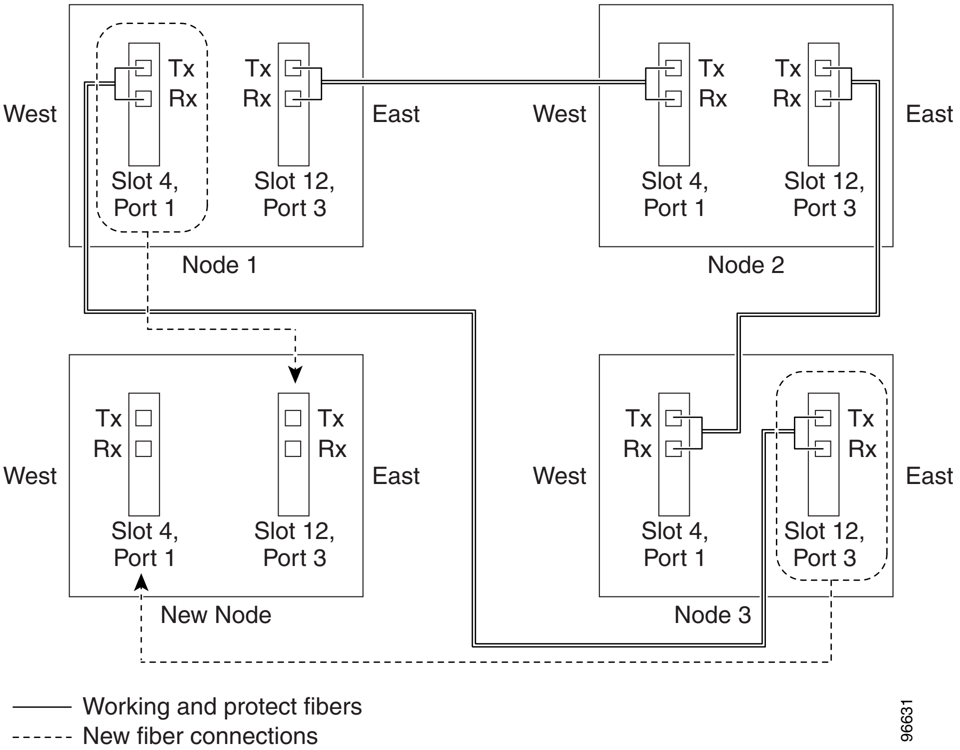
Purpose	This procedure expands an MS-SPRing by adding a node. All nodes in the ring must have the same software version.
Tools/Equipment	Fiber for new node connections
Prerequisite Procedures	Cards must be installed and node turn-up procedures completed on the node that will be added to the MS-SPRing. See Chapter 2, "Install Cards and Fiber-Optic Cable" and Chapter 4, "Turn Up a Node"
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Adding an MS-SPRing node can be service-affecting and should be performed during a maintenance window.

Step 1 Check the software version on the node you are adding to the MS-SPRing from the node view Maintenance > Software subtab. If it is not the same version as the nodes in the ring, you must upgrade or downgrade the new node to the same version as the other nodes in the ring. Refer to the release-specific software upgrade guide for more information on upgrading the ONS node software.

Step 2 Draw a diagram of the MS-SPRing where you will add the node. In the diagram, identify the east and west MS-SPRing STM-N trunk (span) cards and ports that will connect to the new node. (This information is essential to complete this procedure without error.) Figure 13-1 shows a drawing of a three-node, two-fiber MS-SPRing that uses Slot 4/Port 1 and Slot 12/Port 3 for the MS-SPRing trunk cards and ports. The dashed arrows show where the new fiber connections will be made to add a fourth node to the MS-SPRing.

Figure 13-1 Three-Node, Two-Fiber MS-SPRing Before a Fourth Node Is Added



Step 3 According to local site practice, complete the "NTP-F221 Back Up the Database" procedure on page 14-4 for all the nodes in the ring.

Step 4 Verify the card installation on the new node by completing the "NTP-F131 Verify Card Installation" procedure on page 4-2. Verify that the STM-N ports to be used as the MS-SPRing trunk ports match the MS-SPRing optical rate. For example, if the MS-SPRing is STM-16, the new node must have STM-16 ports installed. If the STM-N cards are not installed or the optical rates do not match the MS-SPRing, complete the "NTP-F119 Install the STM-N Cards" procedure on page 2-4.

Step 5 Verify that fiber is available to connect the new node to the existing nodes. Refer to the diagram drawn in Step 2.

Step 6 Complete the "NTP-F144 Verify Node Turn-Up" procedure on page 5-2. In order to have Cisco Transport Controller (CTC) visibility to the new node after adding it, you must be an authorized user on the node and you must have IP connectivity to the node.

Step 7 Create a static route on the new node if the following conditions are present. If the conditions are not present, continue with Step 8.

- The IP address for the new node is on the same subnet as other nodes in the network.
- On the new node Provisioning > Network > General subtab, Enable Socks Proxy on Port, External Network Element (ENE) is not checked under Gateway Settings.
- A CTC computer is directly connected to the new node.
- CTC computers are directly connected to other nodes on the same subnet.

If these conditions are present, add static routes on the node that will be added to the MS-SPRing, using the following settings:

- Destination IP address: *Local-PC-IP-address*
- Net Mask: **255.255.255.255**
- Next Hop: *IP-address-of-the-Cisco-ONS-15600-SDH*
- Cost: **1**

See the "DLP-F186 Create a Static Route" task on page 16-41. To view gateway settings, see the "DLP-F185 Provision IP Settings" task on page 16-38. The gateway settings area provisions the ONS 15600 SDH SOCKS proxy server features.

Step 8 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node in the MS-SPRing.

Step 9 Complete the "DLP-F281 Check MS-SPRing or SNCP Alarms and Conditions" task on page 17-73 to verify that the MS-SPRing is free of service-affecting alarms or problems. If trouble is indicated (for example, a service-affecting alarm exists), resolve the problem before proceeding. See Chapter 9, "Manage Alarms" or, if necessary, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for information.

Step 10 From the View menu, choose **Go to Network View** and click the **Provisioning > MS-SPRing** tabs.

Step 11 On paper, record the Ring Name, Ring Type, Line Rate, Ring Reversion, and Span Reversion (2 Fiber).

Step 12 From the Node column, record the Node IDs in the MS-SPRing. The Node IDs are the numbers in parentheses next to the node name.

Step 13 Log into the new node:

- If the node has a LAN connection and appears on the network map, from the View menu, choose **Go to Other Node**, then enter the new node.
- If the new node is not connected to the network, log into it using the "DLP-F181 Log into CTC" task on page 16-34.

Step 14 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for procedures.

Step 15 Using the information recorded in Steps 11 and 12 and the diagram created in Step 2, create an MS-SPRing on the new node. See the "DLP-F346 Create an MS-SPRing on a Single Node" task on page 18-49.

Step 16 (Optional) Create test circuits, making sure that they pass through the MS-SPRing trunk cards/ports, and run test traffic through the node to ensure that the cards are functioning properly. See the "DLP-F292 Single Shelf Control Card Switch Test" task on page 17-82 and the "NTP-F167 Test Optical Circuits" procedure on page 6-16 for information.

Step 17 Create the data communications channel (DCC) terminations on the new node. See the "DLP-F253 Provision RS-DCC Terminations" task on page 17-46.

Note Creating the DCC terminations causes the regenerator-section DCC (RS-DCC) Termination Failure and Loss of Signal alarms to appear. These alarms will remain active until you connect the node to the MS-SPRing.

Note If you map the K3 byte to another byte (such as E2), you must remap the ports on each side of the new node or span to the same byte. See the "DLP-F255 Remap the K3 Byte" task on page 17-49.

Step 18 Complete the "DLP-F181 Log into CTC" task on page 16-34 at an MS-SPRing node that will connect to the new node.

Step 19 Referring to the diagram created in Step 2, complete the "DLP-F347 Initiate an MS-SPRing Force Ring Switch" task on page 18-50 on the node that will connect to the new node on its west line (port).

Step 20 Referring to the diagram created in Step 2, complete the "DLP-F347 Initiate an MS-SPRing Force Ring Switch" task on page 18-50 on the node that will connect to the new node on its east line (port).

Step 21 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for procedures.

Step 22 Following the diagram created in Step 2, remove the fiber connections from the two nodes that will connect to the new node.

a. Remove the west fiber from the node that will connect to the east port of the new node. In the Figure 13-1 example, this is Node 1/Slot 4/Port 1.

b. Remove the east fiber from the node that will connect to the west port of the new node. In the Figure 13-1 example, this is Node 3/Slot 12/Port 3.

Step 23 Connect fibers from the adjacent nodes to the new node following the diagram created in Step 2. Connect the west port to the east port and the east port to the west port.

Step 24 After the newly added node appears in network view, double-click it to display the node in node view.

Step 25 Click the **Provisioning > MS-SPRing** tabs.

Step 26 Click **Ring Map**. Verify that the new node appears on the Ring Map with the other MS-SPRing nodes, then click **OK**.

Step 27 From the View menu, choose **Go to Network View** and perform the following steps:

a. Click the **Provisioning > MS-SPRing** tabs. Verify that the new node appears in the Node column.

b. Click the **Alarms** tab. Verify that MS-SPRing alarms such as RING-MISMATCH, E-W-MISMATCH, PRC-DUPID (duplicate node ID), and APSCDFLTK (default K) do not appear.

If the new node does not appear in the Node column, or if MS-SPRing alarms are displayed, log into the new node and verify that the MS-SPRing is provisioned on it correctly with the information from Steps 11 and 12. If the node still does not appear, or if alarms persist, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Step 28 Click the **Circuits** tab. Wait until all the circuits are discovered. The circuits that pass through the new node are incomplete.

Note If the circuits take more than a minute to appear, log out of CTC, then log back in.

Step 29 In network view, right-click the new node and choose **Update Circuits With The New Node** from the shortcut menu. Verify that the number of updated circuits in the dialog box is correct.

Step 30 If incomplete circuits still appear, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Step 31 Click the **History** tab. Verify that MS-SPRing_RESYNC conditions are present for every node in the MS-SPRing.

Step 32 Complete the "DLP-F282 Clear an MS-SPRing Force Ring Switch" task on page 17-74 to remove the ring switch from the east MS-SPRing span.

Step 33 According to local site practice, complete the "NTP-F149 Two-Fiber MS-SPRing Acceptance Test" procedure on page 5-8.

Stop. You have completed this procedure.

NTP-F215 Remove an MS-SPRing Node

Purpose	This procedure removes an MS-SPRing or multiple MS-SPRings from a node.
Tools/Equipment	None
Prerequisite Procedures	NTP-F148 Create an MS-SPRing, page 5-8
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution The following procedure minimizes traffic outages during node removals. You will delete all circuits that originate and terminate on the node being removed. In addition, you will verify that circuits passing through the node do not enter and exit the node on different VCs. If they do, you will delete and recreate the circuits, and traffic will be lost on that circuit during this time.

Step 1 According to local site practice, complete the "NTP-F221 Back Up the Database" procedure on page 14-4 for all the nodes in the ring.

Step 2 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node you want to remove from the MS-SPRing.

Step 3 Complete the "DLP-F237 Verify Timing in a Reduced Ring" task on page 17-30.

> **Note** If you remove a node that is the only building integrated timing supply (BITS) timing source for the ring, you also remove the only source of synchronization for all the nodes in that ring. Circuits that leave the ring to connect to other networks synchronized to a Stratum 1 clock will experience a high level of pointer adjustments, which might adversely affect traffic performance.

Step 4 Create a diagram of the MS-SPRing where you will remove the node. You can draw the MS-SPRing manually or complete the following to print the MS-SPRing map from CTC:

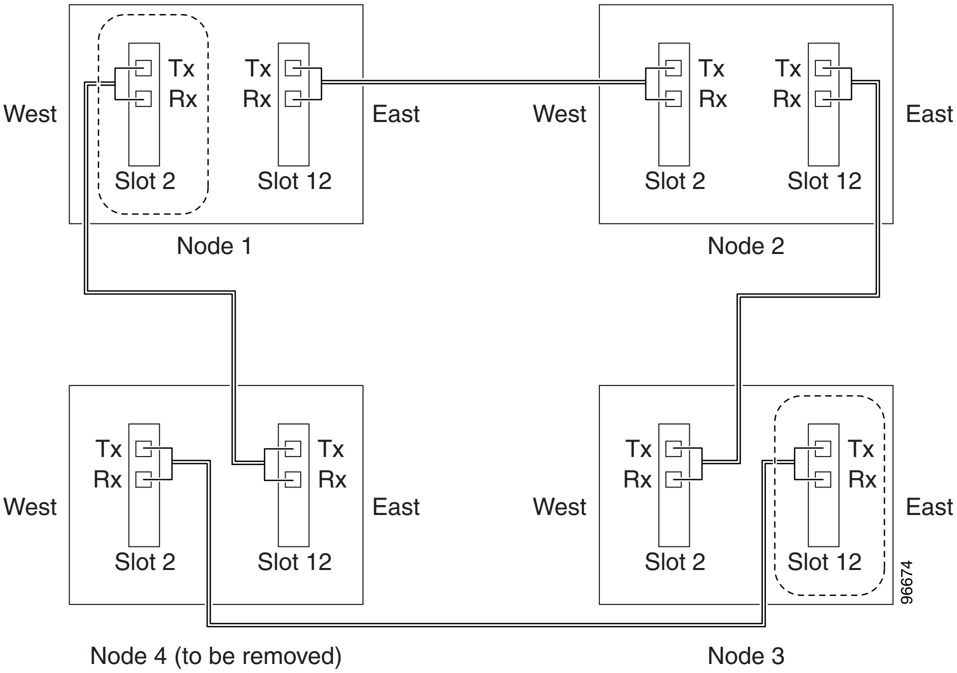
- **a.** From the View menu, choose **Go to Network View**.
- **b.** Click the **Provisioning > MS-SPRing** tabs.
- **c.** Choose the desired MS-SPRing, then click **Edit**.
- **d.** In the MS-SPRing window, verify that all the port information is visible. If not, press **Ctrl** and drag the node icons to a new location so the information can be viewed.
- **e.** Complete the "DLP-F336 Print CTC Data" task on page 18-36.
- **f.** Close the MS-SPRing window by choosing **Close** from the File menu.

Step 5 Referring to the MS-SPRing diagram, identify the following:

- The node that is connected through its west port to the target (removal) node; for example, if you were removing Node 4 in Figure 13-2, Node 1 is the node connected through its west port to Node 4.
- The node that is connected through its east port to the target (removal) node; in Figure 13-2, Node 3 is the node connected through its east port to Node 4.

Record the slot and port of the MS-SPRing ring in the node.

Figure 13-2 Four-Node, Two-Fiber MS-SPRing Before a Node Is Removed



Step 6 Complete the "DLP-F281 Check MS-SPRing or SNCP Alarms and Conditions" task on page 17-73 to verify that the MS-SPRing is free of alarms. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for instructions.

Step 7 From the View menu, choose **Go to Other Node**. Choose the node that you will remove and click **OK**.

Step 8 Click the **Circuits** tab. If the Scope setting is set to Network, choose **Node** from the Scope drop-down list. Make sure the Filter button is off (not indented) to ensure that all circuits are visible.

Step 9 Delete all circuits that originate or terminate on the node. See the "DLP-F293 Delete Circuits" task on page 17-83.

Step 10 Complete the "DLP-F334 Verify Pass-Through Circuits" task on page 18-34.

Step 11 If K3 extension byte mapping is supported on adjacent nodes, complete the "DLP-F291 Verify MS-SPRing Extension Byte Mapping" task on page 17-82. K3 extension byte mapping is supported on all ONS 15600 SDH STM-16 and STM-64 ports, as well as the ONS 15454 STM-16 card.

Step 12 From the View menu, choose **Go to Network View**.

Step 13 Referring to the diagram created in Step 4, complete the "DLP-F347 Initiate an MS-SPRing Force Ring Switch" task on page 18-50 at each node that connects to the target (removal) node to force traffic away from it. You must perform a Force switch at each port connected to the target node. For example, in Figure 13-2, you would perform a Force switch on the east port of Node 3 and the west port of Node 1.

Step 14 Click the **Alarms** tab.

- **a.** Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 as necessary.
- **b.** Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for procedures.

Step 15 Remove the fiber connections between the node being removed and the two neighboring nodes.

Step 16 Reconnect the fiber of the two neighboring nodes directly, west port to east port. For example in Figure 13-2, the east port of Node 3 (Slot 12) connects to the west port of Node 1 (Slot 5).

Step 17 Complete the following substeps:

- **a.** From the View menu, choose **Go to Other Node**. Choose one of the newly connected nodes and click **OK**.
- **b.** Click the **Provisioning > MS-SPRing** tabs.
- **c.** Choose the MS-SPRing that originally contained the removed node, and then click **Ring Map**.
- **d.** Wait until the removed node is no longer listed.
- **e.** Repeat steps a through d for the other newly connected node in the MS-SPRing.

Step 18 Complete the "DLP-F350 Delete an MS-SPRing from a Single Node" task on page 18-56.

Step 19 Click the **History** tab. Verify that the MS-SPRing_RESYNC condition appears for every node in the MS-SPRing.

Step 20 Complete the "DLP-F282 Clear an MS-SPRing Force Ring Switch" task on page 17-74 to remove the Force protection switches.

Step 21 According to local site practice, complete the "DLP-F230 Change the Node Timing Source" task on page 17-26.

Step 22 Complete the "DLP-F311 Remove Pass-through Connections" task on page 18-12.

Step 23 Log back into a node on the reduced ring. In the CTC Login dialog box, uncheck the **Disable Network Discovery** check box.

Note The deleted node will appear in network view until all RS-DCC terminations are deleted. To delete RS-DCC terminations, complete the "DLP-F321 Delete an RS-DCC Termination" task on page 18-20.

Step 24 Click the **Circuits** tab and verify that no incomplete circuits are present. If incomplete circuits appear, repeat Steps 22 and 23.

Step 25 If you delete a node that was in a login node group, you will see incomplete circuits for that node in the CTC network view. Although it is no longer part of the ring, the removed node still reports to CTC until it is no longer in a login node group. If necessary, complete the "DLP-F312 Delete a Node from a Specified Login Node Group" task on page 18-13.

Step 26 To remove another node from an MS-SPRing, repeat this procedure for the desired node.

Step 27 According to local site practice, complete the "NTP-F149 Two-Fiber MS-SPRing Acceptance Test" procedure on page 5-8.

Stop. You have completed this procedure.

NTP-F216 Add an SNCP Node

Purpose	This procedure adds a node to an existing SNCP.
Tools/Equipment	None
Prerequisite Procedures	Cards must be installed and node turn-up procedures completed on the node that will be added to the SNCP. See Chapter 2, "Install Cards and Fiber-Optic Cable," and Chapter 4, "Turn Up a Node." NTP-F152 Provision SNCP Nodes, page 5-13
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 According to local site practice, complete the "NTP-F221 Back Up the Database" procedure on page 14-4 for all the nodes in the ring.

Step 2 Log into a node in the network where you want to add an SNCP node. See the "DLP-F181 Log into CTC" task on page 16-34 for instructions. In order to have CTC visibility to the node after it is added, you must be an authorized user on the node and you must have IP connectivity to the node.

Step 3 Complete the "DLP-F273 Check the Network for Alarms and Conditions" task on page 17-64 to verify that the SNCP is free of major alarms or problems. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See the *Cisco ONS 15600 SDH Troubleshooting Guide*, as necessary.

Step 4 Count the total number of circuits on the fiber that is cut between the existing nodes. To count the number of circuits, right click on the fiber that is cut, and click circuits.

Step 5 In network view, click the **Circuits** tab.

To view Partial circuits, click the Filter button and select **PARTIAL** from the **Status** drop-down list. The Partial circuits, if any, are displayed.

To view Partial_TL1 circuits, click the Filter button and select **PARTIAL_TL1** from the **Status** drop-down list. The Partial_TL1 circuits, if any, are displayed.

Resolve any partial circuits (both Partial and Partial_TL1) in the network before proceeding. However, if you want to continue with Step 6, match the number of partial circuits and circuit names that existed before and after adding a path protection node. This ensures that no additional partial circuits are created after this procedure is completed.

Step 6 Verify the card installation on the new node. See the "NTP-F131 Verify Card Installation" procedure on page 4-2. Verify that the STM-N cards that will serve as the SNCP line cards match the SNCP optical rate. For example, if the SNCP is STM-16, the new node must have STM-16 cards installed. If the STM-N cards are not installed or the rate does not match the SNCP, complete the "NTP-F119 Install the STM-N Cards" procedure on page 2-4 to install them.

Step 7 Verify that fiber is available to connect the new node to the existing nodes.

Step 8 Complete the "NTP-F144 Verify Node Turn-Up" procedure on page 5-2.

Step 9 Create a static route on the new node if the following conditions are present. If the conditions are not present, continue with Step 10.

- The IP address for the new node is on the same subnet as other nodes in the network.
- On the new node Provisioning > Network > General subtab, Enable Socks Proxy on Port, External Network Element (ENE) is not checked under Gateway Settings.
- A CTC computer is directly connected to the new node.
- CTC computers are directly connected to other nodes on the same subnet.

If these conditions are present, add static routes on the node that will be added to the UPSR, using the following settings:

- Destination IP address: *Local-PC-IP-address*
- Net Mask: **255.255.255.255**
- Next Hop: *IP-address-of-the-Cisco-ONS-15600-SDH*
- Cost: **1**

See the "DLP-F186 Create a Static Route" task on page 16-41. To view gateway settings, see the "DLP-F185 Provision IP Settings" task on page 16-38. The gateway settings area provisions the ONS 15600 SDH SOCKS proxy server features.

Step 10 Log into the new node:

- If the node has a LAN connection and appears on the network map, from the View menu, choose **Go to Other Node**, then enter the new node.
- If the new node is not connected to the network, log into it using the "DLP-F181 Log into CTC" task on page 16-34.

Step 11 Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, SF, and SD. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See the *Cisco ONS 15600 Troubleshooting Guide*, as necessary.

Step 12 In network view, click the **Circuits** tab.

To view Partial circuits, click the Filter button and select **PARTIAL** from the **Status** drop-down list. The Partial circuits, if any, are displayed.

To view Partial_TL1 circuits, click the Filter button and select **PARTIAL_TL1** from the **Status** drop-down list. The Partial_TL1 circuits, if any, are displayed.

Resolve any partial circuits (both Partial and Partial_TL1) in the network before proceeding. However, if you want to continue with Step 13, match the number of partial circuits and circuit names that existed before and after adding a path protection node. This ensures that no additional partial circuits are created after this procedure is completed.

Step 13 (Optional) Create test circuits, making sure they pass through the SNCP line cards, and run test traffic through the node to ensure the cards are functioning properly. See the "NTP-F165 Create a Manually Routed Optical Circuit" procedure on page 6-9 and the "NTP-F167 Test Optical Circuits" procedure on page 6-16 for information.

Step 14 Create the DCC terminations on the new node. See the "DLP-F253 Provision RS-DCC Terminations" task on page 17-46.

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

Step 16 Complete the "DLP-F235 Switch All SNCP Circuits on a Span" task on page 17-29 to switch traffic away from the span that will be broken to connect to the new node.

Step 17 Two nodes will connect directly to the new node; remove their fiber connections:

a. Remove the east fiber connection from the node that will connect to the west port of the new node.

b. Remove the west fiber connection from the node that will connect to the east port of the new node.

Step 18 Replace the removed fibers with fibers that are connected to the new node.

Step 19 Log out of CTC and log back into a node in the network.

Step 20 From the View menu, choose **Go to Network View** to display the SNCP nodes. The new node should appear in the network map. Wait for a few minutes to allow all the nodes to appear.

Step 21 Click the **Circuits** tab and wait for all the circuits to appear, including spans. Count the number of incomplete circuits.

Note UNEQ-P alarms might appear on the nodes in your network; this is normal, and the alarms will clear after the circuits are updated.

Step 22 Ensure that nodes involved in the node addition operation are in the initialized state. This is because, CTC does not consider nodes that are not initialized (they appear as gray icons in the CTC network map) when evaluating the circuits.

Note Step 23 is recommended to be performed only on nodes (the newly added node, and the existing two nodes in the network between which the new node is added) involved in the node addition operation. Disable network discovery while launching CTC, add only those nodes involved in the node addition operation.

Note CTC automatically creates VT Tunnels. The cross connects should not be created manually in the intermediate nodes.

Note Step 23 does not create the overlay ring circuits. To create overlay ring circuits that route traffic around multiple rings passing through one or more nodes more than once, see the "NTP-E199 Create an Overlay Ring Circuit" procedure on page 6-32.

Step 23 In the network view, right-click the new node and choose **Update Circuits With New Node** from the shortcut menu. Wait for the confirmation dialog box to appear. Verify that the number of updated circuits in the dialog box is correct (the circuit count should be same as obtained in Step 4).

Step 24 Click the **Circuits** tab and verify that no incomplete circuits are present. However, if the partial circuits still exist in the network, verify whether they were present in Step 5 and Step 12. This will ensure that no additional partial circuits are created by this procedure.

Note If the circuits take more than a minute to appear, log out of CTC, then log back in.

Step 25 Complete the "DLP-F236 Clear a Switch for all SNCP Circuits on a Span" task on page 17-30 to clear the protection switch.

Step 26 According to local site practice, complete the "NTP-F153 SNCP Acceptance Test" procedure on page 5-15.

Stop. You have completed this procedure.

NTP-F217 Remove an SNCP Node

Purpose	This procedure removes an SNCP or multiple SNCPs from a node.
Tools/Equipment	None
Prerequisite Procedures	NTP-F152 Provision SNCP Nodes, page 5-13
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution The following procedure minimizes traffic outages during node removals.

Caution If you remove a node that is the only BITS timing source for the ring, you will remove the only source of synchronization for all the nodes in that ring. Circuits that leave the ring to connect to other networks that are synchronized to Stratum 1 timing reference will experience a high level of pointer adjustments, which might adversely affect customer service.

Step 1 Draw a diagram of the SNCP where you will remove the node. In the diagram, identify the following:

- The node that is connected through its west port to the node that will be removed
- The node that is connected through its east port to the node that will be removed

Step 2 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node in the network where you will remove the SNCP node.

Step 3 Complete the "DLP-F281 Check MS-SPRing or SNCP Alarms and Conditions" task on page 17-73 to verify that the SNCP is free of alarms. If trouble is indicated (for example, a critical or major alarm exists), resolve the problem before proceeding. See Chapter 9, "Manage Alarms" or, if necessary, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Step 4 Complete the "DLP-F293 Delete Circuits" task on page 17-83 for circuits that originate or terminate in the node you will remove. (If a circuit has multiple drops, delete only the drops that terminate on the node you are deleting.)

Step 5 Complete the "DLP-F334 Verify Pass-Through Circuits" task on page 18-34 to verify that circuits passing through the target node enter and exit the node on the same VC.

Step 6 Complete the "DLP-F235 Switch All SNCP Circuits on a Span" task on page 17-29 for all spans connected to the node you are removing.

Step 7 Remove all fiber connections between the node being removed and the two neighboring nodes.

Step 8 Reconnect the fiber of the two neighboring nodes directly, west port to east port.

Step 9 Exit CTC and log back in. Refer to "DLP-F181 Log into CTC" task on page 16-34 for instructions.

Step 10 Complete the "DLP-F281 Check MS-SPRing or SNCP Alarms and Conditions" task on page 17-73.

Step 11 Complete the "DLP-F237 Verify Timing in a Reduced Ring" task on page 17-30.

Step 12 Complete the "DLP-F236 Clear a Switch for all SNCP Circuits on a Span" task on page 17-30 to clear the protection switch.

Step 13 Complete the "NTP-F153 SNCP Acceptance Test" procedure on page 5-15.

Step 14 Complete the "DLP-F311 Remove Pass-through Connections" task on page 18-12.

Step 15 Log back into a node on the reduced ring. In the CTC Login dialog box, uncheck the **Disable Network Discovery** check box.

Note The deleted node will appear in network view until all RS-DCC terminations are deleted. To delete RS-DCC terminations, complete the "DLP-F321 Delete an RS-DCC Termination" task on page 18-20.

Step 16 Click the **Circuits** tab and verify that no incomplete circuits are present. If incomplete circuits appear, repeat Steps 14 and 15.

Step 17 If you delete a node that was in a login node group, you will see incomplete circuits for that node in the CTC network view. Although it is no longer part of the ring, the removed node still reports to CTC until it is no longer in a login node group. If necessary, complete the "DLP-F312 Delete a Node from a Specified Login Node Group" task on page 18-13.

Step 18 To remove another node from an SNCP, repeat this procedure for the desired node.

Stop. You have completed this procedure.

NTP-F218 Add a Node to a Linear ADM

Purpose	This procedure adds an ONS 15600 SDH node between two nodes in a 1+1 configuration without losing traffic.
Tools/Equipment	Compatible hardware necessary for the upgrade. Attenuators might be needed for some applications.

Prerequisite Procedures	The in-service topology upgrade procedure requires that the node to be added is reachable (has IP connectivity with CTC). Two technicians who can communicate with each other during the upgrade might be needed if the PC running CTC and the ONS 15600 SDH node are not at the same location.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note STM-N transmit and receive levels should be in their acceptable range as shown in the specifications for each card in the "NTP-F124 Install the Fiber-Optic Cables" procedure on page 2-9.

Note If overhead circuits exist on the network, an in-service topology upgrade procedure is service-affecting. The overhead circuits will drop traffic and have a status of PARTIAL after the upgrade is complete.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at either node in the 1+1 configuration. If you are already logged in, continue with Step 2.

Step 2 In network view, right-click the span between the two nodes where you want to add the new node. A dialog box appears.

Step 3 Select **Upgrade Protection**. A drop-down list appears.

Step 4 Select **Terminal to Linear** and a wizard appears.

Step 5 The wizard lists the following conditions for adding a new node:

- The terminal network has no Critical or Major alarms.
- The node that you will add has no Critical or Major alarms.
- The node has compatible software version with that of the terminal nodes.
- The node has four unused optical ports matching the speed of the 1+1 protection and no DCC has been provisioned on these four ports.
- Fiber is available to connect the added node to the terminal nodes.

If all of these conditions are met and you wish to continue with the procedure, click **Next**.

Note If you are attempting to add an unreachable node, you must first log in to the unreachable node using a separate CTC session and configure that node. Delete any existing protection groups as described in the "DLP-F229 Delete a 1+1 Protection Group" task on page 17-25. Delete any existing DCC terminations as described in the "DLP-F321 Delete an RS-DCC Termination" task on page 18-20 or the "DLP-F322 Delete an MS-DCC Termination" task on page 18-20.

Step 6 Enter the node host name or IP address, or choose the name of the new node from the drop-down list. If you type in the name, make sure it is identical to the actual node name. The node name is case sensitive.

Step 7 Click **Next**. The Select Protection Group Ports page appears.

Step 8 From the drop-down lists, select the working and protect ports on the new node that you want to connect to each terminal node.

Step 9 Click **Next**. The Re-fiber the Protected Path page appears. Follow the instructions in the dialog box for connecting the fibers between the nodes.

Step 10 When the fibers are connected properly, click **Next**. The Update Circuit(s) on *Node-Name* page appears.

Note The Back button is not enabled in the wizard. You can click the **Cancel** button at this point and choose the **Yes** button if you want to cancel the upgrade protection procedure. If the procedure fails after you have physically moved the fiber-optic cables, you must restore the fiber-optic cables to their original positions and verify (through CTC) that traffic is on the working path of the nodes before restarting the process. To check the traffic status, go to node view and click the **Maintenance > Protection** tabs. In the Protection Groups area, click the 1+1 protection group. You can see the status of the traffic in the Selected Group area.

Step 11 Click **Next** on the Update Circuit(s) on *Node-Name* page to continue with the procedure.

Step 12 The Force Traffic to Protect Path page states that it is about to force the traffic from the working to protect path for the terminal nodes. When you are ready to proceed, click **Next**.

Step 13 Follow each step as instructed by the wizard as it guides you through the process of refibering the working path between nodes and forcing the traffic back to the working path.

Step 14 The Force Traffic to Working Path page states that it is about to force the traffic from the protect to working path for the terminal nodes. When you are ready to proceed, click **Next**.

Step 15 The Completed page appears. This page is the final one in the process. Click **Finish.**

Stop. You have completed this procedure.

NTP-F219 Remove an In-Service Node from a Linear ADM

Purpose	This procedure removes a single ONS 15600 SDH from a linear ADM without disrupting traffic.
Tools/Equipment	None
Prerequisite Procedures	A linear ADM network with an ONS 15600 SDH must be present
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note The 1+1 protection group must be unidirectional in order to delete a node from a linear ADM. If your 1+1 protection group is bidirectional, refer to "DLP-F228 Modify a 1+1 Protection Group" task on page 17-25 to change it to unidirectional. After you have removed the node from the linear group, you can change the protection setting back to bidirectional.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at a node in the network where you will remove the node.

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

Step 3 Click the **Alarms** tab, then complete the following steps:

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* if necessary.

Step 4 Click the **Conditions** tab. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* if necessary.

Step 5 On the network map, double-click a node in the 1+1 protection group that is adjacent to the node you intend to remove from the group (the target node).

Step 6 In node view, click the **Maintenance > Protection** tabs.

Step 7 Initiate a Force switch on the working port:

a. In the Protection Groups area, click the 1+1 protection group.

b. In the Selected Group area, click the working port.

c. Next to Switch Commands, click **Force**.

d. In the Confirm Force Operation dialog box, click **Yes**.

e. In the Selected Group area, verify that the following appears:

- Protect port—Protect/Active [FORCE_SWITCH_TO_PROTECT] [PORT STATE]
- Working port—Working/Standby [FORCE_SWITCH_TO_PROTECT], [PORT STATE]

Step 8 Repeat Step 5 through Step 7 for the node that is connected directly to the other side of the target node.

Step 9 Remove the fiber from the working ports on the target node.

Step 10 Connect the fiber between the working ports of the two nodes that were directly connected to either side of the target node.

Step 11 On the node where you initiated a Force switch in Step 8, clear the switch:

a. Next to Switch Commands, click **Clear**.

b. In the Confirm Clear Operation dialog box, click **Yes**.

Step 12 Initiate a Force switch on the protect port:

a. In the Selected Group area, click the protect port. Next to Switch Commands, click **Force**.

b. In the Confirm Force Operation dialog box, click **Yes**.

c. In the Selected Group area, verify that the following appears:

- Protect port—Protect/Standby [FORCE_SWITCH_TO_WORKING], [PORT STATE]
- Working port—Working/Active [FORCE_SWITCH_TO_WORKING], [PORT STATE]

Step 13 From the View menu, choose **Go to Network View**.

Step 14 On the network map, double-click the other node where you initiated a Force switch.

Step 15 In node view, click the **Maintenance > Protection** tabs.

Step 16 Clear the Force switch on the working port:

a. In the Protection Groups area, click the 1+1 protection group.

b. In the Selected Group area, click the working port.

c. Next to Switch Commands, click **Clear**.

d. In the Confirm Clear Operation dialog box, click **Yes**.

Step 17 Complete Step 12 to initiate a Force switch on the protect port.

Step 18 Remove the fiber from protect ports of the target node.

Step 19 Connect the fiber between the protect ports of the two nodes on each side of the target node.

Step 20 Clear the Force switch:

a. Next to Switch Commands, click **Clear**.

b. In the Confirm Clear Operation dialog box, click **Yes**.

c. In the Selected Group area, verify the following states:

- Protect port — Protect/Standby
- Working port — Working/Active

Step 21 Repeat Step 13 through Step 16 to clear the switch on the other node.

Step 22 Exit CTC.

Step 23 Perform the "DLP-F181 Log into CTC" task on page 16-34 at any one of the nodes that were adjacent to the target node. The nodes will now show the circuit status as DISCOVERED when checked.

Stop. You have completed this procedure.

CHAPTER 14

Maintain the Node

This chapter provides procedures for maintaining the Cisco ONS 15600 SDH.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* as necessary. This section lists the chapter procedures (NTPs). Turn to a procedure to view its tasks (DLPs).

1. NTP-F220 Inspect and Maintain the Air Filter, page 14-2—Complete as needed.
2. NTP-F221 Back Up the Database, page 14-4—Complete as needed.
3. NTP-F222 Restore the Database, page 14-6—Complete as needed.
4. NTP-F223 View and Manage OSI Information, page 14-7—Complete as needed.
5. NTP-F224 Restore the Node to Factory Configuration, page 14-8—Complete as needed.
6. NTP-F225 Initiate an External Switching Command on an Optical Protection Group, page 14-9—Complete as needed.
7. NTP-F226 Initiate an External Switching Command on an SNCP Circuit, page 14-10—Complete as needed.
8. NTP-F227 Initiate an External Switching Command on an MS-SPRing, page 14-11—Complete as needed.
9. NTP-F228 View Audit Trail Records, page 14-12—Complete as needed.
10. NTP-F229 Off-Load the Audit Trail Record, page 14-14—Complete as needed.
11. NTP-F230 Off-Load the Diagnostics File, page 14-15—Complete as needed.
12. NTP-F231 Clean Fiber Connectors and Adapters, page 14-16—Complete as needed.
13. NTP-F232 Perform a Soft-Reset Using CTC, page 14-17—Complete as needed.
14. NTP-F233 Perform a Hard-Reset Using CTC, page 14-17—Complete as needed.
15. NTP-F234 Change the Node Timing Reference, page 14-18—Complete as needed.
16. NTP-F235 View the ONS 15600 SDH Timing Report, page 14-19—Complete as needed.
17. NTP-F236 Replace an SSXC Card, page 14-22—Complete as needed.
18. NTP-F237 Replace an STM-16 or STM-64 Card, page 14-23—Complete as needed.
19. NTP-F238 Replace a 4PIO or 1PIO in the ASAP Card, page 14-25—Complete as needed.

20. NTP-F239 Replace a TSC Card, page 14-27—Complete as needed.
21. NTP-F240 Replace a Fan Tray, page 14-28—Complete as needed.
22. NTP-F241 Replace the Customer Access Panel, page 14-29—Complete as needed.
23. NTP-F242 Remove a Power Distribution Unit, page 14-31—Complete as needed.
24. NTP-F243 Replace the Power Distribution Unit, page 14-33—Complete as needed.
25. NTP-F244 Edit Network Element Defaults, page 14-34—Complete as needed to edit the factory-configured (default) network element settings for the Cisco ONS 15600 SDH.
26. NTP-F245 Import Network Element Defaults, page 14-35—Complete as needed to import the factory-configured (default) network element settings for the Cisco ONS 15600 SDH.
27. NTP-F246 Export Network Element Defaults, page 14-36—Complete as needed to export the factory-configured (default) network element settings for the Cisco ONS 15600 SDH.

Note The battery return connection is treated as DC-I, as defined in Telcordia GR-1089-CORE issue 4.

NTP-F220 Inspect and Maintain the Air Filter

Purpose	This procedure explains how to inspect and maintain reusable fan tray air filters.
Tools/Equipment	Extra filters, pinned hex key
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution Cisco recommends that you inspect the air filter monthly, and clean the filter every three to six months. Replace the air filter every two to three years. Avoid cleaning the air filter with harsh cleaning agents or solvents.

Step 1 Remove the front door of the shelf assembly by completing the following substeps. If the front door is already removed, continue with Step 2.

a. Locate the latches on the bottom left and right sides of the door.

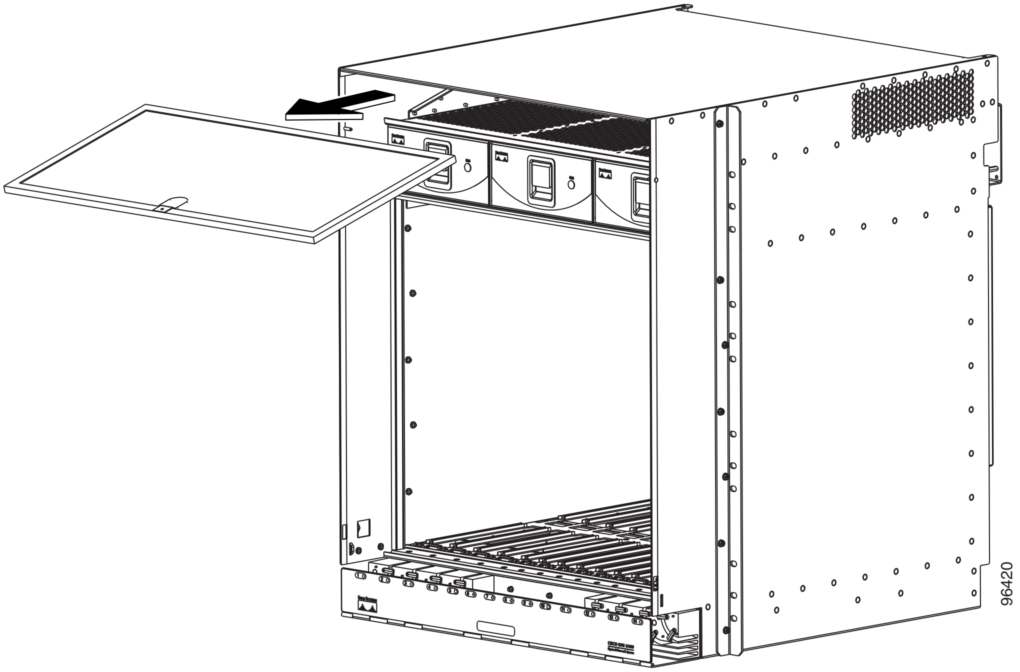
b. Pull each latch outward to release the latch.

c. Swing the door up to open it.

d. Lift the door off its hinge pins and remove it. Set the door aside so you can reinstall it after you complete this procedure.

Step 2 Gently remove the air filter from the shelf assembly (Figure 14-1). Be careful not to dislodge any dust that may have collected on the filter.

Figure 14-1 Removing a Reusable Air Filter (Front Door Removed)



Step 3 Visually inspect the white filter material for dirt and dust.

Step 4 If the reusable air filter contains a concentration of dirt and dust, replace the dirty air filter with a clean air filter (spare filters should be kept in stock) and reinsert the fan-tray assembly. Then, vacuum the dirty air filter or wash it under a faucet with a light detergent.

Caution Do not leave the fan tray out of the chassis for an extended period of time because excessive heat can damage the ONS 15600 SDH cards.

Note Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

Step 5 If you washed the filter, allow it to completely air dry for at least eight hours.

Caution Do not put a damp filter back in the ONS 15600 SDH.

Step 6 Reinstall the front door of the shelf assembly:

a. Insert the front door (removed in Step 1) into the hinge pins on the shelf assembly.

b. Lower the door onto the face of the shelf assembly.

c. Pull the metal latches on the door outward and gently push the door toward the shelf, making sure no optical cables are caught or pinched in the door.

d. Click the latches in place and release.

Stop. You have completed this procedure.

NTP-F221 Back Up the Database

Purpose	This procedure stores a backup version of the CTC software database on a workstation running CTC or on a network server. Cisco recommends performing a database backup at approximately weekly intervals and prior to and after configuration changes.
Tools/Equipment	None
Prerequisite Procedures	NTP-F118 Install the Common Control Cards, page 2-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note You must back up and restore the database for each node on a circuit path in order to maintain a complete circuit.

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

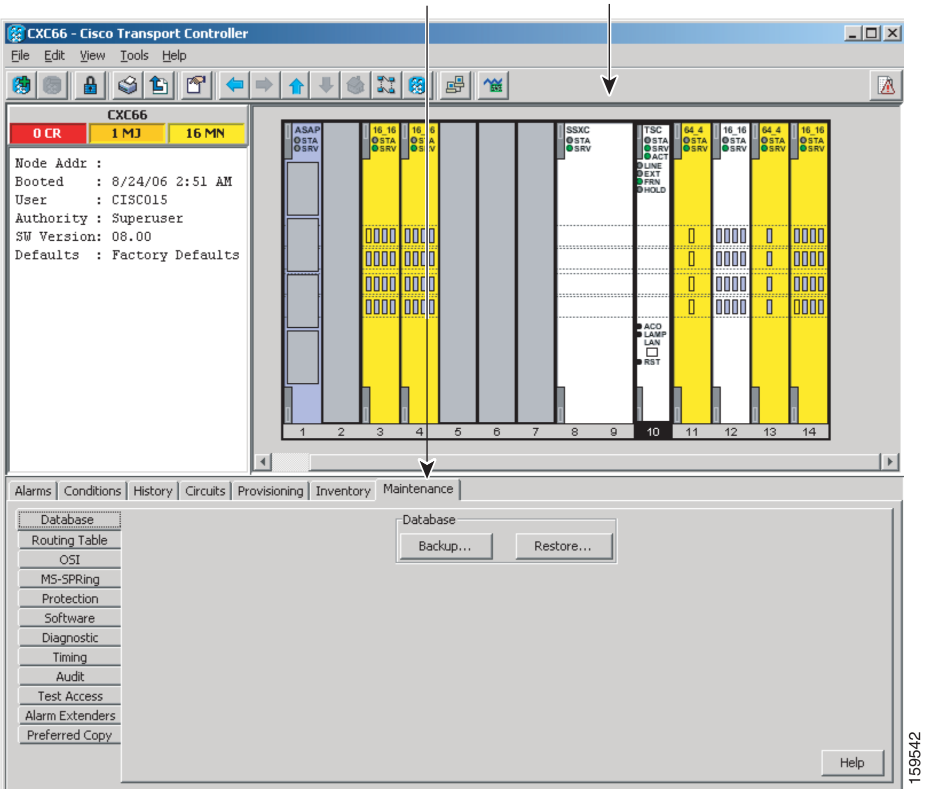
Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node you want to back up. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Maintenance > Database** tabs. (Figure 14-2).

Figure 14-2 Backing Up the TSC Database

Maintenance tab

Node view



```
Node Addr :
Booted     : 8/24/06 2:51 AM
User       : CISCO15
Authority : Superuser
SW Version: 08.00
Defaults   : Factory Defaults
```

Step 3 Click **Backup**.

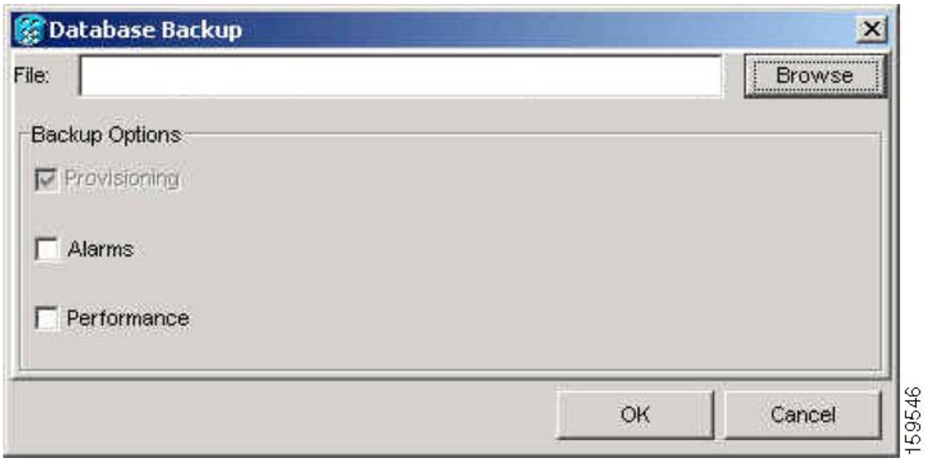
Step 4 In the Database Backup window, click **Browse**. Repeat for the next Database Backup window.

Step 5 In the Save window, navigate to a local PC directory or network directory and enter a database name (such as database.db) in the File name field.

Step 6 Click **Save**.

Step 7 In the Database Backup window, click the **Alarms** check box and/or **Performance** check box if you want to backup these database items in addition to provisioning information (Figure 14-3).

Figure 14-3 Database Filename Entered and Backup Options Checked



Note Provisioning is a default component of the backup file.

Step 8 Click **OK**.

Step 9 If you are overwriting an existing file, click **OK** in the confirmation dialog box.

Step 10 Click **OK** in the Database Backup window.

Stop. You have completed this procedure.

NTP-F222 Restore the Database

Purpose	This procedure restores the TSC software database.
Tools/Equipment	None
Prerequisite Procedures	NTP-F221 Back Up the Database, page 14-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution Restoring an out-of-date database or a database from a different node might affect the service. Any provisioning data that currently exists on the node, but not present in the database file being restored, will be deleted.

Note The following parameters are not backed up and restored: Node name, subnet mask and gateway, and IIOP port. If you change the node name and then restore a backed up database with a different node name, the circuits will map to the new renamed node. Cisco recommends keeping a record of the old and new node names.

Note You need separate backups for each node in a circuit path to be able to restore the entire circuit.

Note If you want to revert to a previously loaded software version, refer to the platform-specific upgrade document for instructions.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you are performing the database restore. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Maintenance > Database** tabs.

Step 3 Click **Restore**.

Step 4 In the Database Restore window, click the **Alarms** check box and/or **Performance** check box to choose these database items in addition to provisioning information.

Note You can back up five databases as part of one back up file package; therefore the 15600 SDH allows you to select all of the files or a subset of the files to restore as part of the restore package.

Step 5 In the Database Restore window, click **Browse**.

Step 6 Navigate to the backup file stored on the workstation hard drive or on network storage.

Step 7 Click the database file to highlight it.

Step 8 Click **Open**. The Database Restore dialog box appears.

Step 9 Click **Restore**.

The Database Restore window monitors the file transfer. Wait for the file to complete the transfer to the TSC.

Step 10 Click **OK** in the Lost connection to node, changing to Network View dialog box. Wait for the node to reconnect.

Stop. You have completed this procedure.

NTP-F223 View and Manage OSI Information

Purpose	This procedure allows you to view and manage OSI including the ES-IS and IS-IS routing information bases, TARP data cache, and manual area table.
Tools/Equipment	None
Prerequisite Procedures	NTP-F221 Back Up the Database, page 14-4 NTP-F143 Provision OSI, page 4-14
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15600 SDH Reference Manual* for additional information about OSI.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34. If you are already logged in, continue with Step 2.

Step 2 Perform any of the following tasks as needed:

- DLP-F376 View IS-IS Routing Information Base, page 18-86
- DLP-F377 View ES-IS Routing Information Base, page 18-87
- DLP-F378 Manage the TARP Data Cache, page 18-87

Stop. You have completed this procedure.

NTP-F224 Restore the Node to Factory Configuration

Purpose	This procedure reinitializes the ONS 15600 SDH using the CTC reinitialization tool. Reinitialization uploads a new software package to the control card, clears the node database, and restores the factory default parameters.
Tools/Equipment	Cisco ONS 15600 SDH System Software CD, Version 8.0.x JRE 5.0 must be installed on the computer to log into a Software R8.0node when reinitialization is complete. The reinitialization tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 5.0.
Prerequisite Procedures	NTP-F221 Back Up the Database, page 14-4 NTP-F126 Set Up Computer for CTC, page 3-1 One of the following: • NTP-F127 Set Up CTC Computer for Local Craft Connection to the ONS 15600 SDH, page 3-3 or • NTP-F128 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15600 SDH, page 3-4
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser only

Caution Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinit tool chooses the first product-specific database in the specified directory if you use the Search Path field instead of the Package and Database fields. You may accidentally copy an incorrect database if multiple databases are kept in the specified directory.

Caution Restoring a node to the factory configuration deletes all cross-connects on the node.

Caution Cisco recommends that you take care to save the node database to safe location if you are not restoring the node using the database provided on the software CD.

Note The following parameters are not backed up and restored when you delete the database and restore the factory settings: node name, IP address, subnet mask and gateway, and IIOP port. If you change the node name and then restore a backed up database with a different node name, the circuits map to the new renamed node. Cisco recommends keeping a record of the old and new node names.

Step 1 If you are using Microsoft Windows, complete the "DLP-F278 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)" task on page 17-69.

Step 2 If you are using UNIX, complete the "DLP-F323 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)" task on page 18-21.

Stop. You have completed this procedure.

NTP-F225 Initiate an External Switching Command on an Optical Protection Group

Purpose	This procedure describes how apply an external switching command (Force, Manual, lock on or lockout) to an optical protection group.
Tools/Equipment	None
Prerequisite Procedures	NTP-F138 Create a 1+1 Protection Group, page 4-10
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If you choose a Manual switch, the command will switch traffic only if the path has an error rate less than the signal degrade bit error rate threshold. A Force switch will switch traffic even if the path has SD or SF conditions. A Force switch has a higher priority than a Manual switch. Lockouts can only be applied to protect cards; they prevent traffic from switching to the protect port under any circumstance. Lock outs have the highest priority. A lock on can be applied to the working port; it prevents traffic from switching to the protect port in the protection group.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to inhibit 1+1 group protection switching. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-F238 Initiate a Manual Switch on a Port in a 1+1 Protection Group" task on page 17-31 as needed.

Step 3 Complete the "DLP-F239 Initiate a Force Switch on a Port in a 1+1 Protection Group" task on page 17-32 as needed.

Step 4 Complete the "DLP-F295 Clear a Manual or Force Switch in a 1+1 Protection Group" task on page 17-86 as needed.

Step 5 To prevent traffic on a working port from switching to the protect port, complete the "DLP-F240 Apply a Lock On in a 1+1 Group" task on page 17-33.

Step 6 To prevent working traffic from switching to the protect port, complete the "DLP-F241 Apply a Lockout in a 1+1 Group" task on page 17-34 to lockout the protect port.

Step 7 Complete the "DLP-F296 Clear a Lock On or Lockout in a 1+1 Protection Group" task on page 17-86 as needed.

Note Refer to the "Card Protection" chapter in the *Cisco ONS 15600 SDH Reference Manual* for a description of protection switching and switch state priorities.

Stop. You have completed this procedure.

NTP-F226 Initiate an External Switching Command on an SNCP Circuit

Purpose	This procedure initiates a Manual, Force, or lockout switch on a subnetwork connection protection ring (SNCP) circuit.
Tools/Equipment	None
Prerequisite Procedures	NTP-F152 Provision SNCP Nodes, page 5-13
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note 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. Lockouts prevent traffic from switching under any circumstance and have the highest priority.

Note This procedure switches traffic on a single SNCP circuit; to switch all circuits on a span, see the "DLP-F235 Switch All SNCP Circuits on a Span" task on page 17-29.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to switch traffic on a SNCP circuit. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-F242 Initiate a Manual Switch on an SNCP Circuit" task on page 17-35 as needed.

Step 3 Complete the "DLP-F243 Initiate a Force Switch to an SNCP Circuit" task on page 17-35 as needed.

Step 4 Complete the "DLP-F297 Initiate a Lockout on an SNCP Path" task on page 17-87 to prevent traffic from switching to the protect path.

Step 5 Complete the "DLP-F298 Clear a Switch or Lockout on an SNCP Circuit" task on page 17-88 as needed.

Note Refer to the *Cisco ONS 15600 SDH Reference Manual* for a description of protection switching and switch state priorities.

Stop. You have completed this procedure.

NTP-F227 Initiate an External Switching Command on an MS-SPRing

Purpose	This procedure initiates and clears multiplex section-shared protection ring (MS-SPRing) manual ring switches and MS-SPRing force ring switches. 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 SD or SF conditions. A Force switch has a higher priority than a Manual switch.
Tools/Equipment	None
Prerequisite Procedures	NTP-F147 Provision MS-SPRing Nodes, page 5-6
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to switch traffic on a SNCP circuit. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-F344 Initiate an MS-SPRing Manual Ring Switch" task on page 18-47 as needed.

Step 3 Complete the "DLP-F345 Clear an MS-SPRing Manual Ring Switch" task on page 18-48 as needed.

Step 4 Complete the "DLP-F347 Initiate an MS-SPRing Force Ring Switch" task on page 18-50 as needed.

Step 5 Complete the "DLP-F282 Clear an MS-SPRing Force Ring Switch" task on page 17-74 as needed.

Stop. You have completed this procedure.

NTP-F228 View Audit Trail Records

Purpose	This procedure explains how to view audit trail records. Audit trail records are useful for maintaining security, recovering lost transactions, and enforcing accountability. Accountability refers to tracing user activities; that is, associating a process or action with a specific user.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

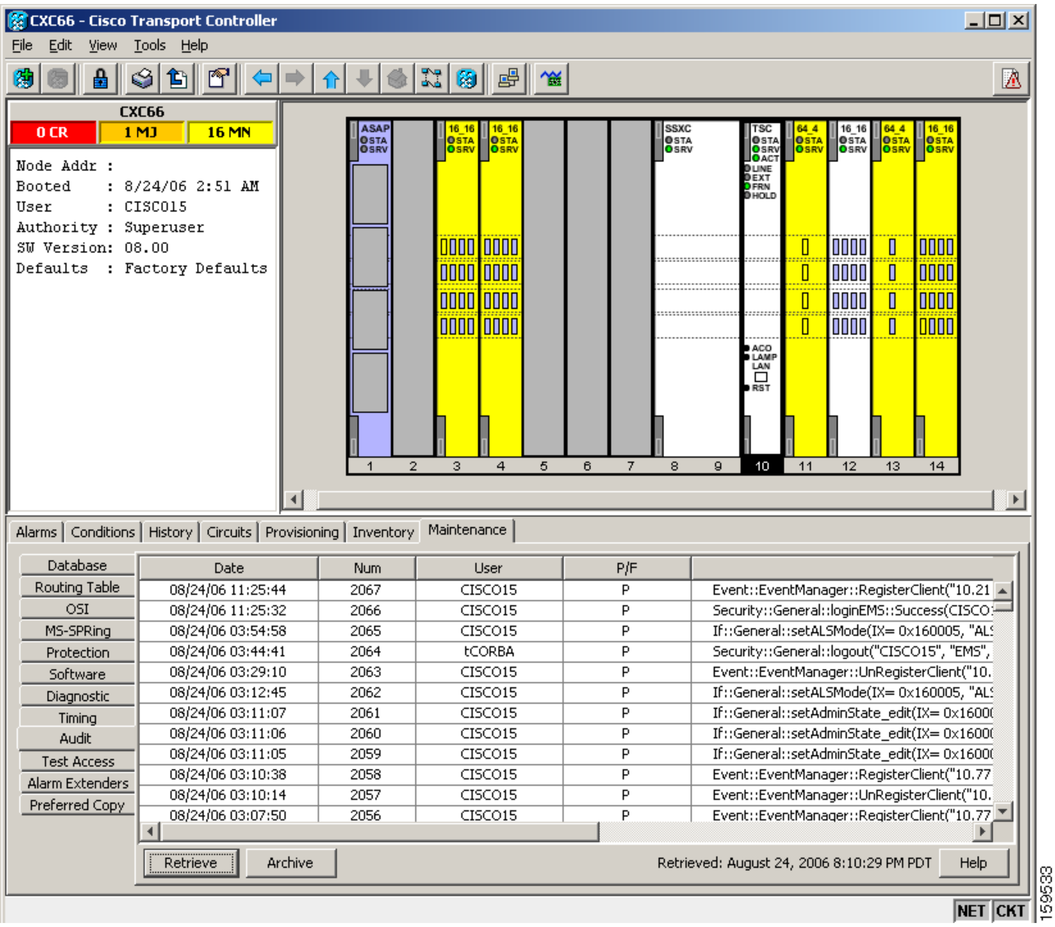
Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to view the audit trail log. If you are already logged in, continue with Step 2.

Step 2 In the node view, click the **Maintenance > Audit** tabs.

Step 3 Click **Retrieve**.

A window containing the most recent Audit Trail records appears as shown in Figure 14-4.

Figure 14-4 Viewing the Audit Trail Records



```
Node Addr :
Booted    : 8/24/06 2:51 AM
User      : CISCO15
Authority : Superuser
SW Version: 08.00
Defaults  : Factory Defaults
```

Date	Num	User	P/F	
08/24/06 11:25:44	2067	CISCO15	P	Event::EventManager::RegisterClient("10.21
08/24/06 11:25:32	2066	CISCO15	P	Security::General::loginEMS::Success(CISCO
08/24/06 03:54:58	2065	CISCO15	P	If::General::setALSMode(IX= 0x160005, "AL
08/24/06 03:44:41	2064	tCORBA	P	Security::General::logout("CISCO15", "EMS",
08/24/06 03:29:10	2063	CISCO15	P	Event::EventManager::UnRegisterClient("10.
08/24/06 03:12:45	2062	CISCO15	P	If::General::setALSMode(IX= 0x160005, "AL
08/24/06 03:11:07	2061	CISCO15	P	If::General::setAdminState_edit(IX= 0x1600
08/24/06 03:11:06	2060	CISCO15	P	If::General::setAdminState_edit(IX= 0x1600
08/24/06 03:11:05	2059	CISCO15	P	If::General::setAdminState_edit(IX= 0x1600
08/24/06 03:10:38	2058	CISCO15	P	Event::EventManager::RegisterClient("10.77
08/24/06 03:10:14	2057	CISCO15	P	Event::EventManager::UnRegisterClient("10.
08/24/06 03:07:50	2056	CISCO15	P	Event::EventManager::RegisterClient("10.77

Retrieved: August 24, 2006 8:10:29 PM PDT

A definition of each column in the Audit Trail log is listed in Table 14-1.

Table 14-1 Audit Trail Column Definitions

Column	Definition
Date	Date when the action occurred in the format MM/dd/yy HH:mm:ss
Num	Incrementing count of actions
User	User ID that initiated the action
P/F	Pass/Fail (that is, whether or not the action was executed)
Operation	Action that was taken

Right-click on the column headings to display the list in ascending-to-descending or descending-to-ascending order.

Left-click on the column heading to display the following options:

- Reset Sorting—Resets the column to the default setting
- Hide Column—Hides the column from view
- Reset Columns Order/Visibility—Displays all hidden columns

- Row Count—Provides a numerical count of log entries

Shift-click on the column heading for an incremental sort of the list.

Stop. You have completed this procedure.

NTP-F229 Off-Load the Audit Trail Record

Purpose	This procedure describes how to off-load up to 640 audit trail log entries to a local or network drive file to maintain a record of actions performed for the node. If the audit trail log is not off-loaded, the oldest entries are overwritten after the log reaches capacity.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to off-load the audit trail log. If you are already logged in, continue with Step 2.

Step 2 In the node view, click the **Maintenance > Audit** tabs.

Step 3 Click **Retrieve**.

Step 4 Click **Archive**.

Step 5 In the Archive Audit Trail dialog box, navigate to the directory (local or network) where you want to save the file.

Step 6 Enter a name in the File Name field.

You do not have to give the archive file a particular extension. It is readable in any application that supports text files, such as WordPad, Microsoft Word (imported), etc.

Step 7 Click **Save**.

640 entries are saved in this file. The next entries continue with the next number in the sequence, rather than starting over.

Note Archiving does not delete entries from the CTC audit trail log. However, entries can be self-deleted by the system after the log maximum is reached. If you archived the entries, you cannot reimport the log file back into CTC and will have to view the log in a different application.

Stop. You have completed this procedure.

NTP-F230 Off-Load the Diagnostics File

Purpose	This procedure describe how to off-load a diagnostic file. The diagnostic file contains a set of debug commands run on a node and its results. This file is useful to TAC when troubleshooting problems with the node.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to off-load the audit trail log. If you are already logged in, continue with Step 2.

Step 2 In the node view, click the **Maintenance > Diagnostic** tabs.

Step 3 Click **Retrieve Tech Support Log**.

Step 4 In the Saving Diagnostic File dialog box, navigate to the directory (local or network) where you want to save the file.

Step 5 Enter a name in the File Name field.

You do not have to give the archive file a particular extension. It is a compressed file (gzip) that can be unzipped and read by Cisco Technical Support.

Step 6 Click **Save**.

The Get Diagnostics status window shows a progress bar indicating the percentage of the file being saved, then shows "Get Diagnostics Complete."

Step 7 Click **OK**.

Stop. You have completed this procedure.

NTP-F231 Clean Fiber Connectors and Adapters

Purpose	This procedure cleans the fiber connectors and adapters.
Tools/Equipment	Inspection microscope (suggested: Westover FBP-CIS-1) Scrub tool Grounding strap Wipes Rinse tool HFE-based cleaning fluid and pump head assembly Replacement scrub tool wipes Replacement rinse tool absorbent pads Desktop hand tool Pen-type hand tool 3M high-performance fiber-optic wipes Empty disposable container Canned air
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 1051

Caution Follow established site safety practices when working with any laser equipment.

Step 1 Using an inspection microscope, inspect each fiber connector for dirt, cracks, or scratches.

Step 2 Replace any damaged fiber connectors.

Note Replace all dust caps whenever the equipment is unused for 30 minutes or more.

Step 3 Complete the "DLP-F245 Clean Fiber Connectors" task on page 17-37 as necessary.

Step 4 Complete the "DLP-F246 Clean the Fiber Adapters" task on page 17-39 as necessary.

Caution Do not reuse the optical swabs. Keep unused swabs off of work surfaces.

Stop. You have completed this procedure.

NTP-F232 Perform a Soft-Reset Using CTC

Purpose	This procedure resets an active card and switches the node to the redundant card using a soft reset.
Tools/Equipment	None
Prerequisite Procedures	NTP-F118 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Note Before you reset the card, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to perform the card reset. If you are already logged in, continue with Step 2.

Step 2 In node view, right-click the appropriate card to reveal a drop-down list.

Step 3 Click **Soft-Reset Card**.

Step 4 Click **Yes** in the "Are you sure you want to soft-rest this card?" dialog box.

Step 5 Click **OK** in the "Lost connection to node, changing to Network View" dialog box.

Note For LED behavior during a TSC/SSXC reboot, see Table 2-1 on page 2-3.

Stop. You have completed this procedure.

NTP-F233 Perform a Hard-Reset Using CTC

Purpose	This procedure resets the active card (TSC, SSXC, optical, ASAP) and switches the node to the redundant card using a hard reset.
Tools/Equipment	None
Prerequisite Procedures	NTP-F118 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Note The hard-reset option is enabled only when the card is placed in the locked-enabled, maintenance service state.

Note Before you reset the TSC, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to perform the TSC card reset. If you are already logged in, continue with Step 2.

Step 2 In node view click the **Inventory** tab. Locate the appropriate card in the inventory list.

Step 3 Click the **Admin State** drop-down list and select **locked, maintenance**. Click **Apply**.

Step 4 Click **Yes** in the "Action may be service affecting. Is it OK to apply the changes?" dialog box.

Step 5 The service state of the card becomes locked-enabled, maintenance. The card's faceplate appears blue in CTC and the SRV LED turns amber.

Step 6 Right-click the card to reveal a pop-up menu.

Step 7 Click **Hard-reset Card**.

Step 8 Click **Yes** in the "Are you sure you want to hard-reset this card?" dialog box.

Step 9 If you hard-reset the active TSC, click **OK** in the "Lost connection to node, changing to Network View" dialog box.

Note For LED behavior during a TSC reboot, see Table 2-1 on page 2-3.

Stop. You have completed this procedure.

NTP-F234 Change the Node Timing Reference

Purpose	This procedure switches the node timing reference to enable maintenance on a timing reference or returning the node timing to normal operation.
Tools/Equipment	None
Prerequisite Procedures	NTP-F137 Set Up Timing, page 4-9
Required/As Needed	As needed
Onsite/Remote	Onsite or Remote
Security Level	Maintenance or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to change the node timing reference. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-F259 Manual Switch the Node Timing Reference" task on page 17-52 as needed.

Step 3 Complete the "DLP-F260 Clear a Manual Switch on a Node Timing Reference" task on page 17-53 as needed.

Stop. You have completed this procedure.

NTP-F235 View the ONS 15600 SDH Timing Report

Purpose	This procedure displays the current status of the ONS 15600 SDH timing references.
Tools/Equipment	None
Prerequisite Procedures	NTP-F137 Set Up Timing, page 4-9
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to view the node timing status. If you are already logged in, continue with Step 2.

Step 2 Click the **Maintenance > Timing > Report** tabs.

Step 3 In the Timing Report area, you can view node timing information. The date and time of the report appear at the top of the report. Table 14-2 describes the report fields and entries.

Step 4 To update the report, click **Refresh**.

Table 14-2 ONS 15600 SDH Timing Report

Item	Description	Option	Option Description
Clock	Indicates the timing clock. The report section that follows applies to the timing clock indicated.	NE	The node timing clock.
		BITS-1 Out	The BITS-1 Out timing clock.
		BITS-2 Out	The BITS-2 Out timing clock.

Table 14-2 ONS 15600 SDH Timing Report (continued)

Item	Description	Option	Option Description
Status Status (cont.)	Indicates the status of the timing clock.	INIT_STATE	The timing reference has not been provisioned. For an NE reference, this status appears just before the first provisioning messages when the TSC is booting. Timing is provisioned to the internal clock of the node.
		HOLDOVER_STATE	The clock was locked onto a valid timing reference for more than 140 seconds when a failure occurred. Holdover state timing is a computation based on timing during normal state combined with the node's internal clock. The node holds onto this frequency until the valid reference is restored. This status appears for NE references only.
		FREERUN_STATE	The node is running off its internal clock without any modification except the calibrated value to bring timing to 0 PPM. Free-run state can occur when a Force switch to the internal clock is initiated, all references fail without the 140 seconds of holdover data, or only Internal timing references are defined. This status appears for NE references only.
		NO_SYNC_STATE	A synchronization timing reference is not defined. BITS-1 Out or BITS-2 Out default to this status until an STM-N card is defined as its reference on the Provisioning > Timing tab. This status appears for external references only.
		NE_SYNCH_STATE	BITS-1 Out and BITS-2 Out use the same timing source as the NE. This is displayed when NE Reference is selected for BITS-1 Out and BITS-2 Out Reference List on the Provisioning > Timing tab.
		NORMAL_STATE	The timing reference is locked onto one of its provisioned references. The reference cannot be Internal or no sync state.
		FAST_START_STATE	The node has switched references, but the reference is too far away to reach normal state within an acceptable amount of time. Fast Start is a fast acquisition mode to allow the node to quickly acquire the reference. After it achieves this goal, the node progresses to the normal state.
		FAST_START_FAILED_STATE	A timing reference is too far away to reach in normal state. The fast start state could not acquire sufficient timing information within the allowable amount of time.
Status Changed At	Date and time of the last status change.	—	—
Switch Type	Type of switch.	AUTOMATIC	The timing switch was system-generated.
		Manual	The timing switch was a user-initiated Manual switch.
		Force	The timing switch was user-initiated Force switch.

Table 14-2 ONS 15600 SDH Timing Report (continued)

Item	Description	Option	Option Description
Reference	Indicates the timing reference.	Three timing references (Ref-1, Ref-2, and Ref-3) are available on the Provisioning > Timing tab.	These options indicate the timing references that the system uses, and the order in which they are called. (For example, if Ref-1 becomes available, Ref-2 is called.)
Selected	Indicates whether the reference is selected.	Selected references are indicated with an X.	—
Facility	Indicates the timing facility provisioned for the reference on the Provisioning > Timing tab.	BITS-1	The timing facility is a building integrated timing supply (BITS) clock attached to the node's BITS-1 pins.
		BITS-2	The timing facility is a BITS clock attached to the node's BITS-2 pins.
		STM-N card with port #	If the node is set to line timing, this is the STM-N card and port provisioned as the timing reference.
		Internal clock	The node is using its internal clock.
State	Indicates the timing reference state.	unlocked	The timing reference is operational.
		locked	The timing reference is not operational.
Condition	Indicates the timing reference state.	OKAY	The reference is valid to use as a timing reference.
		OOB	Out of bounds; the reference is not valid and cannot be used as a timing reference, for example, a BITS clock is disconnected.
Condition Changed	Indicates the date and time of the last status change in MM/DD/YY HH:MM:SS format.	—	—
SSM	Indicates whether SSM is enabled for the timing reference.	Enabled	SSM is enabled.
		Disabled	SSM is not enabled.
SSM Quality	Indicates the SSM timing quality.	8 to 10 SSM quality messages might be displayed.	For a list of SSM message sets, refer to the *Cisco ONS 15600 SDH Reference Manual*.
SSM Changed	Indicates the date and time of the last SSM status change in MM/DD/YY HH:MM:SS format.	—	—

Stop. You have completed this procedure.

NTP-F236 Replace an SSXC Card

Purpose	This procedure replaces a faulty SSXC card with a new SSXC card.
Tools/Equipment	Replacement SSXC card
Prerequisite Procedures	NTP-F221 Back Up the Database, page 14-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Note The ONS 15600 SDH system dynamically changes the preferred copy status from one SSXC to the redundant copy if an error is detected on a card port. You can see this change in the CTC node view Maintenance > Preferred Copy window Currently Used field. If errors are detected on both SSXC copies, the Currently Used field says Both.

Note You do not need to make any changes to the database if you are replacing it with a card of exactly the same type.

Note Card removal raises an improper removal (IMPROPRMVL) alarm, but this clears after the card replacement is complete.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 for the node where you will replace the SSXC card.

Step 2 In node view click the **Inventory** tab. Locate the appropriate SSXC card in the inventory list.

Step 3 Click the **Admin State** drop-down list and select **locked, maintenance**. Click **Apply**.

Step 4 Click the **Maintenance > Preferred Copy** tabs. Verify that the SSXC selected as the preferred data copy is not the SSXC you want to remove.

Step 5 Physically remove the SSXC card to be replaced from the ONS 15600 SDH shelf:

a. Open the card ejectors.

b. Slide the card out of the slot.

Note An UNPROT-XCMTX alarm will be reported when you remove the SSXC card.

Step 6 Install the replacement SSXC card in the shelf:

a. Open the ejectors on the replacement card.

b. Slide the replacement card into the slot along the guide rails until it contacts the backplane.

c. Close the ejectors.

Step 7 Wait for the new card to boot. (This will take approximately one minute.) Ensure that the UNPROT-XCMTX alarm clears.

Step 8 In node view click the **Inventory** tab. Locate the newly installed SSXC card in the inventory list.

Step 9 Click the **Admin State** drop-down list and select **unlocked**. Click **Apply**.

Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

.

NTP-F237 Replace an STM-16 or STM-64 Card

Purpose	This procedure replaces an STM-16 or STM-64 traffic card with a new card of the same type.
Tools/Equipment	Replacement STM-16 or STM-64 card
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Note Card removal raises an improper removal (IMPROPRMVL) alarm, but this clears after the card replacement is completed.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you will replace the STM-16 or STM-64 card.

Step 2 Ensure that the card you are replacing does not carry traffic in a 1+1 protection group:

a. In node view, click the **Maintenance > Protection** tabs.

b. Choose the first group listed under Protection Groups.

c. Verify that the slot number for the card you are replacing does not appear in the Selected Groups list. For example, if you are replacing the STM-16 card in Slot 3, make sure that Selected Groups does not contain any entries that start with s3, regardless of the port.

d. Repeat Steps b and c for each protection group.

e. If any of the groups contain a port on the card you want to replace, complete the "DLP-F239 Initiate a Force Switch on a Port in a 1+1 Protection Group" task on page 17-32.

Step 3 Ensure that the card you are replacing does not carry SNCP circuit traffic:

Note A port can be part of a 1+1 protection group or part of a SNCP, but it cannot be configured for both. However, different ports on one card can be configured in different ways. If you move all of the traffic off some 1+1 ports, you still need to check whether the remaining ports are carrying SNCP traffic.

a. From the **View menu choose Go to Parent View**.

b. Click the **Circuits** tab.

c. View the circuit source and destination ports and slots. If any circuits originate or terminate in the slot containing the card you are replacing, perform the "DLP-F235 Switch All SNCP Circuits on a Span" task on page 17-29 or the DLP-F347 Initiate an MS-SPRing Force Ring Switch, page 18-50.

Note If the card you are replacing is not configured for any port or circuit protection, but does carry traffic, bridge and roll this traffic onto another card. See the "NTP-F181 Bridge and Roll Traffic" procedure on page 7-5.

Step 4 Remove any fiber optic cables from the ports.

Step 5 Physically remove the card that you want to replace from the ONS 15600 SDH shelf:

a. Open the card ejectors.

b. Slide the card out of the slot.

Step 6 Physically replace the STM-16 or STM-64 card in the shelf:

a. Open the ejectors on the replacement card.

b. Slide the replacement card into the slot along the guide rails until it contacts the backplane.

c. Close the ejectors.

Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 7 Clear the Force switches:

- To clear 1+1 Force switches, complete the "DLP-F295 Clear a Manual or Force Switch in a 1+1 Protection Group" task on page 17-86.
- To clear SNCP Force switches, complete the "DLP-F236 Clear a Switch for all SNCP Circuits on a Span" task on page 17-30.
- To clear MS-SPRing Force switches, complete the "DLP-F282 Clear an MS-SPRing Force Ring Switch" task on page 17-74.

Step 8 When the card is in service and receiving traffic, reset the card's physical receive power level threshold in CTC:

a. Double-click the newly installed card in CTC node view.

b. Click the **Provisioning > SDH Thresholds** tabs.

c. Click the **Physical** radio button.

d. Click **Set OPR** for each port on the card.

Step 9 As necessary, refer to the "NTP-F197 Modify Line and Status Thresholds for Optical Ports" procedure on page 10-2 to change the optical card settings.

Stop. You have completed this procedure.

NTP-F238 Replace a 4PIO or 1PIO in the ASAP Card

Purpose	This procedure replaces a 4PIO or 1PIO module (PIM) in the ASAP card with another module of the same type.
Tools/Equipment	Replacement 4PIO(s) and/or 1PIO(s)
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Caution Replacing a provisioned 4PIO with a 1PIO (and vice versa) is not supported. You must replace the PIM with the same PIM type, unless you have deleted the previously installed module before you install the new module type.

Note Card removal raises an improper removal (IMPROPRMVL) alarm, but this clears after the card replacement is completed.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you will replace the 1PIO or 4PIO module.

Step 2 Ensure that the module you are replacing does not carry traffic in a 1+1 protection group:

a. In node view, click the **Maintenance > Protection** tabs.

b. Choose the first group listed under Protection Groups.

c. Verify that none of the port numbers for the 4PIO or 1PIO you are replacing does not appear in the Selected Groups list.

d. Repeat Steps b and c for each protection group.

e. If any of the groups contain a port on the card you want to replace, complete the "DLP-F239 Initiate a Force Switch on a Port in a 1+1 Protection Group" task on page 17-32.

Step 3 Ensure that the card you are replacing does not carry SNCP circuit traffic:

Note A port can be part of a 1+1 protection group or part of a SNCP, but it cannot be configured for both. However, different ports on one card can be configured in different ways. If you move all of the traffic off some 1+1 ports, you still need to check whether the remaining ports are carrying SNCP traffic.

a. From the **View menu choose Go to Parent View**.

b. Click the **Circuits** tab.

c. View the circuit source and destination ports and slots. If any circuits originate or terminate in the slot containing the card you are replacing, perform the "DLP-F235 Switch All SNCP Circuits on a Span" task on page 17-29 or the "DLP-F347 Initiate an MS-SPRing Force Ring Switch" task on page 18-50.

Note If the card you are replacing is not configured for any port or circuit protection, but does carry traffic, bridge and roll this traffic onto another card. See the "NTP-F181 Bridge and Roll Traffic" procedure on page 7-5.

Step 4 Remove any fiber-optic cables from the ports.

Step 5 Physically remove the 4PIO or 1PIO that you want to replace from the ASAP card:

a. Loosen the screws at the top right and bottom left on the 1PIO or 4PIO module. (You can do this using a Phillips screwdriver or by hand.)

b. Slide the module out of the slot on the ASAP card.

Step 6 Physically replace the 4PIO or 1PIO module in the ASAP card:

a. Carefully slide the module along the top and bottom guide rails into the correct slot.

b. Use a Phillips screwdriver or your hand to tighten the screws at the top right and bottom left of the module.

Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 7 Clear the Force switches:

- To clear 1+1 Force switches, complete the "DLP-F295 Clear a Manual or Force Switch in a 1+1 Protection Group" task on page 17-86.
- To clear SNCP Force switches, complete the "DLP-F236 Clear a Switch for all SNCP Circuits on a Span" task on page 17-30.
- To clear MS-SPRing Force switches, complete the "DLP-F282 Clear an MS-SPRing Force Ring Switch" task on page 17-74.

Step 8 When the module is in service and receiving traffic, reset the module's physical receive power level threshold in CTC:

a. Double-click the newly installed module in CTC node view.

b. Click the **Provisioning > Optical > Optics Thresholds** tabs.

c. Click the **Physical** radio button.

d. Click **Set OPR** for each port on the card.

Stop. You have completed this procedure.

NTP-F239 Replace a TSC Card

Purpose	This procedure replaces a TSC card with a new TSC card.
Tools/Equipment	Replacement TSC card
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Note When an error is detected on a TSC card, the ONS 15600 SDH system switches control to the second TSC card; therefore, so it should not be necessary to change control when you replace the card.

Note You do not need to make any changes to the database if you are replacing it with a card of exactly the same type.

Note Card removal raises an improper removal (IMPROPRMVL) alarm, but this clears after the card replacement is completed.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you will replace the TSC card.

Step 2 To ensure that the card you are replacing is not the active TSC card, run the mouse over the card in CTC. If the card says Active, switch it to Standby:

a. Right-click the active TSC card to reveal the shortcut menu.

b. Click **Soft-reset Card**.

c. Click **Yes** when the confirmation dialog box appears.

d. Click **OK** when the "Lost connection to node, changing to Network View" dialog box appears.

Note The TSC card takes several minutes to reboot. See Table 2-1 on page 2-3 for more information about LED behavior during TSC card reboots.

Note Whenever TSC cards are changed from active to standby, it takes approximately 12 minutes to completely synchronize to the new system clock source due to the more accurate Stratum 3E timing module being adopted.

Step 3 Confirm that the TSC card you reset is in standby mode after the reset.

A TSC card that is ready for service has a green SRV LED illuminated. An active TSC card has a green ACT STBY LED illuminated, but a standby card does not have this LED illuminated.

Tip If you run the cursor over the TSC card in CTC, a popup displays the card's status (whether active or standby).

Step 4 Physically remove the card you want to replace from the ONS 15600 SDH:

a. Open the card ejectors.

b. Slide the card out of the slot.

Step 5 Insert the replacement TSC card into the empty slot:

a. Open the ejectors on the replacement card.

b. Slide the replacement card into the slot along the guide rails until it contacts the backplane.

c. Close the ejectors.

Step 6 If you want to make the replaced TSC card active, complete Steps 2b through 2d again.

Stop. You have completed this procedure.

Note The estimated time that a skilled technician takes to replace a fan tray is 2 minutes.

NTP-F240 Replace a Fan Tray

Purpose	This procedure replaces a fan tray with a new fan tray.
Tools/Equipment	Replacement fan tray
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Caution The center fan tray (tray 2) in the ONS 15600 SDH shelf is the most critical tray because it cools the common control cards. If both fans in this tray are inoperative, CTC initiates a five-minute countdown to shut down one of the SSXC cards. You should swap a working fan tray (tray 1 or 3) with tray 2 as soon as possible to prevent equipment damage.

Caution When a fan tray is removed from a shelf assembly, it momentarily creates the same situation that occurs if two fans in a single tray fail. In this situation (that is, the system is running on two fans), CTC software begins a five-minute countdown before shutting down SSXC card operation in order to protect the cards. Replace the fan tray in the shelf assembly as quickly as possible to avoid SSXC card shutdown.

Note The ONS 15600 SDH system requires at least one working fan in each of the three fan trays. When a single fan in a tray fails, Cisco recommends replacing the tray with a fully working tray as soon as practically possible. To replace a fan tray, it is not necessary to move any of the cable management facilities.

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

Step 1 Lift the latch on the fan tray that you want to replace, and pull the fan tray away from the shelf assembly.

Step 2 Insert the new fan tray in the shelf assembly.

Step 3 Press the latch down to secure the fan tray.

Stop. You have completed this procedure.

Note The estimated time that a skilled technician takes to replace a fan tray is 2 minutes.

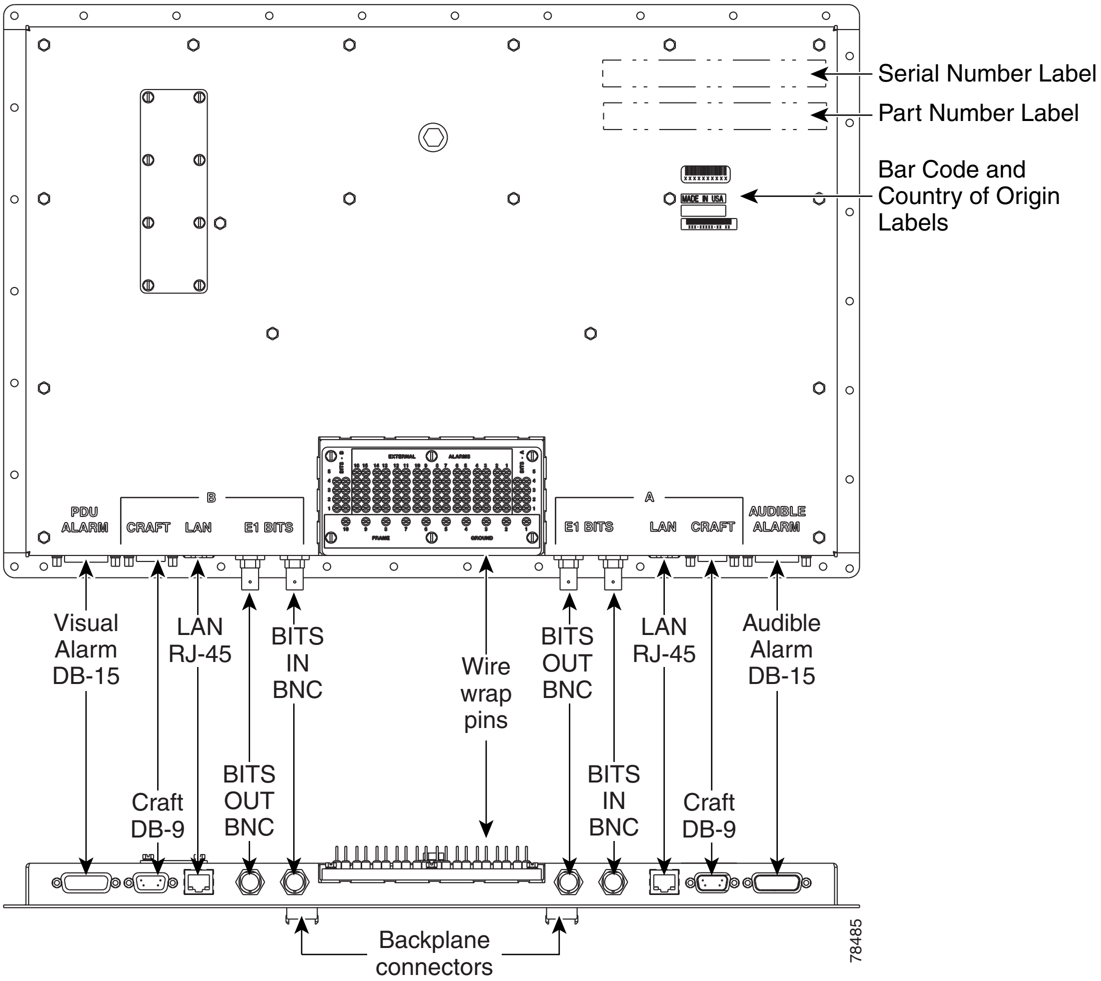
NTP-F241 Replace the Customer Access Panel

Purpose	This procedure replaces a customer access panel (CAP)/customer access panel version 2 (CAP2) with a new CAP/CAP2.
Tools/Equipment	Replacement CAP/CAP2
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note The 15600 SDH node is viewable only when CTC is connected to its front panel. You will not be able to view any other node that is connected to the ONS 15600 SDH through a DCC.

Step 1 Remove any tie wraps and cables attached to the CAP/CAP2 (Figure 14-5).

Figure 14-5 CAP/CAP2 Faceplate and Connections



Step 2 Remove the pin-field card, leaving the wires attached if possible. (If this is not possible, remove and label the wires.)

Step 3 To remove the CAP/CAP2:

a. Remove the 14 screws on the left and right sides of the CAP/CAP2 using a 3/16-inch (4.76-mm) socket.

b. Remove the 17 nuts on the top and bottom of the CAP/CAP2 using a 1/4-inch (6.35-mm) socket.

c. Loosen the center bolt using a 7/16-inch (11.113-mm) socket. This creates an extraction force on the connectors to successfully unmate them.

d. Pull the CAP/CAP2 off of the alignment pins.

Step 4 Place the replacement CAP/CAP2 over the alignment pins on the backplane and tighten the center bolt using a 7/16-inch (11.113-mm) socket. This creates an insertion force that successfully mates the connectors.

Step 5 Verify that the CAP/CAP2 cover is contacting the rear cover around the CAP/CAP2 perimeter.

Step 6 Replace the CAP/CAP2 screws and tighten to the specified torque (6 to 7 foot pounds).

Step 7 If you removed the wire-wrap wires from the pin field card, replace them on the pin field according to their labeled positions. If you removed the pin field card with the wires intact, reinstall the pin field card.

Step 8 Replace the tie wraps and cables.

Stop. You have completed this procedure.

NTP-F242 Remove a Power Distribution Unit

Purpose	This procedure removes the ONS 15600 SDH power distribution unit (PDU).
Tools/Equipment	Replacement PDU
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note The PDU can be ordered in entirety (including PDU-A, PDU-B, and alarm panel), or by part.

Step 1 Remove a PDU from a donor unit:

a. Secure an ESD-safe area to place dismounted equipment.

b. Working on the front of the donor unit, remove the donor PDU alarm unit from the center of the PDU:

- Use a slot screwdriver to loosen the front two screws on the PDU alarm unit until they click.
- Remove the alarm unit from the cabinet by pulling it straight out. Place it in an ESD-safe area.

c. Remove the donor PDU:

- Remove 1/4-inch (6.35-mm) nut and washer from frame ground lug on back side.
- Use a slot screwdriver to loosen the front two screws on the PDU until they click.
- Remove the PDU from the cabinet by pulling it straight out. Place it in an ESD-safe area.

Step 2 Disconnect the faulty PDU:

Note Wiring positions are mirrored for PDU-A and PDU-B with the exception of the frame ground wire and are marked on the top face of the PDU.

a. Disconnect DC power to the PDU to be replaced. For more information about bay power connections, see the "DLP-F167 Connect Office Power to the ONS 15600 SDH Bay" task on page 16-10.

b. Working on the side of the PDU, use a voltage meter to verify that there is no DC power present at the terminals. See the "DLP-F169 Verify Office Power" task on page 16-14.

c. Secure an ESD-safe area to place dismounted equipment.

d. Working on the side of the bay, use the 9/64-in. Allen wrench to loosen the two socket-head screws holding the plastic safety cover over the power terminals.

e. Remove the side plastic safety cover and screw down the socket-head screws by hand far enough for the PDU to clear the chassis when removed.

Note If socket-head screws are left partially screwed outward, the PDU cannot be removed from the chassis.

f. Working on the side of the bay, remove the electrical wiring of the faulty PDU:

Note In this procedure, all wiring screw post positions are referenced from right to left, starting with screw post one being rear-most.

- Use a 3/8-in. socket and wrench or socket driver to remove the green ground wire from the first vertical pair of screw posts.
- Remove the jumper cable from the frame to logic ground terminals.
- Remove the red 48-VDC power return wire from the third pair of screw posts.
- Remove the black 48-VDC power supply wire from the fourth pair of screw posts.

Note Looking at the back of the power unit from the rear of the bay, there are three areas of screw posts on the rear of the unit: (1) The top 12 screw posts hold the busbars; (2) the right-bottom (PDU-A) or left-bottom (PDU-B) three screw posts hold the black frame ground, and (3) the bottom-left (PDU-A) or bottom-right (PDU-B) six screw posts hold the green frame and logic grounds.

g. Working on the rear of the bay, remove the two thumbnuts holding the plastic safety cover. Remove the plastic safety cover.

h. Working on the rear of the power unit with the six bottom-left (PDU-A) or bottom-right (PDU-B) screw posts, remove the nuts, washers, frame and logic ground wires. Use a 7/16-inch (11.113-mm) socket on the nuts, and needle-nose pliers to remove the star washers.

Note Wiring positions are mirrored for PDU-A and PDU-B with the exception of the green frame ground wire to the rear of the bay.

i. Working on the rear of the bay with the top 12 screw posts, use a 7/16-inch (11.113-mm) socket and socket driver to remove the last four nuts holding PDU-B to the top-bay busbar. Use needle-nose pliers to remove the star washers.

j. Remove the 1/4-inch (6.35-mm) nut and washer from the frame ground lug.

Step 3 Working on the front of the bay, remove the faulty PDU:

a. Use a slot screwdriver to unscrew the two PDU slot screws until they click.

b. Pull the PDU straight out and place the PDU in the ESD-safe area.

Step 4 Continue with the "NTP-F243 Replace the Power Distribution Unit" procedure on page 14-33.

Stop. You have completed this procedure.

NTP-F243 Replace the Power Distribution Unit

Purpose	This procedure replaces the B-side PDU. To replace the PDU A-side, use the same procedure but reverse the wiring screw post positions.
Tools/Equipment	Replacement PDU
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note The PDU can be ordered in entirety (including PDU-A, PDU-B, and alarm panel) or by part.

Step 1 Working on the front of the bay:

a. Push the new PDU straight into the cabinet in the shelf.

b. Replace 1/4-inch (6.35-mm) nut and washer on rear frame ground lug.

c. Use a slot screwdriver to tighten the two slot screws on the front of the PDU.

Step 2 Working on the front of the bay, reinsert the alarm unit in the middle of the PDU:

a. Push the alarm unit straight into the cabinet in the bay.

b. Use a slot screwdriver to tighten the two slot screws on the front of the alarm unit.

Step 3 Working on the rear of the bay with the six bottom-right (PDU-A) or bottom-left (PDU-B) screw posts, replace the wires and the star washers. Use a 7/16-inch (11.113-mm) socket and wrench to replace the second and third nuts on the screw posts.

Note Wiring positions are mirrored for PDU-A and PDU-B with the exception of the green frame ground wire to the rear of the bay.

Step 4 Working on the rear of the bay with the top 12 screw posts, replace the busbars, the star washers, and the nuts holding the busbars to the PDU.

Step 5 Working on the rear of the bay, replace the PDU receive output cover over the top 12 screw posts.

Step 6 Working on the rear of the bay, replace the two thumbnuts that secure the PDU receive output cover.

Step 7 Working on the side of the bay, replace the electrical wiring:

a. Place the green jumper cable on the frame ground and logic ground screw posts.

b. Use a 7/16-inch (11.113-mm) socket and wrench or socket driver to replace the green ground wire on the rear-most vertical pair of screw posts. Torque all PDU side screw post nuts to 36 in.-lb.

c. Replace the red 48– VDC power return wire on the third pair of screw posts.

d. Replace the black 48– VDC power supply wire on the fourth pair of screw posts.

Step 8 Working on the side of the bay, replace the plastic safety cover over the power leads.

Step 9 Use the 9/64-inch (3.57-mm) Allen wrench to replace the two nuts that secure the plastic safety cover.

Step 10 Restore power to the bay.

Step 11 Check the voltage at the PDU input, output, and backplane busbar connections with a voltage meter. See the "DLP-F169 Verify Office Power" task on page 16-14.

Stop. You have completed this procedure.

NTP-F244 Edit Network Element Defaults

Purpose	This procedure edits the factory-configured network element (NE) defaults using the NE Defaults editor. The new defaults can either be applied only to the node on which they are edited or exported to a file and imported for use on other nodes.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note For a list of card and node default settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15600 SDH Reference Manual*. To change card settings individually (that is, without changing the defaults), see Chapter 10, "Change Card Settings." To change node settings, see Chapter 11, "Change Node Settings."

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to edit NE defaults.

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

Step 3 Under Defaults Selector, choose a card type (if editing card-level defaults), **CTC** (if editing CTC defaults), or **NODE** (if editing node-level defaults). Clicking on the node name (at the top of the Defaults Selector column) lists all available NE defaults in the Default Name column. To selectively display just the defaults for a given card type, for node-level, or for CTC-level, you can drill down the Defaults Selector menu structure.

Step 4 Locate a default you want to change under Default Name.

Step 5 Click in the **Default Value** column for the default property you are changing and either choose a value from the drop-down menu (when available), or type in the desired new value.

Note If you click **Reset** before you click **Apply**, all values will return to their original settings.

Step 6 Click **Apply** (click in the **Default Name** column to activate the Apply button if it is unavailable). You can modify multiple default values before applying the changes.

A pencil icon will appear next to any default value that will be changed as a result of editing the defaults file.

Step 7 If you are modifying node-level defaults, a dialog box appears telling you that applying defaults for node level attributes overrides current provisioning and asks if you want to continue. Click **Yes**.

If you are modifying the IIOP Listener Port setting, a dialog box appears warning you that the node will reboot and asks if you want to continue. Click **Yes**.

Note Changes to most node defaults reprovision the node when you click Apply. Changes made to card settings using the Defaults Editor do not change the settings for cards that are already installed or slots that are preprovisioned for cards, but rather, change only cards that are installed or preprovisioned thereafter. To change settings for installed cards or pre-provisioned slots, see Chapter 10, "Change Card Settings."

Note Changing some NE defaults can cause CTC disconnection or a reboot of the node in order for the default to take effect. Before you change a default, view the Side Effects column of the Defaults editor (right-click a column header and select **Show Column > Side Effects**) and be prepared for the occurrence of any side effects listed for that default.

Stop. You have completed this procedure.

NTP-F245 Import Network Element Defaults

Purpose	This procedure imports the NE defaults using the NE Defaults editor. The defaults can either be imported from the CTC software CD (factory defaults) or from a customized file exported and saved from a node.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note For a list of card and node default settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15600 SDH Reference Manual*.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to import NE defaults.

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

Step 3 Click **Import**.

Step 4 Click **Browse** and browse to the file you are importing if the correct file name and location of the desired file do not appear in the Import Defaults from File dialog box.

Step 5 When the correct file name and location appear in the dialog box, click **OK**. (The correct file name is 15600SDH-defaults.txt if you are importing the factory defaults.)

A pencil icon will appear next to any default value that will be changed as a result of importing the new defaults file.

Step 6 Click **Apply**.

Step 7 If the imported file fails to pass all edits, the problem field shows the first encountered problem default value that must be fixed. Change the problem default value and click **Apply**. Repeat until the imported file passes all edits successfully.

Step 8 If you are modifying node-level defaults, a dialog box appears telling you that applying defaults for node level attributes overrides current provisioning and asks if you want to continue. Click **Yes**.

If you are modifying the IIOP Listener Port setting, a dialog box appears warning you that the node will reboot and asks if you want to continue. Click **Yes**.

Note Changes to most node defaults reprovision the node when you click Apply. Changes made to card settings using the Defaults Editor do not change the settings for cards that are already installed or slots that are preprovisioned for cards, but rather, change only cards that are installed or preprovisioned thereafter. To change settings for installed cards or pre-provisioned slots, see Chapter 10, "Change Card Settings."

Note Changing some NE defaults can cause CTC disconnection or a reboot of the node in order for the default to take effect. Before you change a default, view the Side Effects column of the Defaults editor (right-click a column header and select **Show Column > Side Effects**) and be prepared for the occurrence of any side effects listed for that default.

Stop. You have completed this procedure.

NTP-F246 Export Network Element Defaults

Purpose	This procedure exports the NE defaults using the NE Defaults editor. The exported defaults can be imported to other nodes.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note The defaults currently displayed are exported whether or not they have been applied to the current node.

Note The NE defaults can also be exported from the File > Export menu. These exported defaults are for reference only and cannot be imported.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to export NE defaults.

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

Step 3 Click **Export**.

Step 4 If the desired file to export to does not appear in the Export Defaults to File dialog box (or does not yet exist) click **Browse** and browse to the directory where you want to export the data; then either choose or type in (to create) the file to export to [the defaults will be exported as a text file delimited by equals (=) signs].

Step 5 Click **OK**.

Stop. You have completed this procedure.

CHAPTER 15

Power Down the Node

This chapter explains how to power down a node and stop all node activity on the Cisco ONS 15600 SDH.

NTP-F247 Power Down the ONS 15600 SDH

Purpose	This procedure stops all node activity.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	For software steps, Provisioning level or higher is required. For hardware steps, any level is allowed.

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Caution The following procedure is designed to minimize traffic outages when powering down nodes, but traffic is lost if you delete and recreate circuits that passed through a working node.

Note Always use the supplied ESD wristband when working with the Cisco ONS 15600 SDH. Plug the wristband into the ESD jack located on the fan-tray assembly or on the lower-left outside edge of the shelf on the shelf assembly.

Step 1 Identify the node that you want to power down. If no cards are installed, go to Step 13. If cards are installed, complete the "DLP-F181 Log into CTC" task on page 16-34.

Step 2 In node (login) view, choose **Go to Network View** from the View menu.

Step 3 In network view, verify that the node is not connected to a network:

a. If the node is part of a working network, log out of the node and complete the "NTP-F217 Remove an SNCP Node" procedure on page 13-11, or the "NTP-F215 Remove an MS-SPRing Node" procedure on page 13-5. Continue with Step 4.

b. If the node is not connected to a working network and the current configurations are no longer required, proceed to Step 4.

Note Current configurations will be saved if Steps 4 through 11 are skipped.

Step 4 In node view, click the **Circuits** tab and verify that no circuits appear, then proceed to Step 5. If circuits appear, complete the "DLP-F293 Delete Circuits" task on page 17-83 to delete all the circuits that originate or terminate in the node. Repeat until no circuits are present.

Step 5 Complete the "DLP-F229 Delete a 1+1 Protection Group" task on page 17-25 to delete all protection groups. Repeat until no protection groups are present.

Step 6 Complete the "NTP-F209 Modify or Delete Communications Channel Terminations" procedure on page 11-8 to delete all RS-DCC and MS-DCC terminations. Repeat until no RS-DCC or MS-DCC terminations are present.

Step 7 Complete the "DLP-F254 Change the Service State for a Port" task on page 17-48 for each installed STM-N or DS-N card and change all ports to the Locked-enabled,disabled service state.

Step 8 Remove all fiber connections to the cards.

Step 9 Complete the "DLP-F389 Remove an SFP/XFP" task on page 18-105 if there are any SFPs installed.

Warning **Class 1 laser product.** Statement 1008

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 1051

Step 10 In node view, right-click an installed card and choose **Delete Card**.

Step 11 Click **Yes**.

Step 12 After you have deleted the cards, open the card ejectors for each card and remove each card from the node.

Step 13 Shut off the power from the power supply that feeds the node. For more information about power issues, see the "NTP-F113 Install the Bay Power and Ground" procedure on page 1-10.

Step 14 Disconnect the node from its external fuse source.

Step 15 Store all cards and update inventory records according to local site practice.

Stop. You have completed this procedure.

CHAPTER 16

DLPs F100 to F199

DLP-F161 Unpack and Verify the Bay Assembly

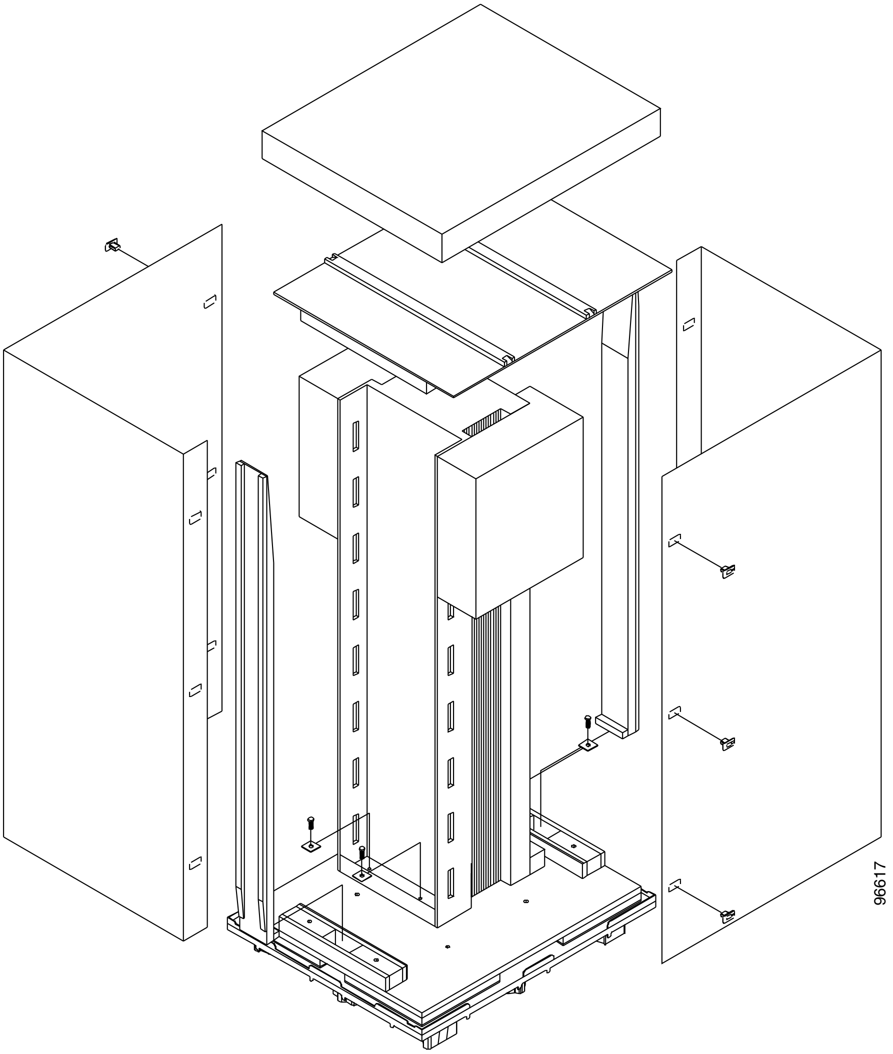
Purpose	This task removes the bay assembly from the package.
Tools/Equipment	Scissors Phillips screwdriver 3/4-in. Society of Automotive Engineers (SAE) socket wrench
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **In order to safeguard both equipment and personnel during the installation process, we recommend that four people participate in moving the unit. Using adequate manpower is the best guarantee that you will avoid harming people or equipment.** Statement 129

Step 1 Use a pallet jack or forklift to place the shipping container as close to the installation location as possible. Ensure that the space is sufficient to unpack the ONS 15600 SDH.

Figure 16-1 shows the packaging you must remove from the ONS 15600 SDH.

Figure 16-1 ONS 15600 SDH Bay Assembly Packaging



Step 2 Cut all of the plastic banding off the cardboard shipping container.

Step 3 Remove the cap from the corrugated container.

Step 4 Pull the side panels away from the shipping pallet and set them aside.

Step 5 Cut the banding that holds the top cap and ramps on the bay.

Step 6 Remove the top cap and ramps and set them aside.

Step 7 Carefully cut the plastic covering off the bay and remove.

Step 8 Remove the four bolts that hold the rack to the pallet (rack base bolts) using a 3/4-in. socket wrench.

Step 9 Open all other boxes shipped with this product. Verify that you have received all of the contents listed in the Included Materials, page 1-2.

Step 10 Return to your originating procedure (NTP).

DLP-F162 Inspect the Bay Assembly

Purpose	This task verifies that all parts of the bay assembly are in good condition.
Tools/Equipment	None
Prerequisite Procedures	DLP-F161 Unpack and Verify the Bay Assembly, page 16-1
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Look for any loose parts on the bay assembly.

Step 2 Verify that the wire-wrap pins on the customer access panel (CAP)/customer access panel version 2 (CAP2) at the rear of the bay are not bent or broken.

Step 3 Verify that the power distribution unit (PDU) is not damaged.

Step 4 If the pins on the CAP/CAP2 are bent or broken or the PDU is damaged, call your Cisco sales engineer for a replacement.

Step 5 Return to your originating procedure (NTP).

DLP-F163 Install the Dollies onto the Bay Assembly

Purpose	This task explains how to install the dollies on the bay assembly to assist with unloading the bay assembly at your site.
Tools/Equipment	Dollies (2) Ratchet 6-in. (or greater) ratchet extension (optional) 1-1/8-in. SAE socket 3/4-in. SAE socket 15/16-in. SAE socket
Prerequisite Procedures	NTP-F108 Unpack and Inspect the ONS 15600 SDH Bay Assembly, page 1-4
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note For information about obtaining installation dollies, contact your Cisco sales engineer.

Step 1 Inspect the dollies to make sure the caster wheels turn freely. If the wheels come in contact with the metal frame of the dolly, turn the screws at the top of the dolly until the wheels move freely.

Step 2 Use a ratchet to unscrew and remove the bolts attached to the top of one of the dollies.

Step 3 Line up the holes on one dolly with the holes at the front base of the bay.

Step 4 Use a ratchet to install the screws that secure the dolly to the bay.

Note A 6-in. (or greater) ratchet extension might be helpful when you install the dolly screws.

Step 5 Repeat Steps 2 through 4 to attach the other dolly to the rear base of the bay.

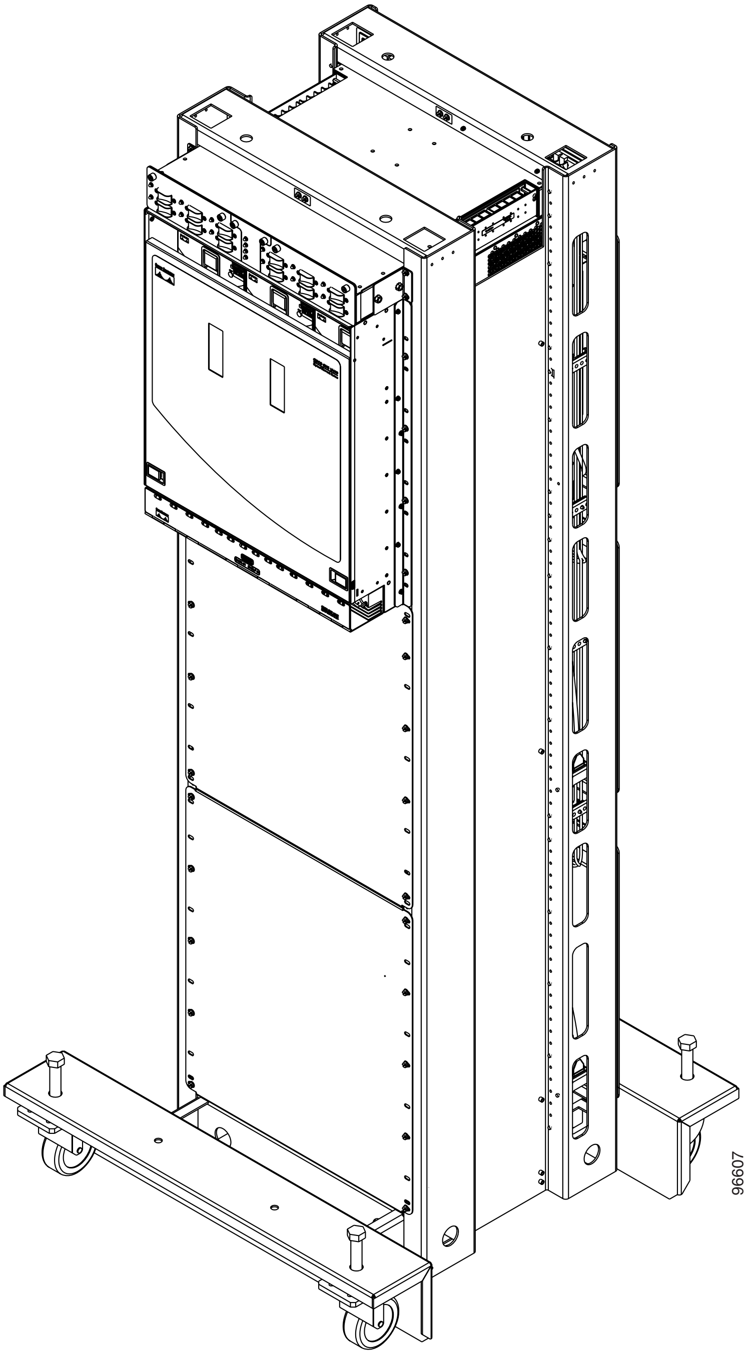
Step 6 Use a socket wrench to turn one of the screws attached to a caster five turns to the right (clockwise). Repeat this at each screw and repeat in sequence so that the bay gradually rises to maximum height (1-3/4 in. [44.45 mm]) off the pallet.

Step 7 Lay the wooden ramps down so that they line up with the dolly wheels.

Step 8 Remove the wooden blocks from the pallet to allow the bay to roll down the wooden ramps.

Step 9 With one person on each side of the bay assembly, carefully roll the bay down the ramps and onto the floor (Figure 16-2).

Figure 16-2 ONS 15600 SDH with Dollies Installed



Step 10 Return to your originating procedure (NTP).

DLP-F164 Install the Bay Assembly

Purpose	This task explains how to install the bay assembly at the installation site.
Tools/Equipment	Ratchet 6-in. (or greater) ratchet extension (optional) SAE socket wrench SAE torque wrench Phillips screwdriver, 6 in. long 600-mm kick plate kit (53-2177-XX), or 900-mm kick plate kit (53-2178-XX) Rectangular seismic washers (4) (53-2141-XX) 5/8-in. floor anchor bolts (4)
Prerequisite Procedures	NTP-F108 Unpack and Inspect the ONS 15600 SDH Bay Assembly, page 1-4 DLP-F248 Drill Holes to Anchor and Provide Access to the Bay Assembly, page 17-41 DLP-F163 Install the Dollies onto the Bay Assembly, page 16-3
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note This procedure describes how to install an ONS 15600 SDH bay in an overhead power environment. Test and install according to local site practice.

Step 1 Place the bay directly over the bolt holes in the floor. (To install an ONS 15600 SDH in a raised-floor environment, place the bay directly over the studs that protrude from the floor.)

Step 2 Position the four rectangular seismic washers and floor bolts into the bolt holes.

Step 3 Use a socket wrench to turn one of the screws attached to a caster five turns to the left (counter-clockwise). Repeat this at each screw and repeat in sequence so that the bay gradually lowers and firmly rests on the floor.

Step 4 Use a ratchet and socket to remove the two bolts that attach the dolly to the bay.

Note A 6-in. (or greater) ratchet extension might be helpful when you remove the dolly bolts.

Step 5 Repeat Steps 3 and 4 for the other dolly.

Step 6 Use the torque wrench to torque the 5/8-in. floor bolts according to the bolt manufacturer’s torque specification.

Step 7 Install both kick plates at the front and rear base of the bay:

a. Line up the kick plates with the holes on the bay’s frame.

b. Use a Phillips screwdriver to tighten the five screws that fasten each kick plate to the bay.

Step 8 Return to your originating procedure (NTP).

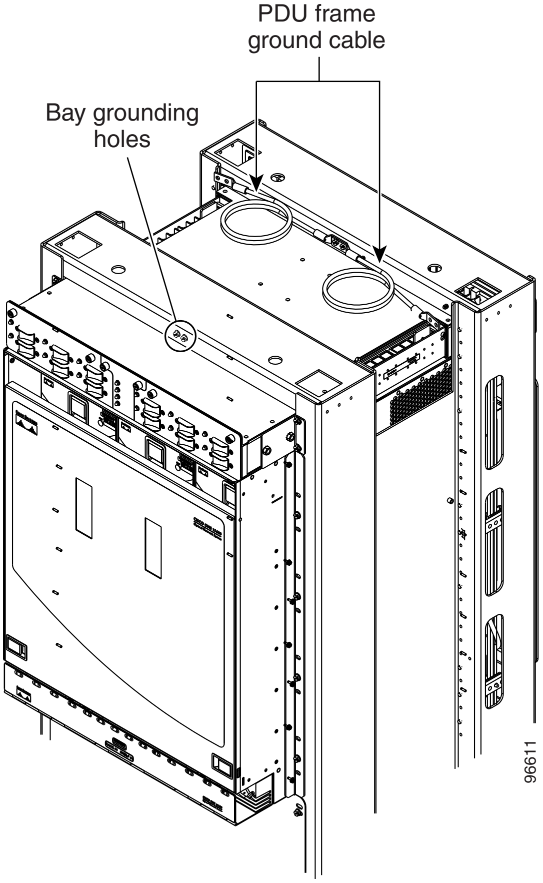
DLP-F165 Connect the Office Ground to the ONS 15600 SDH

Purpose	This task connects the office ground to the ONS 15600 SDH bay assembly.
Tools/Equipment	7/16-in. SAE socket Socket driver Ground cable, rated for at least 125-A delivery Crimp tool Wire strippers Wire cutters Listed pressure terminal connectors (two hole lug, 0.63-in. spaced, 1/4-in. bolt size); connectors must be suitable for at least 125-A delivery copper conductors Antioxidant compound
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 213

Step 1 Remove any paint from the two-hole lug position on the bay front ground holes (Figure 16-3).

Figure 16-3 PDU Ground Cables and Grounding Holes



Step 2 Apply the antioxidant compound to the two-hole lug position.

Step 3 Connect the office ground cable to the bay front two-hole lug position.

Step 4 Return to your originating procedure (NTP).

DLP-F166 Create an IP-Encapsulated Tunnel

Purpose	This task creates a an IP-encapsulated tunnel to transport traffic from third-party SDH equipment across ONS 15600 SDH networks. IP-encapsulated tunnels are created on the regenerator-section data communications channel (RS-DCC) channel (D1-D3) (if not used by the ONS 15600 SDH as a terminated DCC).
Tools/Equipment	STM-N cards must be installed.
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 NTP-F163 Verify Network Turn-Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Each ONS 15600 SDH can have up to 128 IP-encapsulated tunnel connections. Terminated Regenerator-Section DCCs (RS-DCCs) used by the ONS 15600 SDH cannot be used as tunnel endpoints, and an RS-DCC that is used as a tunnel endpoint cannot be terminated. All tunnel connections are bidirectional.

Step 1 Verify that IP addresses are provisioned at both the source and destination nodes of the planned tunnel. For more information, see the "DLP-F185 Provision IP Settings" task on page 16-38.

Step 2 In network view, click the **Provisioning > Overhead Circuits** tabs.

Step 3 Click **Create**.

Step 4 In the Overhead Circuit Creation dialog box, complete the following in the Circuit Attributes area:

- Name—Type the tunnel name.
- Type—Choose **IP Tunnel-D1-D3**.
- Maximum Bandwidth—Type the percentage of total RS-DCC bandwidth used in the IP tunnel (the minimum percentage is 10 percent).

Step 5 Click **Next**.

Step 6 In the Circuit Source area, complete the following:

- Node—Choose the source node.
- Slot—Choose the source slot.
- Port—If available, choose the source port.
- Channel—Displays IPT (D1-D3).

Step 7 Click **Next**.

Step 8 In the Circuit Destination area, complete the following:

- Node—Choose the destination node.
- Slot—Choose the destination slot.
- Port—If available, choose the destination port.
- Channel—Displays IPT (D1-D3).

Step 9 Click **Finish**.

Step 10 Put the ports that are hosting the IP-encapsulated tunnel in service. See the "DLP-F254 Change the Service State for a Port" task on page 17-48 for instructions.

Step 11 Return to your originating procedure (NTP).

DLP-F167 Connect Office Power to the ONS 15600 SDH Bay

Purpose	This task connects power to the ONS 15600 SDH bay assembly.
Tools/Equipment	9/64-in. Allen wrench Wire-wrap tool (suitable for #22 to #28 AWG alarm wires) Wire cutters Wire strippers Crimp tool Power cables, rated for at least 125-A delivery Listed pressure terminal connectors (two hole lug, 0.63-in. spaced, 1/4-in. bolt size); connectors must be suitable for at least 125-A delivery copper conductors
Prerequisite Procedures	DLP-F165 Connect the Office Ground to the ONS 15600 SDH, page 16-7
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **This warning applies only to units equipped with DC input power supplies. Wire the DC power supply using the appropriate lugs at the wiring end. The proper wiring sequence is ground to ground, positive to positive (line to L), and negative to negative (neutral to N). Note that the ground wire should always be connected first and disconnected last.** Statement 152

Caution Cisco supports only dual office-power feeds.

Note If you encounter problems with the power supply, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Step 1 Measure and cut the cables as needed to reach the ONS 15600 SDH PDU from the office power distribution panel. Figure 17-8 on page 17-72 shows the ONS 15600 SDH power terminal block on the right side (B side) of the bay.

Step 2 If either PDU terminal cover is still installed, use the 9/64-in. Allen wrench to loosen the two screws that hold the plastic PDU. Pull the cover away from the shelf and set the cover aside.

Note Use only pressure terminal connectors, such as two-hole lug types, when terminating the battery, battery return, and frame ground conductors.

Caution Before you make any crimp connections, coat all bare conductors (battery, battery return, and frame ground) with an appropriate antioxidant compound. Bring all unplated connectors, braided strap, and bus bars to a bright finish, then coat with an antioxidant before you connect them. You do not need to prepare tinned, solder-plated, or silver-plated connectors and other plated connection surfaces, but always keep them clean and free of contaminants.

Caution When terminating power, return, and frame ground, do not use soldering lug, screwless (push-in) connectors, quick-connect, or other friction-fit connectors.

Step 3 Strip 1/2 in. (12.7 mm) of insulation from all power cables that you will use.

Step 4 If the bay is being installed in a raised-floor environment, complete the "DLP-F168 Route and Terminate Raised-Floor Power Cables" task on page 16-12.

Step 5 Crimp the lugs onto the ends of all power leads.

Note When terminating battery and battery return connections as shown in Figure 17-8 on page 17-72, follow a torque specification of 36 in-lb. When terminating a frame ground, use the Kepnut provided with the ONS 15600 SDH and tighten it to a torque specification of 36 in-lb.

Step 6 Put the 48 VDC power return wire on the third pair of screw posts (counting from the rear of the PDU).

Note All screw posts are labeled at the top of the PDU.

Step 7 Put the 48 VDC power supply wire on the fourth pair of screw posts.

Step 8 Hold the plastic safety cover in place over the power leads. Use the 9/64-in. Allen wrench to tighten the two screws that hold the plastic safety cover in place.

Step 9 Repeat Steps 6 through 8 for the left (A) side of the bay.

Step 10 Apply power to the node.

Step 11 Return to your originating procedure (NTP).

DLP-F168 Route and Terminate Raised-Floor Power Cables

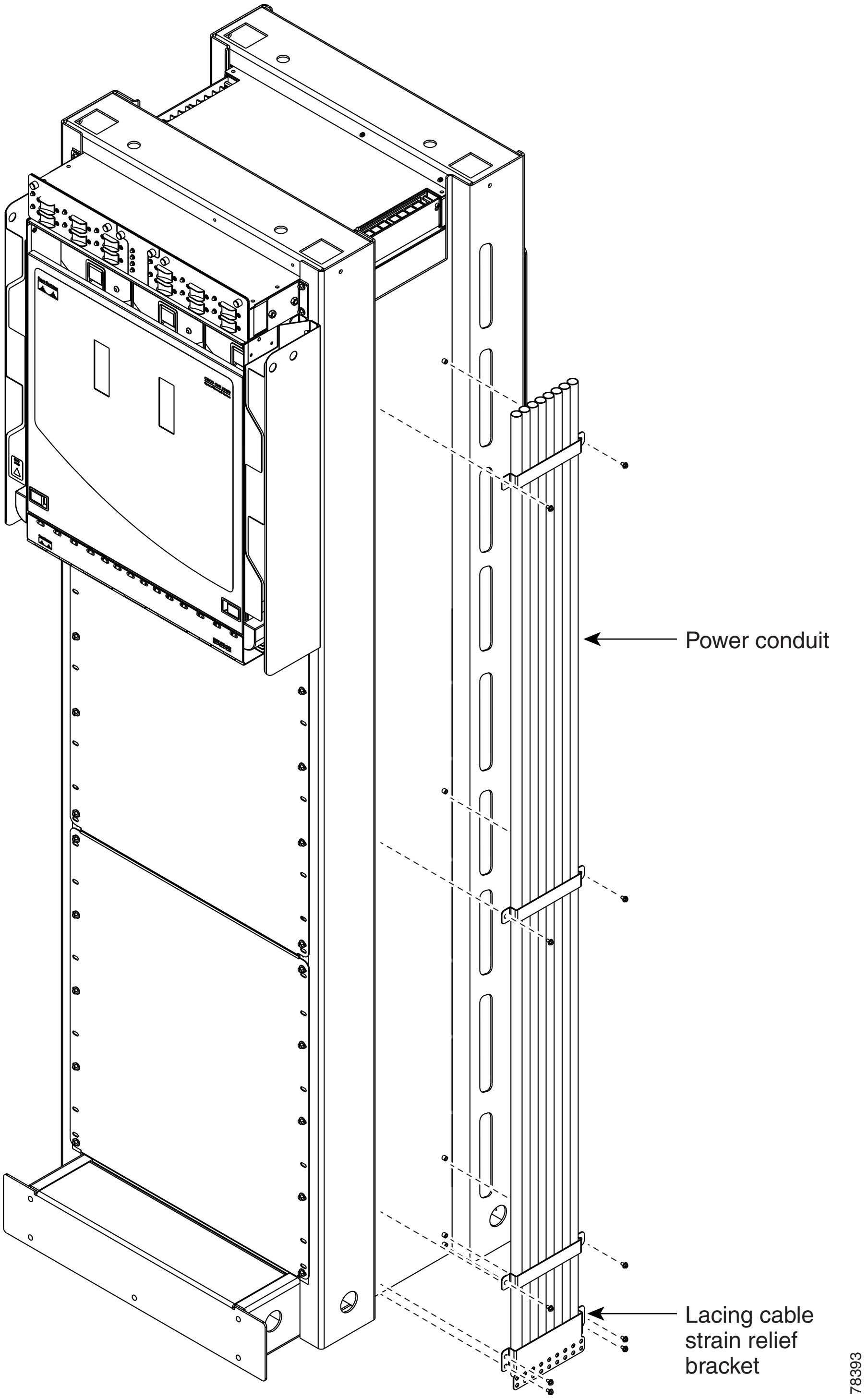
Purpose	This task installs the power conduit included in the raised-floor power kit and routes and terminates the power cables.
Tools/Equipment	Screwdriver Ground cables, rated for at least 125-A capacity Two-hole power lugs, 0.625-in. hole spacing; 0.25-in. bolt holes (Panduit LCCF2-14AZFW-E) (for underfloor-routed power cables) (16) **Note** You must use the specified lug type in order to terminate raised floor cables. Raised-floor power kit (800-23062-XX), which includes: • Screws and washers, #8 x 0.75 in. (12) • Screws and washers, #8 x 0.375 in. (8) • Power conduits (2) • Strain-relief cable brackets (2) • Panduit heat shrink #HSTT50-C
Prerequisite Procedures	DLP-F165 Connect the Office Ground to the ONS 15600 SDH, page 16-7 DLP-F167 Connect Office Power to the ONS 15600 SDH Bay, page 16-10
Required/As Needed	As needed for bays installed in a raised-floor environment where the power cables originate from the floor.
Onsite/Remote	Onsite
Security Level	None

Step 1 On either side of the bay, locate the holes provided to mount the power conduit (Figure 16-4).

Step 2 On one side of the bay, line up the conduit's braces with the mounting holes.

Step 3 Use a screwdriver to install 6 screws (0.75 in.) into the mounting holes with one washer under the head of each screw.

Figure 16-4 Installing the Power Conduit in a Raised-Floor Power Environment



Step 4 Line up the strain-relief cable bracket at the base of the conduit. Install four of the 0.375-in. screws.

Step 5 Carefully push the power cables up through the conduit.

Step 6 Place the heat shrink tube on the cable.

Step 7 Crimp a lug onto one of the power cables.

Step 8 Put the heat shrink over the barrel of the power terminals to provide insulation.

Step 9 Secure the lug with the two nuts provided onto the PDU terminal. Torque to 36 in-lb.

Step 10 Lace or tie-wrap the cable to the cable strain relief bracket according to local site practice.

Step 11 Repeat Steps 7 through 10 for every power and ground cable on that side of the bay.

Step 12 Repeat this task for the other side of the bay.

Step 13 Return to your originating procedure (NTP).

DLP-F169 Verify Office Power

Purpose	This task measures the power to verify correct power and returns.
Tools/Equipment	Voltmeter
Prerequisite Procedures	DLP-F165 Connect the Office Ground to the ONS 15600 SDH, page 16-7 DLP-F167 Connect Office Power to the ONS 15600 SDH Bay, page 16-10
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Turn office power on to the A side of the PDU and turn office power off to the B side of the PDU.

Step 2 Observe that the A side, Shelf 1 green LED is lit on the front face of the PDU. The green LED indicates the voltage is within the appropriate range and the polarity is correct. Reversed voltage will result in unlit LEDs. Red LEDs indicate the circuit breakers are off or voltage is too low. Diagnose any errors and correct before continuing with this procedure. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for more information.

Step 3 To verify power using a voltmeter, place the black test lead of the voltmeter to the PDU A-side frame ground input terminal. Place the red test lead to the PDU A-side supply input terminal. Verify that the voltage reading is between –40.5 VDC and –57 VDC.

Note All PDU terminals are labeled on the top of the PDU.

Step 4 To verify ground, place the black test lead of the voltmeter to the PDU A-side frame ground input terminal. Place the red test lead to the PDU A-side logic ground terminal and verify that no voltage is present.

Step 5 Turn office power on to the B side of the PDU and turn office power off to the A side of the PDU.

Step 6 Observe that the B side, Shelf 1 green LED is lit on the front face of the PDU. Diagnose any errors and correct them before continuing with this task.

Step 7 To verify power using a voltmeter, put the black test lead of the voltmeter to the PDU B-side frame ground input terminal. Put the red test lead to the PDU B-side supply input terminal. Verify that the voltage reading is between –40.5 VDC and –57 VDC.

Step 8 To verify ground, put the black test lead of the voltmeter to the PDU B-side frame ground input terminal. Put the red test lead to the PDU B-side logic ground terminal and verify that no voltage is present.

Step 9 Turn office power back on to the A side of the PDU.

Step 10 Return to your originating procedure (NTP).

DLP-F170 Install T1 (100 Ohm) Timing Connections on the CAP/CAP2

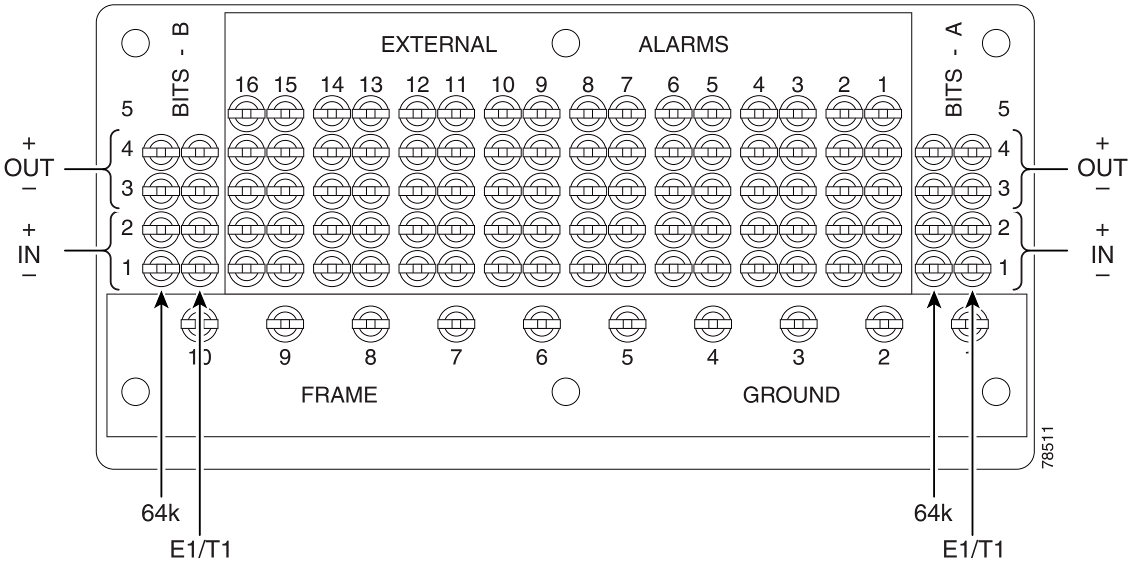
Purpose	This task installs timing connections from a 100-ohm T1 source to the CAP/CAP2; it is required if the node is using a T1 timing source for external building integrated timing supply (BITS) timing.
Tools/Equipment	Wire-wrap tool (suitable for #22 to #28 AWG alarm wires)
	#22 or #24 AWG wire shielded twisted pair
Prerequisite Procedures	NTP-F113 Install the Bay Power and Ground, page 1-10
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Wrap the clock wires on the appropriate wire-wrap pins according to local site practice.

Figure 16-5 shows the location of the timing connections on the pin field.

Note Only 100-ohm T1 BITS is supported in Release 8.0.

Figure 16-5 BITS Timing Connections on the CAP/CAP2



Step 2 Wrap the ground shield of the alarm cable to one of the frame ground pins beneath the timing pin field.

Note For more detailed information about timing, refer to the *Cisco ONS 15600 SDH Reference Manual*. To set up system timing, see the NTP-F137 Set Up Timing, page 4-9.

Step 3 Lace or tie wrap cables to the tie-wrap features that are located below the connector pattern, according to local site practice.

Step 4 Return to your originating procedure (NTP).

DLP-F171 Install LAN Cables on the CAP/CAP2

Purpose	This task installs the LAN wires on the CAP/CAP2; it is required to create external LAN connections.
Tools/Equipment	Straight-through (CAT-5) LAN cables
Prerequisite Procedures	NTP-F113 Install the Bay Power and Ground, page 1-10
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Only the active TSC card's connector is active. If you connect to the standby or switch TSCs, you will lose connectivity. Cisco recommends that you use the RJ-45 connector on the CAP/CAP2 card so that connection to the ONS 15600 SDH will not be lost during a TSC switch.

Step 1 Plug the straight-through (CAT-5) LAN cable into one of the ports labeled "LAN" on the CAP/CAP2 (Figure 16-6 on page 16-20).

Note You can cable both LAN ports but only one will be active at a time.

Step 2 Lace or tie wrap the cable to one of the tie-wrap features located below the connector pattern, according to local site practice.

Step 3 Return to your originating procedure (NTP).

DLP-F172 Install the TL1 Craft Interface Cable

Purpose	This task installs the Transaction Language One (TL1) craft interface cable on the CAP/CAP2.
Tools/Equipment	EIA/TIA-232 cable (9 pin D-sub)
Prerequisite Procedures	NTP-F113 Install the Bay Power and Ground, page 1-10
Required/As Needed	As needed

Onsite/Remote	Onsite
Security Level	None

Note Rather than using the craft pins, you can use a straight-through cable connected to the TSC RS-232 (EIA/TIA-232) port to access a TL1 craft interface.

Step 1 Plug the EIA/TIA-232 cable into the port labeled "CRAFT" on the CAP/CAP2.

Figure 18-28 on page 18-110 shows the back of the ONS 15600 SDH, including the CAP/CAP2 and the location of the CRAFT ports.

Note Use a null-modem adapter if you will be connecting a UNIX-based computer to the ONS 15600 SDH. Refer to the *Cisco ONS SDH TL1 Command Guide* for further information.

Step 2 Return to your originating procedure (NTP).

DLP-F173 Inspect the Bay Installation and Connections

Purpose	This task inspects the bay installation and connections to verify that everything is installed and connected properly.
Tools/Equipment	None
Prerequisite Procedures	Table 1-1 on page 1-13
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Check each wire and cable connection to make sure all cables are locked securely. If a wire or cable is loose, return to the appropriate procedure in this chapter to correct it.

Step 2 To check that the CAP/CAP2 is seated correctly, verify that the screws are secure and the pin field is firmly attached.

Step 3 Return to your originating procedure (NTP).

DLP-F174 Delete a Card from CTC

Purpose	This task deletes a card from Cisco Transport Controller (CTC).
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, right-click the card you want to delete on the shelf graphic. A shortcut menu appears.

Step 2 Choose **Delete Card** from the menu and click **Yes** in the confirmation dialog box.

You cannot delete a card if any of the following conditions apply:

- The card is part of a protection group; see the "DLP-F229 Delete a 1+1 Protection Group" task on page 17-25.
- The card has any circuits; see the "DLP-F293 Delete Circuits" task on page 17-83.
- The card is being used for timing; see the "DLP-F230 Change the Node Timing Source" task on page 17-26.
- The card has an SDH DCC termination; see the NTP-F209 Modify or Delete Communications Channel Terminations, page 11-8.

Note If the card that you deleted is still installed, it will reboot and reappear in CTC.

Step 3 Return to your originating procedure (NTP).

DLP-F175 Install Fiber-Optic Cables in a 1+1 Configuration

Purpose	This task installs fiber-optic cables on optical (STM-N) cards in a 1+1 linear configuration.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-F119 Install the STM-N Cards, page 2-4 NTP-F231 Clean Fiber Connectors and Adapters, page 14-16
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note With all fiber types, network planners/engineers should review the relative fiber type and optics specifications to determine attenuation, dispersion, and other characteristics to ensure appropriate deployment.

Step 1 Align the white stripe of the cable connector with the white stripe on the receiving connector (OGI for STM-16 or STM-64 cards, LC for ASAP cards) of the faceplate connection point. Each card has four connectors on the faceplate.

Table 16-1 shows the OGI connector pinouts on the STM-16 card faceplate.

Table 16-1 OC48/STM16 Cards OGI Connector Pinout

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

Table 16-2 shows the OGI connector pinouts on the front of the STM-64 card faceplate.

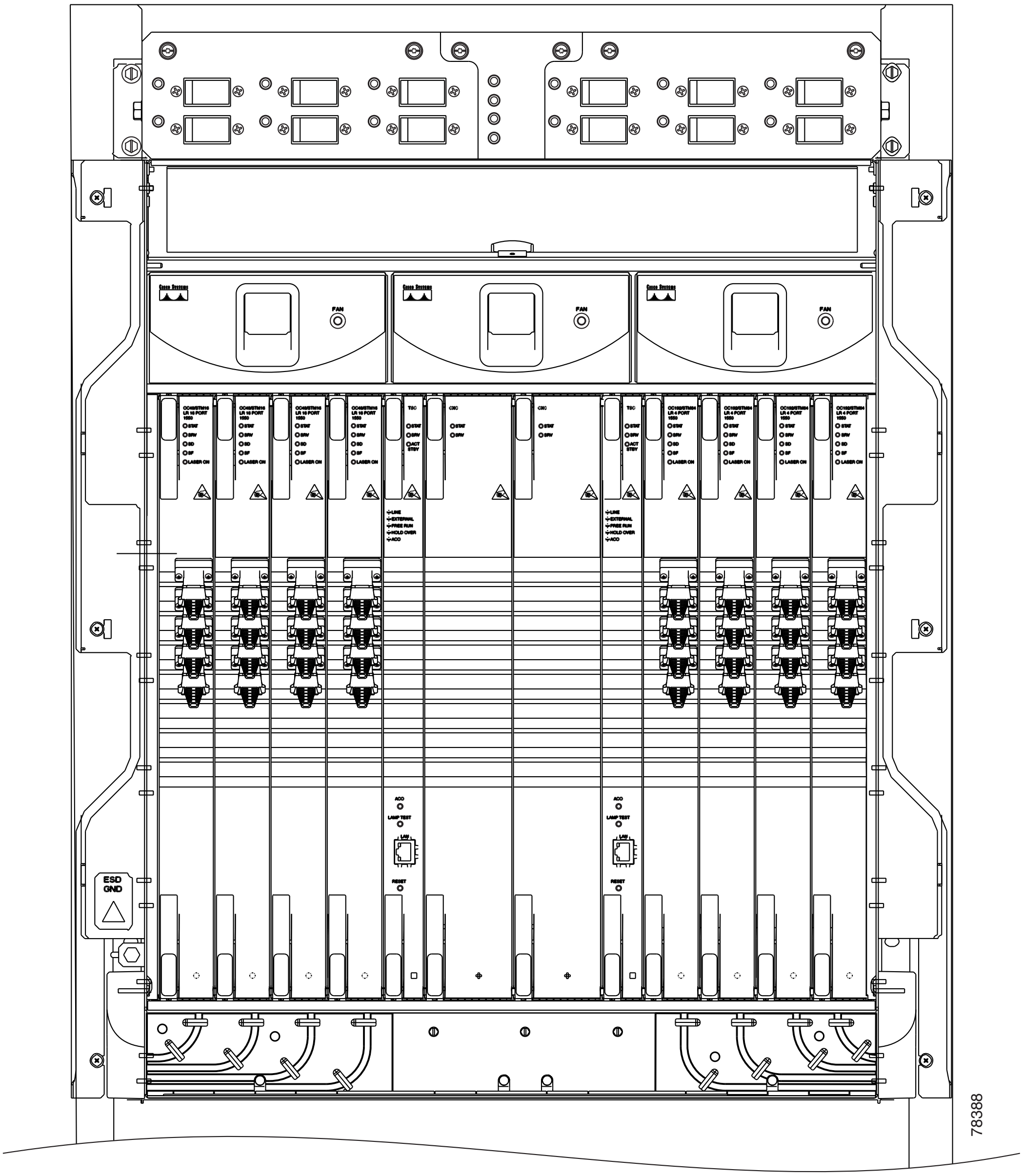
Table 16-2 OC192/STM64 Cards OGI Connector Pinout

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

Note Refer to the “Card Features and Functions” chapter of the *Cisco ONS 15600 SDH Reference Manual* for information about the ASAP card connector numbering.

Figure 16-6 shows all of the cards installed in the shelf and the optical connectors.

Figure 16-6 ONS 15600 SDH with Optical Cards Installed



Step 2 Remove the dust cap from the OGI or LC connector adapter on the front of the card.

Step 3 Plug the fiber into the connector (Tx and Rx) of a working (instead of protect) STM-N port at one node by squeezing the latches on either side of the connector and gently pushing it into the faceplate connection point until the connector snaps into place.

Step 4 Plug the other end of the fiber into the connector of a working port on an STM-N card at an adjacent node.

Step 5 Repeat Steps 2 through 4 for the protect ports on the two STM-N cards you are using, and then for each fiber-optic cable you require.

Step 6 Return to your originating procedure (NTP).

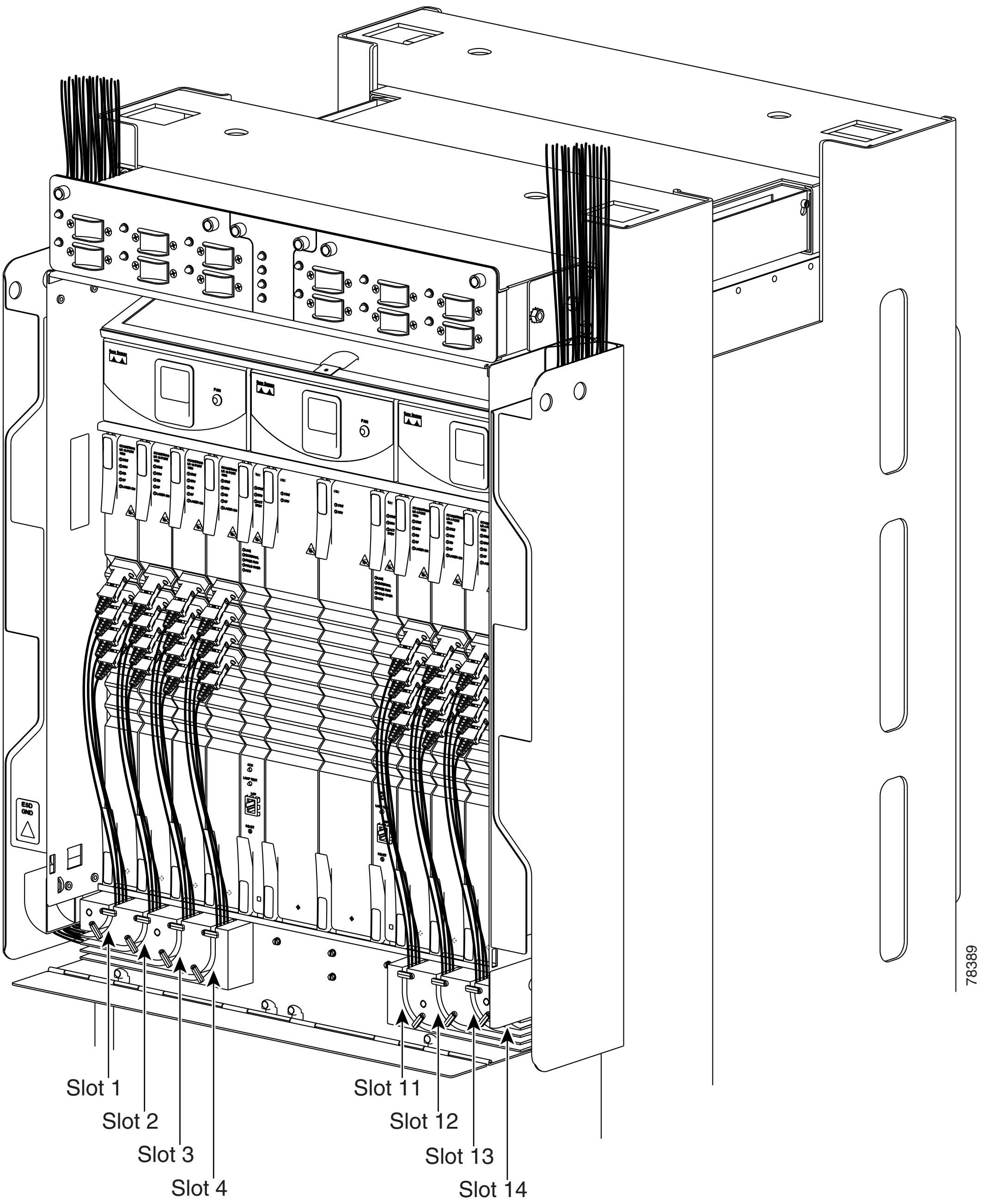
DLP-F176 Route Fiber-Optic Cables

Purpose	This task explains how to route fiber-optic cables away from the card faceplates and onto the side of the shelf.
Tools/Equipment	Tie-wrap (Suggested: Panduit TAK-TAPE TTS-20R0 Nelcro tie-wraps)
Prerequisite Procedures	NTP-F124 Install the Fiber-Optic Cables, page 2-9
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Open the fold-down front door on the cable-management tray.

Step 2 For each optical card you plan to install, find the corresponding cable routing channel directly below that card (Figure 16-7.)

Figure 16-7 ONS 15600 SDH with All Optical Cards Cabled and Routed



Step 3 Rotate the plastic cable latches for each optical card you will install to the open position so that they do not block the cable routing channels in the cable-management tray.

Step 4 Route the fiber cable from the connector on the card through the corresponding cable routing channel in the cable-management tray. Start from the innermost card on one side of the shelf (Slot 4 on the left side, for instance).

Note If a slot is empty, leave the corresponding cable routing channel empty for later use.

Step 5 If narrow cable routing modules (CRMs) are installed:

a. Route the fiber cables through the cable-management tray toward the edge of the bay and then up through the narrow CRM attached to the side of the bay, inserting the fiber into the open tracks in the narrow CRM (Figure 16-7 on page 16-22). Make sure the cables line up directly in front of the corresponding card so the cables are not disturbed if later a card is removed.

b. Rotate the corresponding cable latch to the closed position so it secures the fiber cables within the corresponding cable routing channel.

c. Repeat Steps a and b for the fiber cables from each installed STM-N card, working from the innermost cards outward.

Step 6 If wide CRMs are installed:

a. Gently pull the spool flanges toward you until they click open.

b. Route the fiber cables through the cable-management tray toward the edge of the bay and then up through the wide CRM attached to that side of the bay. Gently loop the cable around the spools. Store no more than one meter of slack (on average) for each cable that you route through the wide CRM.

Note If your site uses underfloor cabling, route the cables down to the CRM on the shelf directly below the node for which you are routing cables.

c. Rotate the corresponding cable latch to the closed position so it secures the fiber cables within the corresponding cable routing channel.

d. Repeat Steps a through c for the fiber cables from each installed STM-N card, working from the innermost cards outward. Distribute the cables as evenly as possible on the three storage spools of the CRM.

e. Push any extended spool flanges away from you so that they click closed.

f. Use tie wrap to secure the cable and minimize slack. Start with the cables closest to the outside edge of the CRM.

Step 7 Make sure all the plastic cable latches are in the closed position.

Step 8 Close the fold-down tray door when all fiber cables are properly routed.

Step 9 Return to your originating procedure (NTP).

DLP-F177 Run the CTC Installation Wizard for Windows

Purpose	This task installs the CTC online user manuals, Acrobat Reader 6.0.1, Java Runtime Environment (JRE) 5.0, and the CTC Java archive (JAR) files. JRE 5.0 is required to run Software Release 8.0. Preinstalling the CTC JAR files saves time at initial login. If the JAR files are not installed, they are downloaded from the TSC card the first time you log in.
Tools/Equipment	Cisco ONS 15600 SDH Release 8.0 software CD
Prerequisite Procedures	None
Required/As Needed	This task is required if any one of the following is true: • JRE 5.0 is not installed. • CTC online user manuals are not installed and are needed. • CTC JAR files are not installed and are needed.
Onsite/Remote	Onsite or remote
Security Level	None

Note If you will log into nodes running CTC software earlier than Release 4.6, uninstall JRE 5.0 and reinstall JRE 1.3.1_2. To run R5.0 and later, uninstall JRE 1.3.1_2 and reinstall JRE 5.0. Software R8.0 requires JRE 5.0.

Note JRE 1.4.2 requires Netscape 7.x or Internet Explorer 6.x.

Step 1 Verify that your computer has the following:

- Processor—Pentium III, 700 Mhz or faster
- RAM—384 MB recommended, 512 MB optimum
- Hard drive—20 GB hard drive recommended with at least 50 MB of space available
- Operating System—Windows 98 (1st and 2nd editions), Windows NT 4.0 (with Service Pack 6a), Windows 2000 (with Service Pack 3), or Windows XP Home

  If your operating system is Windows NT 4.0, verify that Service Pack 5 or later is installed. From the Start menu, choose **Programs > Administrative Tools > Windows NT Diagnostics** and check the service pack on the Version tab of the Windows NT Diagnostics dialog box. If Service Pack 6a or later is not installed, do not continue. Install Service Pack 6a following the computer upgrade procedures for your site.

  Note Processor and RAM requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM. Refer to the *Cisco ONS 15600 SDH Reference Manual* to find computer requirements needed for small, medium, and large ONS 15600 SDH networks.

Step 2 Insert the Cisco ONS 15600 SDH Release 8.0 software CD into your computer CD drive. The installation program begins running automatically. If it does not start, navigate to your computer's CD directory and double-click **setup.exe**.

The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer:

- Java Runtime Environment 5.0
- Acrobat Reader 6.0.1
- Online User Manuals
- CTC JAR files

Step 3 Click **Next**.

Step 4 Complete one of the following:

- Click **Typical** to install both the Java Runtime Environment and online user manuals. If you already have JRE 5.0 installed on your computer, choose **Custom**.
- Click **Custom** if you want to install either the JRE or the online user manuals. By default, Acrobat Reader and the online user manuals are selected.

Step 5 Click **Next**.

Step 6 Complete the following, as applicable:

- If you selected Typical in Step 4, skip this step and continue with Step 7.
- If you selected Custom, check the CTC component that you want to install and click **Next**.
  - If you selected Online User Manuals, continue with Step 7.
  - If you did not select Online User Manuals, continue with Step 9.

Step 7 The directory where the installation wizard will install CTC online user manuals appears. The default is C:\Program Files\Cisco\CTC\Documentation.

- If you want to change the CTC online help directory, type the new directory path in the Directory Name field, or click **Browse** to navigate to the directory.
- If you do not want to change the directory, skip this step.

Step 8 Click **Next**.

Step 9 Review the components that will be installed. If you want to change the components, complete one of the following:

- If you selected Typical in Step 4, click **Back** twice to return to the installation setup type page. Choose **Custom** and repeat Steps 6 through 8.
- If you selected Custom in Step 4, click **Back** once or twice (depending on the components selected) until the component selection page appears. Repeat Steps 6 through 8.

Step 10 Click **Next**. It might take a few minutes for the JRE installation wizard to appear. If you selected Custom in Step 4 and need to install a JRE, continue with Step 12.

Step 11 To install the JRE, complete the following:

a. In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and choose one of the following:

   - **I accept the terms of the license agreement**—Accepts the license agreement. Continue with Step b.
   - **I do not accept the terms of the license agreement**—Disables the Next button on the Java 2 Runtime Environment License Agreement dialog box. Click **Cancel** to return to the CTC installation wizard. CTC will not install the JRE. Continue with Step 12.

Note If JRE 5.0 is already installed on your computer, the License Agreement page does not appear. You must click Next and then choose Modify to change the JRE installation or Remove to uninstall the JRE. If you choose Modify and click Next, continue with Step e. If you choose Remove and click Next, continue with Step i.

b. Click **Next**.

c. Choose one of the following:

- Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
- Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.

d. Click **Next**.

e. If you selected Typical, continue with Step i. If you selected Custom, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:

- Java 2 Runtime Environment—(Default) Installs JRE 5.0 with support for European languages.
- Support for Additional Languages—Adds support for non-European languages.
- Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

The drop-down list options for each program feature include:

- This feature will be installed on the local hard drive—Installs the selected feature.
- This feature and all subfeatures will be installed on the local hard drive—Installs the selected feature and all subfeatures.
- Don’t install this feature now—Does not install the feature (not an option for Java 2 Runtime Environment).

To modify the directory where the JRE version is installed, click **Change**, navigate to the desired directory, and click **OK**.

f. Click **Next**.

g. In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.

Note Setting the JRE as the default for these browsers might cause problems with these browsers.

h. Click **Next**.

i. Click **Finish**.

Note If you are uninstalling the JRE, click **Remove**.

Step 12 In the Cisco Transport Controller Installation Wizard, click **Next**. The online user manuals are installed.

Step 13 Click **Finish**.

Step 14 Return to your originating procedure (NTP).

DLP-F178 Run the CTC Installation Wizard for UNIX

Purpose	This task installs the CTC online user manuals, Acrobat Reader 6.0.1, JRE 5.0, and the CTC JAR files. JRE 5.0 is required to run Software R8.0. Preinstalling the CTC JAR files saves time at initial login. If the JAR files are not installed, they are downloaded from the TSC card the first time you log in.
Tools/Equipment	ONS 15600 SDH Release 8.0 software CD
Prerequisite Procedures	None
Required/As Needed	Required if any of the following are true: • JRE 5.0 is not installed. • CTC online help is not installed and is needed. • JRE files are not installed and are needed.
Onsite/Remote	Onsite or remote
Security Level	None

Note If you will log into nodes running CTC software earlier than Release 4.6, uninstall JRE 5.0 and reinstall JRE 1.3.1_2. To run Software R8.0 and later, uninstall JRE 1.3.1_2 and reinstall JRE 5.0. Software R8.0 requires JRE 5.0.

Note JRE 1.4.2 requires Netscape 7.x or Internet Explorer 6.x.

Step 1 Verify that your computer has the following:

- RAM—384 MB recommended, 512 MB optimum
- Hard drive—20 GB hard drive recommended with at least 50 MB of space available
- Operating System—Solaris 9 or 10

Note These requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM. Refer to the *Cisco ONS 15600 SDH Reference Manual* for computer requirements needed for small, medium, and large ONS 15600 SDH networks.

Step 2 Change the directory. Type:

```
cd /cdrom/cdrom0/
```

Step 3 From the techdoc600 SDH CD directory, type:

```
./setup.bat
```

The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer:

- Java Runtime Environment 1.4.2
- Acrobat Reader 6.0.1
- Online User Manuals
- JRE JAR files

Step 4 Click **Next**.

Step 5 Complete one of the following:

- Click **Typical** to install both the Java Runtime Environment and online user manuals. If you already have JRE 5.0 installed on your computer, choose **Custom**.
- Click **Custom** if you want to install either the JRE or the online user manuals.

Step 6 Click **Next**.

Step 7 Complete the following, as applicable:

- If you selected Typical in Step 5, continue with Step 8.
- If you selected Custom, check the CTC component that you want to install and click **Next**.
  - If you selected Online User Manuals, continue with Step 8.
  - If you did not select Online User Manuals, continue with Step 10.

Step 8 The directory where the installation wizard will install CTC online user manuals appears. The default is /usr/doc/ctc.

- If you want to change the CTC online help directory, type the new directory path in the Directory Name field, or click **Browse** to navigate to the directory.
- If you do not want to change the CTC online help directory, skip this step.

Step 9 Click **Next**.

Step 10 Review the components that will be installed. If you want to change the components, complete one of the following:

- If you selected Typical in Step 5, click **Back** twice to return to the installation setup type page. Choose **Custom** and repeat Steps 6 through 9.
- If you selected Custom in Step 5, click **Back** once or twice (depending on the components selected) you reach the component selection page and check the desired components. Repeat Steps 7 through 9.

Step 11 Click **Next**. It might take a few minutes for the JRE installation wizard to appear. If you selected Custom in Step 5 and need to install a JRE, continue with Step 13.

Step 12 To install the JRE, complete the following:

a. In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and choose one of the following:

  - **I accept the terms of the license agreement**—Accepts the license agreement. Continue with Step b.
  - **I do not accept the terms of the license agreement**—Disables the Next button on the Java 2 Runtime Environment License Agreement dialog box. Click **Cancel** to return to the CTC installation wizard. CTC will not install the JRE. Continue with Step 13.

Note If JRE 5.0 is already installed on your computer, the License Agreement page does not appear. You must click Next and then choose Modify to change the JRE installation or Remove to uninstall the JRE. If you choose Modify and click Next, continue with Step e. If you choose Remove and click Next, continue with Step i.

b. Click **Next**.

c. Choose one of the following:

- Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
- Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.

d. Click **Next**.

e. If you selected Typical, continue with Step i. If you selected Custom, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:

- Java 2 Runtime Environment—(Default) Installs JRE 5.0 with support for European languages.
- Support for Additional Languages—Adds support for non-European languages.
- Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

The drop-down list options for each program feature include:

- This feature will be installed on the local hard drive—Installs the selected feature.
- This feature and all subfeatures will be installed on the local hard drive—Installs the selected feature and all subfeatures.
- Don’t install this feature now—Does not install the feature (not an option for Java 2 Runtime Environment).

To modify the directory where the JRE version is installed, click **Change**, navigate to the desired directory, and click **OK**.

f. Click **Next**.

g. In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.

Note Setting the JRE version as the default for these browsers might cause problems with these browsers.

h. Click **Next**.

i. Click **Finish**.

Note If you are uninstalling the JRE, click **Remove**.

Step 13 In the Cisco Transport Controller Installation Wizard, click **Next**. The Online Help installs.

Step 14 Click **Finish**.

Note Be sure to record the names of the directories you choose for JRE and the online help.

Step 15 Return to your originating procedure (NTP).

DLP-F179 Set Up a Windows PC for Craft Connection to an ONS 15600 SDH on the Same Subnet Using Static IP Addresses

Purpose	This task sets up your computer for a local craft connection to the ONS 15600 SDH when: • You will connect to one ONS 15600 SDH; if you will connect to multiple ONS 15600 SDHs, you might need to reconfigure your computer's IP settings each time you connect to an ONS 15600 SDH. • You need to use non-ONS 15600 SDH applications such as ping and tracert (trace route).
Tools/Equipment	None
Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify the operating system that is installed on your computer:

a. From the Windows Start menu, choose **Settings > Control Panel**.

b. In the Control Panel window, double-click the **System** icon.

c. On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows 2000, Windows NT 4.0, or Windows XP.

Step 2 According to the Windows operating system installed on your computer, perform one of the following steps:

- For Windows 98, complete Step 3.
- For Windows NT 4.0, complete Step 4.
- For Windows 2000, complete Step 5.
- For Windows XP, complete Step 6.

Step 3 If you have Windows 98 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings** > **Control Panel**.

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, choose **TCP/IP** for your network interface card (NIC), then click **Properties**.

d. In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.

e. Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.

f. Click the **IP Address** tab.

g. In the IP Address window, click **Specify an IP address**.

h. In the IP Address field, enter an IP address that is identical to the ONS 15600 SDH IP address except for the last octet. The last octet must be 1 or 3 through 254.

i. In the Subnet Mask field, type the same subnet mask as the ONS 15600 SDH. The default is 255.255.255.0 (24 bit).

j. Click **OK**.

k. In the TCP/IP dialog box, click the **Gateway** tab.

l. In the New Gateway field, type the ONS 15600 SDH IP address. Click **Add**.

m. Verify that the IP address appears in the Installed Gateways field, then click **OK**.

n. When the prompt to restart your PC appears, click **Yes**.

Step 4 If you have Windows NT 4.0 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings** > **Control Panel**.

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, click the **Protocols** tab, choose **TCP/IP Protocol**, then click **Properties**.

d. Click the **IP Address** tab.

e. In the IP Address window, click **Specify an IP address**.

f. In the IP Address field, enter an IP address that is identical the ONS 15600 SDH IP address except for the last octet. The last octet must be 1 or 3 through 254.

g. In the Subnet Mask field, type **255.255.255.0**.

h. Click **Advanced**.

i. In the Gateways List, click **Add**. The TCP/IP Gateway Address dialog box appears.

j. Type the ONS 15600 SDH IP address in the Gateway Address field.

k. Click **Add**.

l. Click **OK**.

m. Click **Apply**.

n. In some cases, Windows NT 4.0 prompts you to reboot your PC. If you receive this prompt, click **Yes**.

Step 5 If you have Windows 2000 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings** > **Network and Dial-up Connections > Local Area Connection**.

b. In the Local Area Connection Status dialog box, click **Properties**.

c. On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. Click **Use the following IP address**.

e. In the IP Address field, enter an IP address that is identical the ONS 15600 SDH IP address except for the last octet. The last octet must be 1 or 3 through 254.

f. In the Subnet Mask field, type **255.255.255.0**.

g. In the Default Gateway field, type the ONS 15600 SDH IP address.

h. Click **OK**.

i. In the Local Area Connection Properties dialog box, click **OK**.

j. In the Local Area Connection Status dialog box, click **Close**.

Step 6 If you have Windows XP installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Control Panel > Network Connections**.

Note If the Network Connections menu is not available, click **Switch to Classic View**.

b. From the Network Connections dialog box, click the **Local Area Connection** icon.

c. From the Local Area Connection Properties dialog box, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. In the IP Address field, enter an IP address that is identical the ONS 15600 SDH IP address except for the last octet. The last octet must be 1 or 3 through 254.

e. In the Subnet Mask field, type **255.255.255.0**.

f. In the Default Gateway field, type the ONS 15600 SDH IP address.

g. Click **OK**.

h. In the Local Area Connection Properties dialog box, click **OK**.

i. In the Local Area Connection Status dialog box, click **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-F180 Set Up a Solaris Workstation for a Craft Connection to an ONS 15600 SDH

Purpose	This task sets up a Solaris workstation for a craft connection to the ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Log into the workstation as the root user.

Step 2 Check to see if the interface is plumbed by typing:

```
# ifconfig device
```

For example:

```
# ifconfig hme1
```

If the interface is plumbed, a message similar to the following appears:

```
hme1:flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 2 inet 0.0.0.0 netmask
0
```

If a message similar to this one appears, go to Step 5.

If the interface is not plumbed, a message similar to the following appears:

```
if config: status: SIOCGLIFFLAGS: hme1: no such interface.
```

If a message similar to this one appears, go to Step 3.

Step 3 Plumb the interface by typing:

```
# ifconfig device plumb
```

For example:

```
# ifconfig hme1 plumb
```

Step 4 Configure the IP address on the interface by typing:

```
# ifconfig interface ip-address netmask netmask up
```

For example:

```
# ifconfig hme0 192.1.0.3 netmask 255.255.255.0 up
```

Note Enter an IP address that is identical to the ONS 15600 SDH IP address except for the last octet. The last octet must be between 1 and 254.

Step 5 In the Subnet Mask field, type **255.255.255.0**. Skip this step if you checked Enable Socks Proxy on Port and External Network Element (ENE) at Provisioning > Network > General > Gateway Settings.

Step 6 Test the connection:

a. Start Netscape Navigator.

b. Enter the Cisco ONS 15600 SDH IP address in the web address (URL) field. If the connection is established, a Java Console window, CTC caching messages, and the Cisco Transport Controller Login dialog box appear. If this occurs, go to Step 2 of the "DLP-F181 Log into CTC" task on page 16-34 to complete the login. If the Login dialog box does not appear, complete Steps c and d.

c. At the prompt, type:

```
ping ONS-15600-SDH-IP-address
```

For example, to connect to an ONS 15600 SDH with the default IP address 192.168.1.2, type:

```
ping 192.168.1.2
```

If your workstation is connected to the ONS 15600 SDH, the following message appears:

```
IP address is alive
```

Note Skip this step if you checked Enable Socks Proxy on Port and External Network Element (ENE) at Provisioning > Network > General > Gateway Settings.

d. If CTC is not responding, a "Request timed out" (Windows) or a "no answer from *x.x.x.x*" (UNIX) message appears. Verify the IP and subnet mask information. Check that the cables connecting the workstation to the ONS 15600 SDH are securely attached. Check the link status by typing:

```
# ndd -set /dev/device instance 0
# ndd -get /dev/device link_status
```

For example:

```
# ndd -set /dev/hme instance 0
# ndd -get /dev/hme link_status
```

A result of 1 means the link is up. A result of 0 means the link is down.

Note Check the man page for ndd. For example, type:

```
# man ndd
```

Step 7 Return to your originating procedure (NTP).

DLP-F181 Log into CTC

Purpose	This task logs into CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1 One of the following procedures: • NTP-F127 Set Up CTC Computer for Local Craft Connection to the ONS 15600 SDH, page 3-3 • NTP-F128 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15600 SDH, page 3-4
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note For information about CTC views and navigation, see Appendix A, “CTC Information and Shortcuts.”

Step 1 From the computer connected to the ONS 15600 SDH, start Mozilla Firefox (PC or UNIX) or Netscape (PC only):

- If you are using a PC, launch Netscape or Mozilla Firefox from the Windows Start menu or a shortcut icon.
- If you are using UNIX, launch Netscape from the command line by typing one of the following:
  - To install Netscape colors for Netscape use, type:

    ```
    netscape -install
    ```

  - To limit Netscape to 32 colors so that if the requested color is not available, Netscape chooses the closest color option, type:

    ```
    netscape -ncols 32
    ```

Note CTC requires a full 24-color palette to run properly. When using color-intensive applications such as Netscape in UNIX, it is possible that UNIX could run out of colors to use for CTC. The -install and -ncols 32 command line options limit the number of colors that Netscape uses.

Step 2 In the Netscape or Mozilla Firefox Web address (URL) field, enter the ONS 15600 SDH IP address. For initial setup, this is the default address: 192.168.1.2. Press **Enter**.

Note Netscape or Internet Explorer can be used for IPv4 address and Mozilla Firefox or Netscape can be used for IPv6 address.

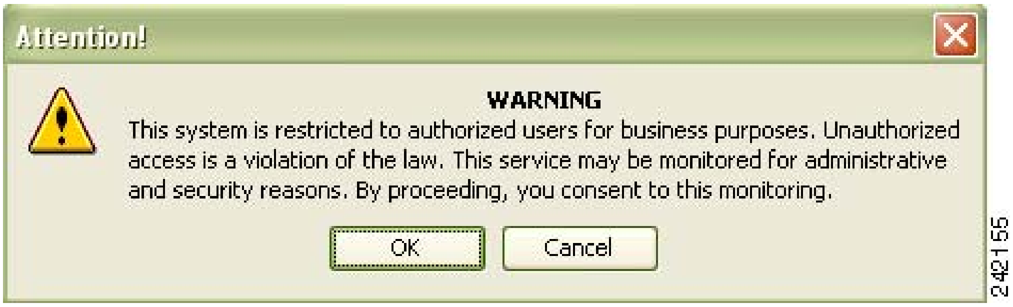
To log into CTC using an IPv6 address, you must first log into CTC using an IPv4 or IPv6 address and assign an IPv6 address to the node. Then, use the IPv6 address that you assigned to the node to log into CTC. For more information about configuring IPv6 address, see "DLP-F185 Provision IP Settings" section on page 16-38. Enter the IPv6 address in the address bar of the browser, enclosed in square brackets.

Note If you are logging into ONS 15600 SDH nodes running different releases of CTC software, log into the node running the most recent release. If you log into a node running an older release, you will receive an INCOMPATIBLE-SW alarm for each node in the network running a new release, and CTC will not be able to manage these nodes. To check the software version of a node, select About CTC from the CTC Help menu. To resolve an alarm, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Step 3 If a Java Plug-in Security Warning dialog box appears, complete the "DLP-F283 Install Public-Key Security Certificate" task on page 17-74 to install the public-key security certificate.

After you complete the security certificate dialog box (or if the certificate is already installed), a Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments. If this is the first [1], CTC caching messages appear while CTC files are downloaded to your computer. The first time you connect to an ONS 15600 SDH, this process can take several minutes. After the download, a warning message window appears (Figure 16-8).

Figure 16-8 Warning Message Window

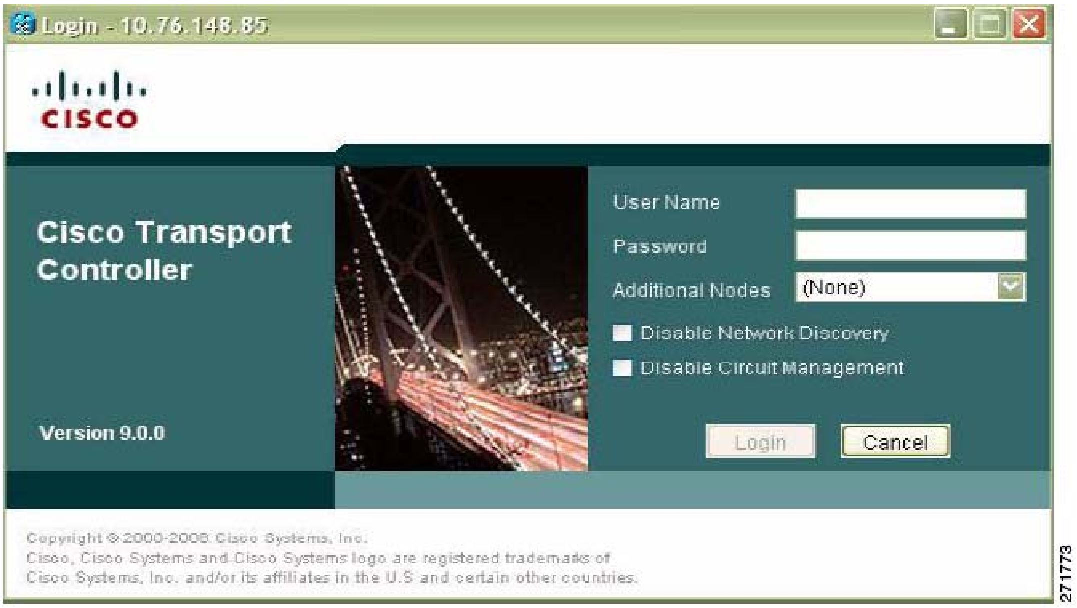


WARNING
This system is restricted to authorized users for business purposes. Unauthorized access is a violation of the law. This service may be monitored for administrative and security reasons. By proceeding, you consent to this monitoring.

Step 4 Click OK. The CTC Login dialog box appears (Figure 16-9).

[1]

Figure 16-9 Logging into CTC



Login - 10.76.148.85

Cisco Transport Controller

Version 9.0.0

User Name

Password

Additional Nodes (None)

□ Disable Network Discovery

□ Disable Circuit Management

Copyright © 2000-2008 Cisco Systems, Inc.
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S and certain other countries.

Step 5 In the Login dialog box, type a user name and password (both are case sensitive). For initial setup, type the user name **CISCO15** and password **otbu+1**.

Note The CISCO15 user is provided with every ONS 15600 SDH. CISCO15 has Superuser privileges, so you can create other users. You must create another Superuser before you can delete the CISCO15 user. CISCO15 is delivered with the otbu+1 password. To change the password for CISCO15, click the **Provisioning** > **Security** tabs after you log in and change the password. To set up ONS 15600 SDH users and assign security, go to the "NTP-F132 Create Users and Assign Security" procedure on page 4-3. For additional information, refer to the *Cisco ONS 15600 SDH Reference Manual*.

Step 6 Each time you log into an ONS 15600 SDH, you can select the following login options:

- Additional Nodes—Displays a list of login node groups. To create a login node group or add additional groups, see the "DLP-F307 Create Login Node Groups" task on page 18-9.
- Disable Network Discovery—Check this box to view only the ONS 15600 SDH (and login node group members, if any) entered in the Node Name field. Nodes linked to this node through the DCC are not discovered and will not appear in CTC network view. Using this option can decrease the CTC startup time in networks with many DCC-connected nodes and reduces memory consumption.

  If you keep Disable Network Discovery unchecked, CTC attempts to upgrade the CTC software by downloading more recent versions of the JAR files it finds during the network discovery. Click **Yes** to allow CTC to download the newer JAR files, or **No** to prevent CTC from downloading the JAR files.
- Disable Circuit Management—Check this box to disable discovery of existing circuits. Using this option can decrease the CTC initialization time in networks with many existing circuits and reduce memory consumption. This option does not prevent the creation and management of new circuits.

Step 7 Click **Login**.

If login is successful, the CTC window appears. From here, you can navigate to other CTC views to provision and manage the ONS 15600 SDH. If you need to turn up a shelf for the first time, go to Chapter 4, "Turn Up a Node." If login problems occur, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Step 8 Return to your originating procedure (NTP).

DLP-F183 Add a Node to the Current Session or Login Group

Purpose	This task adds a node to the current CTC session or login node group.
Tools	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the CTC File menu, choose **Add Node**.

Step 2 In the Add Node dialog box, enter the node name (or IP address).

Step 3 If you want to add the node to the current login group, check **Add Node to Current Login Group**. Otherwise, leave it unchecked.

Note The Add Node to Current Login Group check box is active only if you selected a login group when you logged into CTC.

Step 4 Click **OK**.

After a few seconds, the new node will appear on the network view map.

Step 5 Return to your originating procedure (NTP).

DLP-F184 Change the Login Legal Disclaimer

Purpose	This task modifies the legal disclaimer statement shown in the CTC login dialog box so that it will display customer-specific information when users log into the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > Security > Legal Disclaimer > HTML** tabs.

Step 2 The existing statement is a default, non-customer-specific disclaimer. If you want to edit this statement with specifics for your company, you can change the text. You can also use the HTML commands in Table 16-3 to format the text.

Table 16-3 HTML Commands Used to Format the Legal Disclaimer

Code	Description
<b>	Begins boldface font
</b>	Ends boldface font
<center>	Aligns type in the center of the window
</center>	Ends the center alignment
<font=*n*> (where *n* = point size)	Changes the font to the new size
</font>	Ends the font size command
<p>	Creates a line break
<sub>	Begins subscript
</sub>	Ends subscript
<sup>	Begins superscript
</sup>	Ends superscript
<u>	Starts underline
</u>	Ends underline

Step 3 If you want to preview your changed statement and formatting, click the **Preview** subtab.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-F185 Provision IP Settings

Purpose	This task provisions IP settings, which include the IP address, IP address version,, default router, Dynamic Host Configuration Protocol (DHCP) access, firewall access, and SOCKS proxy server settings for an ONS 15600 SDH node.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution All network changes should be approved by your network or LAN administrator.

Caution Verify that any IPv4 or IPv6 addresses assigned to the node are unique in the network. Duplicate IP addresses in the same network cause loss of visibility.

Step 1 From the View menu, choose **Go To Home View**.

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

Step 3 Complete the following information in the fields listed:

- Node Address—Type the IP address assigned to the ONS 15600 SDH node.
- Default Router— If the ONS 15600 SDH is connected to a LAN, enter the IP address of the default router. The default router forwards packets to network devices that the ONS 15600 SDH cannot directly access. This field is ignored if any of the following are true:
  - The ONS 15600 SDH is not connected to a LAN.
  - SOCKS proxy server is enabled and the ONS 15600 SDH is provisioned as an end network element (ENE).
  - Open Shortcut Path First (OSPF) is enabled on both the ONS 15600 SDH and the LAN where the ONS 15600 SDH is connected.
- Suppress CTC IP Display—Check this check box if you want to prevent the node IPv4 address and IPv6 address (if enabled) from being displayed in CTC (IP Address field, information area) to users with Provisioning, Maintenance, or Retrieve security levels. If the IP address is not suppressed, both the IPv4 address and IPv6 addresses are shown in the IP Address field.
- IPv6 Configuration—Allows provisioning of IPv6 addresses. After you provision an IPv6 address, you can access the device using the IPv6 address. Configure these settings only if you want to enable IPv6 on the node. IPv6 cannot be configured using the LCD push buttons.
  - Enable IPv6—Select this check box to assign an IPv6 address to the node. The IPv6 Address, Prefix Length, and IPv6 Default Router fields are enabled only if this check box is selected. The check box is disabled by default.

Note If TCC2P cards are installed, dual IPv4 addressing through secure mode is available for IPv4 only. If IPv6 is enabled on ONS 15600 with TCC2P in secure mode, IPv6 address support applies to the backplane LAN port only. There is no IPv6 address for the front TCC2P TCP/IP (LAN) port. However, when the TCC2P card is in normal mode (repeater mode), the IPv6 address support applies to both the backplane LAN port as well as the TCC2P TCP/IP (LAN) port.

Note IPv6 address can be enabled only when 'Enable SOCKS Proxy on Port' checkbox is enabled. For IPv6 connectivity, once the SOCKS Proxy is enabled, the ONS 15600 node can be configured as'External Network Element(ENE)' or 'Gateway Network Element(GNE)' or 'SOCKS proxy only' by enabling the suitable radio button.

Note By default, when IPv6 is enabled, the node processes both IPv4 and IPv6 packets on the LAN interface. If you want the node to process only IPv6 packets, you need to disable IPv4 on the node. For more information, see DLP-F332 Change Node Access and PM Clearing Privilege, page 18-31

  - IPv6 Address—Enter the IPv6 address that you want to assign to the node. This IP address is the global unicast IPv6 address. This field is disabled if the Enable IPv6 check box is not selected.
  - Prefix Length—Enter the prefix length of the IPv6 address. This field is disabled if the Enable IPv6 check box is not selected. The valid range for Prefix Length is 0 - 128.
  - IPv6 Default Router—Enter the IPv6 address of the default router of the IPv6 NE. This field is disabled if the Enable IPv6 check box is not selected. This field can be set to 0 or 0::0 or 0:0:0:0:0:0:0:0 if any of the following are true:

    The ONS 15600 is not connected to a LAN.

    The ONS 15600 is provisioned as an end network element (ENE).

Note ONS platforms use NAT-PT internally to support native IPv6. NAT-PT uses the IPv4 address range 128.x.x.x for packet translation. Do not use this address range when you enable IPv6 feature.

Note You can provision IPv6 in secure or nonsecure mode. To enable secure mode, see "NTP-F248 Set Up the ONS 15600 in EMS Secure Access" section on page 4-7.

- Forward DHCP Request To—Check this check box to enable DHCP. Also, enter the DHCP server IP address in the Request To field. Unchecked is the default. If you will enable any of the gateway settings to implement the ONS 15600 SDH SOCKS proxy server features, leave this field blank.

  Note If you enable DHCP, computers connected to an ONS 15600 SDH node can obtain temporary IP addresses from an external DHCP server. The ONS 15600 SDH only forwards DHCP requests; it does not act as a DHCP server.

- MAC Address—(Read only) Displays the ONS 15600 SDH IEEE 802 MAC address.
- Net/Subnet Mask Length—If the ONS 15600 SDH is part of a subnet, type the subnet mask length (decimal number representing the subnet mask length in bits) or click the arrows to adjust the subnet mask length. The subnet mask length is the same for all ONS 15600 SDHs in the same subnet.
- Gateway Settings—Provisions the ONS 15600 SDH SOCKS proxy server features. (SOCKS is a standard proxy protocol for IP-based applications.) Do not change these options until you review the SOCKS proxy server scenario in the *Cisco ONS 15600 SDH Reference Manual*. In SOCKS proxy server networks, the ONS 15600 SDH is either an ENE, gateway network element (GNE), or proxy-only server. Provisioning must be consistent for each NE type.
- Enable SOCKS proxy server on port—If checked, the ONS 15600 SDH serves as a proxy for connections between CTC clients and ONS 15600 SDHs that are connected by DCCs to the proxy ONS 15600 SDH. The CTC client establishes connections to DCC-connected nodes through the proxy node. The CTC client does not require IP connectivity to the DCC-connected nodes, only to the proxy ONS 15600 SDH. If Enable SOCKS proxy server on port is off, the node does not proxy for any CTC clients. When this box is checked, you can provision one of the following options:

  Note For the ONS 15600 SDH, the ENE and GNE settings have the same behavior.

- External Network Element (ENE) or Gateway Network Element (GNE)—Choose either of these options when the ONS 15600 SDH is not connected to a LAN but has DCC connections to other ONS nodes. A CTC computer connected to the ENE/GNE through the TSC TCP/IP (craft) port can manage nodes that have DCC connections to the ENE/GNE. However, the CTC computer does not have direct IP connectivity to these nodes or to any LAN/WAN that those nodes might be connected to.
- SOCKS Proxy-Only—Choose this option when the ONS 15600 SDH is connected to a LAN and the LAN is separated from the node by a firewall. The SOCKS Proxy Only is the same as the ENE/GNE option, except the SOCKS Proxy Only option does not isolate the DCC network from the LAN.

Step 4 Click **Apply**.

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

Both ONS 15600 SDH TSC cards will reboot, one at a time. Next, a “Lost node connection, switching to network view” message appears. The reset causes the standby TSC to become the active TSC.

Step 6 If the cable was connected to the RJ-45 port on the active TSC (now the standby TSC), disconnect the cable and connect it to the RJ-45 port on the other TSC (now the active TSC).

Step 7 Click **OK**. The network view appears with the node icon in gray, during which time you cannot access the node.

Step 8 Double-click the node icon when it becomes green.

Step 9 Return to your originating procedure (NTP).

DLP-F186 Create a Static Route

Purpose	This task creates a static route to establish CTC connectivity to a computer on another network.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	Required if either of the following conditions is true: • You need to connect ONS 15600 SDHs to CTC sessions on one subnet connected by a router to ONS 15600 SDHs residing on another subnet when OSPF is not enabled and the ENE or GNE setting is not checked. • You need to enable multiple CTC sessions among ONS 15600 SDHs residing on the same subnet, and the Craft Access server feature is not enabled.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network > Static Routing** tabs.

Step 2 Click **Create**.

Step 3 In the Create Static Route dialog box, enter the following:

- Destination—Enter the IP address of the computer running CTC. To limit access to one computer, enter the full IP address and a subnet mask of 255.255.255.255. To allow access to all computers on the 192.168.1.0 subnet, enter 192.168.1.0 and a subnet mask of 255.255.255.0. You can enter a destination of 0.0.0.0 to allow access to all CTC computers that connect to the router.
- Mask—Enter a subnet mask. If Destination is a host route (that is, one CTC computer), enter a 32-bit subnet mask (255.255.255.255). If Destination is a subnet, adjust the subnet mask accordingly, for example, 255.255.255.0. If Destination is 0.0.0.0, CTC automatically enters a subnet mask of 0.0.0.0 to provide access to all CTC computers. You cannot change this value.
- Next Hop—Enter the IP address of the router port or the node IP address if the CTC computer is connected to the node directly.
- Cost—Enter the number of hops between the ONS 15600 SDH and the computer.

Step 4 Click **OK**. Verify that the static route appears in the Static Route window.

Note Static route networking scenarios are provided in the “Management Network Connectivity” chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Step 5 Return to your originating procedure (NTP).

DLP-F187 Set Up or Change Open Shortest Path First Protocol

Purpose	This task enables the OSPF routing protocol to include the ONS 15600 SDH in OSPF-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 You will need to know the OSPF Area ID, Hello and Dead intervals, and authentication key (if OSPF authentication is enabled) provisioned on the router to which the ONS 15600 SDH is connected.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If the ONS 15600 SDH has DCC or LAN interfaces in multiple OSPF areas, at least one ONS 15600 SDH DCC or LAN interface must be in the backbone area 0.0.0.0.

Note CTC will not allow both a DCC interface and a LAN interface in the same non-zero OSPF area.

Note To create OSPF virtual links, OSPF must be enabled on the LAN.

Step 1 In node view, click the **Provisioning > Network > OSPF** tabs.

Step 2 In the top left side of the OSPF pane, complete the following:

- DCC/GCC OSPF Area ID Table—In dotted decimal format, enter the number that identifies the ONS 15600 SDHs as a unique OSPF area ID. The Area ID can be any number between 000.000.000.000 and 255.255.255.255, but must be unique to the LAN OSPF area.
- RS-DCC Metric—This value is normally unchanged. It sets a “cost” for sending packets across the regenerator-section DCC (RS-DCC), which is used by OSPF routers to calculate the shortest path. This value should always be higher than the LAN metric. The default RS-DCC metric is 100.
- MS-DCC Metric—Sets a cost for sending packets across the MS-DCC. This value should always be lower than the RS-DCC metric. The default MS-DCC metric is 33. It is usually not changed.

Step 3 In the OSPF on LAN area, complete the following:

- OSPF active on LAN—When checked, enables ONS 15600 SDH OSPF topology to be advertised to OSPF routers on the LAN. Enable this field on ONS 15600 SDHs that directly connect to OSPF routers.
- LAN Port Area ID —Enter the OSPF area ID (dotted decimal format) for the router port where the ONS 15600 SDH is connected. (This number is different from the DCC/GCC OSPF Area ID.)

Step 4 By default, OSPF is set to No Authentication. If the OSPF router requires authentication, complete the following steps. If not, continue with Step 5.

a. Click the **No Authentication** button.

b. In the Edit Authentication Key dialog box, complete the following:

   - Type—Choose **Simple Password**.
   - Enter Authentication Key—Enter the password.
   - Confirm Authentication Key—Enter the same password to confirm it.

c. Click **OK**.

The authentication button label changes to Simple Password.

Step 5 Provision the OSPF priority and interval settings.

The OSPF priority and intervals default to values most commonly used by OSPF routers. In the Priority and Intervals area, verify that these values match those used by the OSPF router where the ONS 15600 SDH is connected:

- Router Priority—Selects the designated router for a subnet.
- Hello Interval (sec)—Sets the number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
- Dead Interval—Sets the number of seconds that will pass while an OSPF router’s packets are not visible before its neighbors declare the router down. Forty seconds is the default.
- Transit Delay (sec)—Indicates the service speed. One second is the default.
- Retransmit Interval (sec)—Sets the time that will elapse before a packet is resent. Five seconds is the default.
- LAN Metric—Sets a cost for sending packets across the LAN. This value should always be lower than the DCC metric. Ten is the default.

Step 6 Under OSPF Area Range Table, create an area range table if one is needed.

Note Area range tables consolidate the information that is propagated outside an OSPF Area border. One ONS 15600 SDH in the ONS 15600 SDH OSPF area is connected to the OSPF router. An area range table on this node points the router to the other nodes that reside within the ONS 15600 SDH OSPF area.

a. Under OSPF Area Range Table, click **Create**.

b. In the Create Area Range dialog box, enter the following:

- Range Address—Enter the area IP address for the ONS 15600 SDHs that reside within the OSPF area. For example, if the ONS 15600 SDH OSPF area includes nodes with IP addresses 10.10.20.100, 10.10.30.150, 10.10.40.200, and 10.10.50.250, the range address would be 10.10.0.0.
- Range Area ID—Enter the OSPF area ID for the ONS 15600 SDHs. This is either the ID in the DCC OSPF Area ID field or the ID in the Area ID for LAN Port field.
- Mask Length—Enter the subnet mask length. In the Range Address example, this is 16.
- Advertise—Check this box if you want to advertise the OSPF range table.

c. Click **OK**.

Step 7 All OSPF areas must be connected to Area 0. If the ONS 15600 SDH OSPF area is not physically connected to Area 0, use the following steps to create a virtual link table that will provide the disconnected area with a logical path to Area 0:

a. Under OSPF Virtual Link Table, click **Create**.

b. In the Create Virtual Link dialog box, complete the following fields (OSPF settings must match OSPF settings for the ONS 15600 SDH OSPF area):

- Neighbor—The router ID of the Area 0 router.
- Transit Delay (sec)—The service speed. One second is the default.
- Hello Int (sec)—The number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
- Auth Type—If the router where the ONS 15600 SDH is connected uses authentication, choose **Simple Password**. Otherwise, choose **No Authentication**.
- Retransmit Int (sec)—Sets the time that will elapse before a packet is resent. Five seconds is the default.
- Dead Int (sec)—Sets the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.

c. Click **OK**.

Step 8 After entering ONS 15600 SDH OSPF area data, click **Apply**.

If you changed the Area ID, the TSC cards will reset, one at a time. The reset will take approximately 10 to 15 minutes.

Step 9 Return to your originating procedure (NTP).

DLP-F188 Set Up External or Line Timing

Purpose	This task defines the SDH timing source for the ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2 DLP-F181 Log into CTC, page 16-34
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If you do not perform this procedure, the ONS 15600 SDH defaults to its internal Stratum 3E clock.

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 In the General Timing area, complete the following information:

- Timing Mode—Choose **External** if the ONS 15600 SDH derives its timing from a BITS source wired to the backplane pins; choose **Line** if timing is derived from an STM-N card that is optically connected to the timing node. A third option, Mixed, allows you to set external and line timing references. (Because Mixed timing might cause timing loops, Cisco does not recommend its use. Use this mode with care.)
- Revertive—If this check box is selected, the ONS 15600 SDH reverts to a primary reference source after the conditions that caused it to switch to a secondary timing reference are corrected.
- Reversion Time—If Revertive is checked, indicate the amount of time the ONS 15600 SDH will wait before reverting to its primary timing source.

Step 3 In the Reference Lists area, complete the following information:

- NE Reference—Allows you to define three timing references (Ref-1, Ref-2, and Ref-3). The node uses Reference 1 unless a failure occurs to that reference, in which case, the node uses Reference 2. If that fails, the node uses Reference 3, which is typically set to Internal Clock. This is the Stratum 3E clock provided on the TSC. The options shown depend on the Timing Mode setting.
  - Timing Mode is set to External—Your options are BITS1, BITS2, and Internal Clock.
  - Timing Mode is set to Line—Your options are the node's STM-N ports (except for ports that have been specified as protection ports in 1+1 protection groups) and Internal Clock. Choose the cards/ports that are directly or indirectly connected to the node wired to the BITS source, that is, the node's trunk cards. Set Reference 1 to the trunk card that is closest to the BITS source. For example, if Slot 3/Port 16 is connected to the node wired to the BITS source, choose Slot 3 as Reference 1.
  - Timing Mode is set to Mixed—Both BITS and STM-N cards are available, allowing you to set a mixture of external BITS and STM-N trunk cards as timing references.
- BITS-1 Out/BITS-2 Out—Sets the timing references for equipment wired to the BITS Out backplane pins. BITS-1 Out and BITS-2 Out are enabled when BITS-1 and BITS-2 facilities are put in service. If Timing Mode is set to external, choose the STM-N card used to set the timing. If Timing Mode is set to Line, you can choose an STM-N card or choose NE Reference to have the BITS-1 Out and/or BITS-2 Out follow the same timing references as the NE.

Step 4 Click **Apply**.

Step 5 Click the **BITS Facilities** tab, and complete the following information:

Note The BITS Facilities section sets the parameters for your BITS-1 and BITS-2 timing references. Many of these settings are determined by the timing source manufacturer. If equipment is timed through BITS Out, you can set timing parameters to meet the requirements of the equipment.

Step 6 In the BITS In area, complete the following information:

- Facility Type—Choose **E1, 2 MHz, 64KHz+8KHz, or DS1** depending on the signal supported in your market. E1, 2 MHz, 64KHz+8KHz, and DS1 are physical signal modes used to transmit the external clock (from a global positioning satellite [GPS], for example) to BITS.
- BITS In State—If Timing Mode is set to External or Mixed, set the BITS In State for BITS-1 and/or BITS-2 to **unlocked** depending whether one or both BITS input pin pairs on the backplane are connected to the external timing source. If Timing Mode is set to Line, set the BITS In State to **locked**.

Step 7 If the BITS In State for BITS-1 and BITS-2 is set to **locked**, continue with Step 8. If the BITS In State is set to **unlocked** for either BITS-1 or BITS-2, complete the following information:

- Coding—Choose the coding used by your BITS reference, either **HDB3** or **AMI** (alternate mark inversion). HDB3 coding is only for the E1 facility type. If you selected 2 MHz, the coding option is disabled.
- Framing—Choose the framing used by your BITS reference, either **unframed**, **FAS**, **FAS + CAS**, **FAS + CRC**, or **FAS + CAS + CRC** . FAS + CAS + CRC is only for the E1 facility type. If you selected 2 MHz or 64KHz+8KHz, the framing option is disabled.
- Sync Messaging—Select the check box to enable synchronization status messages (SSMs). SSM is used to deliver clock quality. The SSMs supported in SDH are G811, STU, G812T, G812L, SETS, and DUS (ordered from high quality to low quality).
- Admin SSM—If the Sync Messaging check box is not checked, you can choose the SSM from the drop-down list: G811, STU, G812T, G812L, SETS, or DUS (ordered from high quality to low quality. If you selected DS1, the Admin SSM option is disabled.
- Sa bit—Choose one of 5 Sa bits (**Sa4**, **Sa5**, **Sa6**, **Sa7**, or **Sa8**). The Sa bit setting is only for the E1 facility type. The Sa bit transmits the SSM message. If you selected 2 MHz, the Sa bit option is disabled.
- Cable Type—Choose **75 ohm** or **120 ohm**. The cable type is fixed at 100 ohm for DS1.

Step 8 In the BITS Out area, complete the following information, as needed:

- Facility Type—Choose **E1, 2 MHz, 64KHz+8KHz, or DS1** depending on the signal supported in your market.
- BITS Out State—If equipment is connected to the node's BITS output pins on the backplane and you want to time the equipment from a node reference, set the BITS Out State for BITS-1 and/or BITS-2 to **unlocked**, depending on which BITS Out pins are used for the external equipment. If equipment is not attached to the BITS output pins, set the BITS Out State to **locked**.

Step 9 If the BITS Out State is set to **locked**, continue with Step 10. If BITS Out State is set to **unlocked**, complete the following information:

- Coding—Choose the coding used by your BITS reference, either **HDB3** or **AMI**. If you selected 2 MHz, the coding option is disabled.
- Framing—Choose the framing used by your BITS reference. If the facility type is set to DS1, the options are either **ESF** or **SF (D4)**. If the facility type is set to E1, the options are **Unframed, FAS, FAS+CAS, FAS+CRC,** or **FAS+CAS+CRC**. If you selected 2 MHz or 64KHz+8KHz, the framing option is disabled.

- AIS Threshold—Sets the quality level at which a node sends an alarm indication signal (AIS) from the BITS-1 Out and BITS-2 Out connectors. When a node times at or below the AIS threshold quality, an AIS is raised. (The AIS threshold is used when SSM is disabled or framing is set to unframed, FAS, or FAS + CAS.)
- Sa bit—Choose one of 5 Sa bits (**Sa4**, **Sa5**, **Sa6**, **Sa7**, or **Sa8**). The Sa bit transmits the SSM message. If you selected 2 MHz, the Sa bit option is disabled.
- Cable Type—Choose **75 ohm** or **120 ohm**.

Step 10 Click **Apply**.

Note Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* to resolve timing-related alarms.

Step 11 Return to your originating procedure (NTP).

DLP-F189 Set Up Internal Timing

Purpose	This task sets up internal timing (Stratum 3E) for an ONS 15600 SDH or sets up other nodes in the network to be line timed off of the node's internal clock.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	Not recommended; use only if no BITS source or line timing sources are available
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Internal timing is synchronous equipment (SETS) timing, and is not intended for permanent use. All ONS 15600 SDH nodes should be timed to a SETS or better primary reference source.

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 In the General Timing area, enter the following:

- Timing Mode—Choose **External**.
- Revertive—Not applicable for internal timing; the default setting (checked) is sufficient.
- Reversion Time—Not applicable; leave unchanged. For internal timing, the default setting (5 minutes) is sufficient.

Step 3 In the Reference Lists section, enter the following information:

- NE Reference
  - Ref1—Set to **Internal Clock**.
  - Ref2—Set to **Internal Clock**.
  - Ref3—Set to **Internal Clock**.
- BITS-1 Out/BITS-2 Out—Set to **None**.

Step 4 Click **Apply**.

Step 5 Click the **Provisioning > Timing** > **BITS Facilities** tabs.

Step 6 In the BITS Facilities area, enter the following information:

- Facility Type—Choose **E1, 2 MHz, 64KHz+8KHz, or DS1** depending on the signal supported in your market. E1, 2 MHz, 64KHz+8KHz, and DS1 are physical signal modes used to transmit the external clock (from a GPS, for example) to BITS.
- BITS In State—Set BITS-1 and BITS-2 to **locked**.
- BITS Out State—Set BITS-1 and BITS-2 to **locked**.
- Coding—Not relevant for internal timing; the default (HDB3) is sufficient.
- Framing—Not relevant for internal timing; the default is sufficient.
- Sync Messaging—The box is checked automatically. SSM is used to deliver clock quality. The SSMs supported in SDH are G811, STU, G812T, G812L, SETS, and DUS (ordered from high quality to low quality). If you selected 2 MHz, the SSM option is disabled.
- AIS Threshold—Not relevant for internal timing.
- Sa bit—Not applicable for internal timing.

Step 7 Click **Apply**.

Step 8 Log into a node that will be timed from the node set up in Steps 1 through 7 (the internally timed node).

Step 9 Click the **Provisioning > Timing > General** tabs.

Step 10 In the General Timing area, enter the same information as entered in Step 2, except set Timing Mode to **Line**.

Step 11 In the Reference Lists area, enter the same information as entered in Step 3, except set NE Reference as follows:

- Ref1—Set to the STM-N trunk card with the closest connection to the internally timed node.
- Ref2—Set to the STM-N trunk card with the next closest connection to the internally timed node.
- Ref3—Set to **Internal Clock**.
- BITS-1 Out/BITS-2 Out—Set to **None**.

Step 12 Click **Apply**.

Step 13 Repeat Steps 9 through 12 at each node that will be timed by the internally timed node.

Step 14 Return to your originating procedure (NTP).

DLP-F190 Create a New User on a Single Node

Purpose	This task creates a new user for one ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning** > **Security** > **Users** tabs.

Step 2 Click **Create**.

Step 3 In the Create User dialog box, enter the following:

- Name—Type the user name. The name must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters. For Transaction Language One (TL1) compatibility, the user name must be 6 to 10 characters, and the first character must be an alpha character.
- Password—Type the user password. The password length, by default, is set to a minimum of six and a maximum of 20. You can configure the default values in node view through Provisioning > NE Defaults > Node > security > passwordComplexity. The minimum length can be set to eight, ten or twelve characters, and the maximum length to 80 characters. The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters, where at least two characters are nonalphabetic and at least one character is a special character. For TL1 compatibility, the password must be 6 to 10 characters, and the first character must be an alpha character. The password must not contain the user name.
- Confirm Password—Type the password again to confirm it.
- Security Level—Choose a security level for the user: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. Refer to the *Cisco ONS 15600 SDH Reference Manual* for information about the capabilities provided with each level.

Note Idle time is the length of time that CTC can remain unused before it locks and requires that a user reenter the password. Each security level has a different idle time: Retrieve is unlimited, Maintenance is 60 minutes, Provisioning is 30 minutes, and Superuser is 15 minutes. To change the idle times, refer to the "NTP-F206 Modify Users and Change Security" procedure on page 11-6.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-F191 Create a New User on Multiple Nodes

Purpose	This task adds a new user to multiple ONS 15600 SDHs.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note All nodes where you want to add users must be accessible in network view.

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Provisioning** > **Security** > **Users** tabs.

Step 3 Click **Create**.

Step 4 In the Create User dialog box, enter the following:

- Name—Type the user name. The name must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters. For TL1 compatibility, the user name must have no more than 10 characters, and the first character must be an alpha character.
- Password—Type the user password. The password length, by default, is set to a minimum of six and a maximum of 20. You can configure the default values in node view through Provisioning > NE Defaults > Node > security > passwordComplexity. The minimum length can be set to eight, ten or twelve characters, and the maximum length to 80 characters. The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters, where at least two characters are non alphabetic and at least one character is a special character. For TL1 compatibility, the password must be six to ten characters, and the first character must be an alpha character. The password must not contain the user name.
- Confirm Password—Type the password again to confirm it.
- Security Level—Choose a security level for the user: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. Refer to the *Cisco ONS 15600 SDH Reference Manual* for information about the capabilities provided with each level.

Note Idle time is the length of time that CTC can remain unused before it locks and requires that a user reenter the password. Each security level has a different idle time: Retrieve is unlimited, Maintenance is 60 minutes, Provisioning is 30 minutes, and Superuser is 15 minutes. To change the idle times, refer to the "NTP-F206 Modify Users and Change Security" procedure on page 11-6.

Step 5 In the Select applicable nodes area, uncheck any nodes where you do not want to add the user (all network nodes are checked by default).

Step 6 Click **OK**.

Step 7 In the User Creation Results dialog box, click **OK**.

Step 8 Return to your originating procedure (NTP).

DLP-F192 Optical 1+1 Manual Protection Switch Test

Purpose	This task verifies that a 1+1 protection group will switch properly.
Tools/Equipment	Optical test set and cables
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34; a test circuit as part of the topology acceptance test
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 for instructions.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Step 3 Click the **Conditions** tab. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Step 4 Double-click the node containing the 1+1 protection group you are testing. The node view appears.

Step 5 Click the **Maintenance > Protection** tabs.

Step 6 In the Protection Groups area, click the 1+1 protection group.

Step 7 Click the working port. Next to Switch Commands, click **Force**.

Step 8 In the Confirm Manual Operation dialog box, click **Yes**.

Step 9 In the Selected Group area, verify that the following appears:

```
Protect port - Protect/Active [FORCE_SWITCH_TO_PROTECT], [PORT STATE]
Working port - Working/Standby [FORCE_SWITCH_TO_PROTECT], [PORT STATE]
```

Step 10 Verify that the traffic on the test set connected to the node is still running. Some bit errors are normal. The traffic flow can be interrupted for less than 50 ms. If a traffic interruption of more than 50 ms occurs, complete Step 11 to clear the switch, then repeat Steps 6 through 9, monitoring traffic on your test set. If the problem remains, contact your next level of support.

Step 11 Next to Switch Commands, click **Clear**.

Step 12 In the Confirm Clear Operation confirmation dialog box, click **Yes**.

Step 13 In the Selected Group area, click the protect port. Next to Switch Commands, click **Force**.

Step 14 In the Confirm Force Operation dialog box, click **Yes**.

Step 15 In the Selected Group area, verify that the following appears:

```
Protect port - Protect/Standby [FORCE_SWITCH_TO_WORKING], [PORT STATE]
Working port - Working/Active [FORCE_SWITCH_TO_WORKING], [PORT STATE]
```

Step 16 Verify that traffic on the test set connected to the node is still running. The traffic flow can be interrupted for less than 50 ms. If a traffic interruption of more than 50 ms occurs, complete Step 11 and Step 12 to clear the switch, then repeat Steps 13 through 15, monitoring traffic on your test set. If the problem remains, contact your next level of support.

Step 17 Return to your originating procedure (NTP).

DLP-F193 SNCP Protection Switching Test

Purpose	This task verifies that an SNCP span is switching correctly.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	Required

Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note Although a service interruption under 60 ms might occur, the test circuit should continue to work before, during, and after the switches. If the circuit stops working, do not continue. Contact your next level of support.

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Right-click the span where you want to switch SNCP traffic and choose **Circuits**.

The Circuits on Span dialog box displays the SNCP circuits, including circuit names, location, and a color code showing which circuits are active on the span.

Step 3 Initiate a Force switch for all circuits on the span:

Caution The FORCE command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

a. Click the **Perform SNCP span switching** field.

b. Choose **FORCE** from the drop-down list.

c. Click **Apply**.

d. In the confirmation dialog box, click **Yes**.

e. In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the Switch State for all circuits is FORCE.

Note Unprotected circuits will not switch.

Step 4 Clear the Force switch:

a. Click the **Perform SNCP span switching** field.

b. Choose **CLEAR** from the drop-down list.

c. Click **Apply**.

d. In the confirmation dialog box, click **Yes**.

e. In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the Switch State for all SNCP circuits is CLEAR.

Step 5 Return to your originating procedure (NTP).

DLP-F194 Provision an Optical Circuit Source and Destination

Purpose	This task provisions the source and destination cards for an optical circuit.
Tools/Equipment	None

Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 Perform this task during one of the following procedures: DLP-F291 Verify MS-SPRing Extension Byte Mapping, page 17-82 DLP-F292 Single Shelf Control Card Switch Test, page 17-82 Circuit creation procedures in Chapter 6, "Create Circuits"
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Node drop-down list, choose the node where the circuit will originate.

Step 2 From the Slot drop-down list, choose the slot containing the optical card where the circuit originates. (If a card's capacity is fully utilized, it does not appear in the list.)

Step 3 Choose the source port from the Port drop-down list.

Step 4 Choose the virtual container (VC) from the VC drop-down list. VCs do not appear if they are already in use by other circuits.

Note The VCs that appear depend on the card, circuit size, and protection scheme.

Step 5 If you need to create a secondary source, for example, an SNCP bridge/selector circuit entry point in a multivendor SNCP, click **Use Secondary Source** and repeat Steps 1 through 4 to define the secondary source.

Step 6 Click **Next.**

Step 7 From the Node drop-down list, choose the destination node.

Step 8 From the Slot drop-down list, choose the slot containing the optical card where the circuit will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the list.)

Step 9 Choose the destination port from the Port drop-down list.

Step 10 Choose the VC from the VC drop-down list. VCs do not appear if they are already in use by other circuits.

Note The VCs that appear depend on the card, circuit size, and protection scheme.

Step 11 If you need to create a secondary destination, for example, an SNCP bridge/selector circuit entry point in a multivendor SNCP, click **Use Secondary Destination** and repeat Steps 7 through 10 to define the secondary destination.

Step 12 Click **Next**.

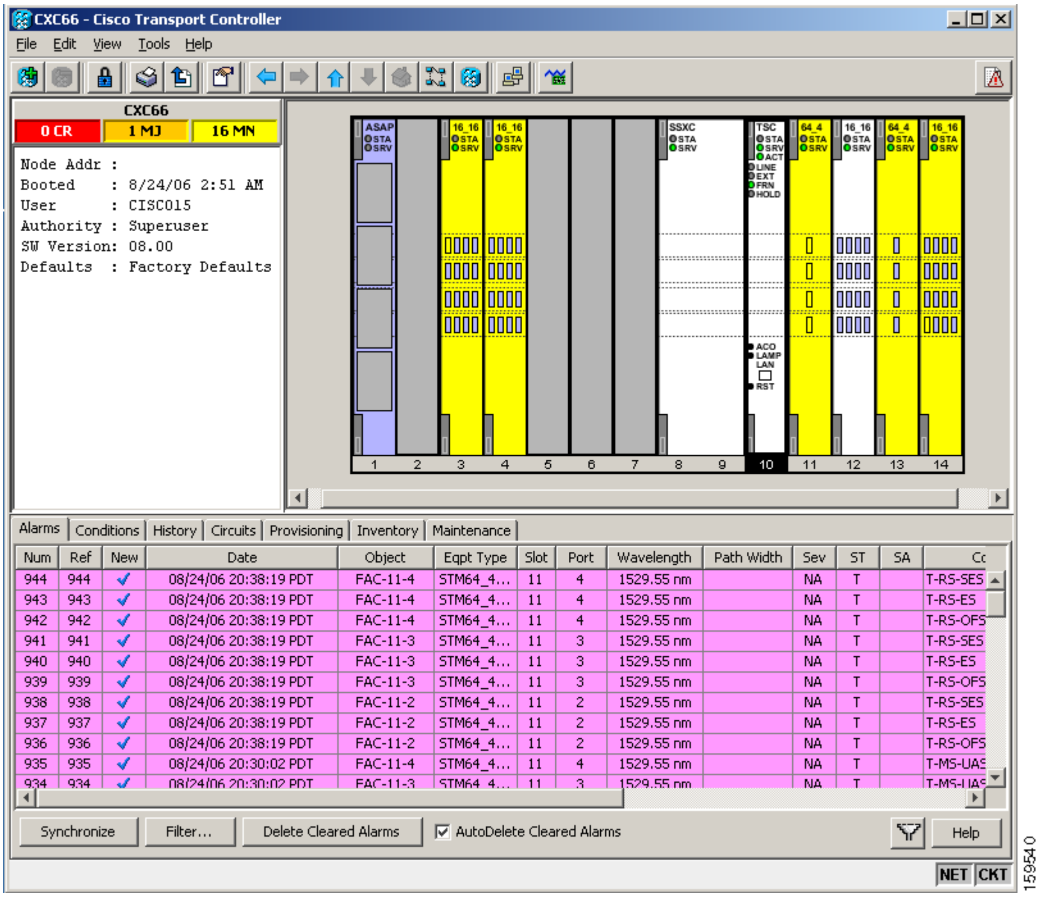
Step 13 Return to your originating procedure (NTP).

DLP-F195 View Alarms

Purpose	This task displays ONS 15600 SDH alarms at the card, node, or network level.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the card, node, or network view, click the **Alarms** tab to display the alarms for that card, node, or network. Figure 16-10 shows the Alarms window.

Figure 16-10 Viewing Alarms in CTC Node View



```
Node Addr :
Booted    : 8/24/06 2:51 AM
User      : CISCO15
Authority : Superuser
SW Version: 08.00
Defaults  : Factory Defaults
```

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Wavelength	Path Width	Sev	ST	SA	Cc
944	944	✓	08/24/06 20:38:19 PDT	FAC-11-4	STM64_4...	11	4	1529.55 nm		NA	T		T-RS-SES
943	943	✓	08/24/06 20:38:19 PDT	FAC-11-4	STM64_4...	11	4	1529.55 nm		NA	T		T-RS-ES
942	942	✓	08/24/06 20:38:19 PDT	FAC-11-4	STM64_4...	11	4	1529.55 nm		NA	T		T-RS-OFS
941	941	✓	08/24/06 20:38:19 PDT	FAC-11-3	STM64_4...	11	3	1529.55 nm		NA	T		T-RS-SES
940	940	✓	08/24/06 20:38:19 PDT	FAC-11-3	STM64_4...	11	3	1529.55 nm		NA	T		T-RS-ES
939	939	✓	08/24/06 20:38:19 PDT	FAC-11-3	STM64_4...	11	3	1529.55 nm		NA	T		T-RS-OFS
938	938	✓	08/24/06 20:38:19 PDT	FAC-11-2	STM64_4...	11	2	1529.55 nm		NA	T		T-RS-SES
937	937	✓	08/24/06 20:38:19 PDT	FAC-11-2	STM64_4...	11	2	1529.55 nm		NA	T		T-RS-ES
936	936	✓	08/24/06 20:38:19 PDT	FAC-11-2	STM64_4...	11	2	1529.55 nm		NA	T		T-RS-OFS
935	935	✓	08/24/06 20:30:02 PDT	FAC-11-4	STM64_4...	11	4	1529.55 nm		NA	T		T-MS-UAS
934	934	✓	08/24/06 20:30:02 PDT	FAC-11-3	STM64_4...	11	3	1529.55 nm		NA	T		T-MS-UAS

Step 2 Return to your originating procedure (NTP).

DLP-F196 View Alarm History

Purpose	This task displays past cleared and uncleared ONS 15600 SDH alarms at the card, node, or network level.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 To view history for the login node, go to Step 2.

To view alarm history for the network, go to Step 3.

To view alarm history for the card, go to Step 4.

Step 2 To display the node-level alarm history:

a. Click the **History > Session** tabs if you want to see only the alarms and events that have occurred since you logged into the current CTC session.

b. Click the **History > Shelf** tabs if you want to retrieve all available alarms for the node.

c. Go to Step 5.

Note At the network-level view, CTC displays only network alarms and events that occur during your current login session.

Step 3 To view alarm information for the network level:

a. From the View menu, choose **Go to Network View**.

b. Click the **History** tab.

Alarms and events that have occurred on the network since you logged into CTC appear.

c. Go to Step 5.

Step 4 To view alarm information for the card level:

a. In node view, double-click a card on the shelf graphic to display the card view.

b. Click the **History > Session** tabs if you want to see only the alarms and events that have occurred since you logged into CTC.

c. Click the **History > Card** tabs if you want to retrieve all available alarms for the card.

d. Go to Step 5.

Note The ONS 15600 SDH can store up to 3,000 total alarms and events: 750 Critical (CR) alarms, 750 Major (MJ) alarms, 750 Minor (MN) alarms, and 750 events. When the limit is reached for an alarm or event type, the ONS 15600 SDH overwrites the oldest alarms and events.

Step 5 Verify that the Alarms check box is selected. Alarms are events with a severity of Minor (MN), Major (MJ), or Critical (CR).

Step 6 If you want to retrieve events, check the **Events** check box.

Events include both alarms and conditions. Conditions are events with a severity of Not Alarmed (NA) or Not Reported (NR).

Step 7 Click **Retrieve**.

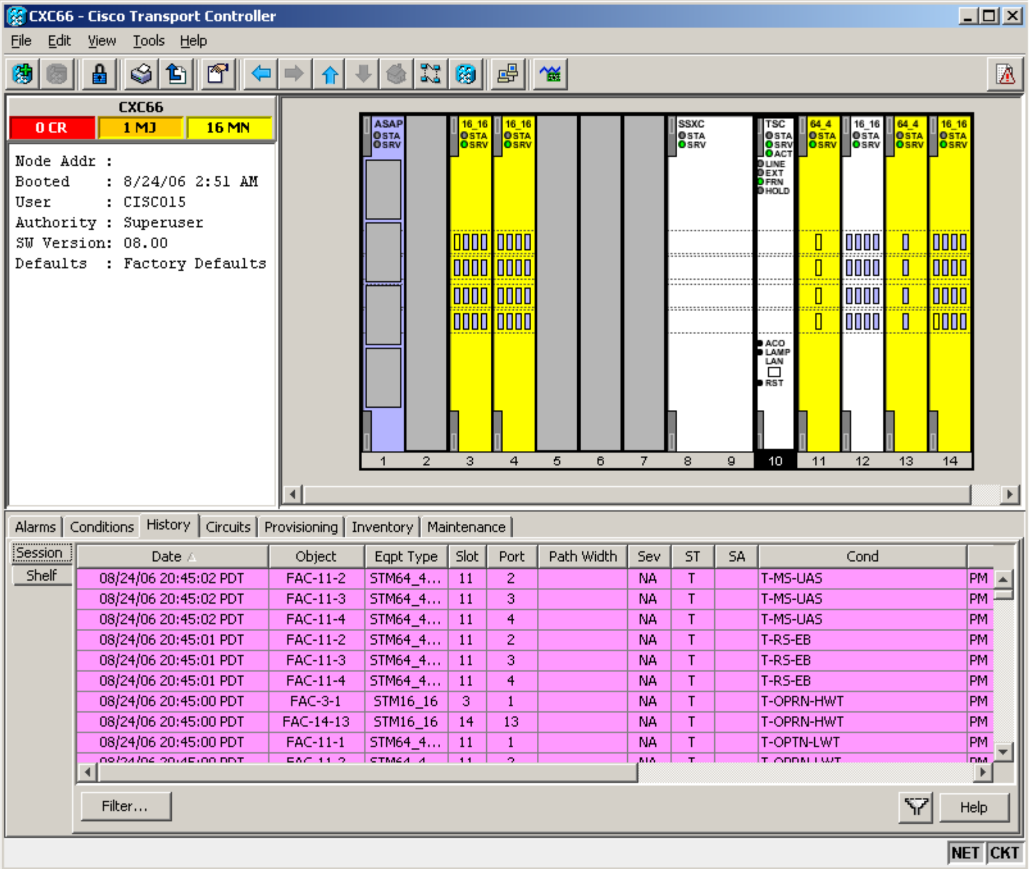
Tip Double-click an alarm in the alarm table or an event in the history table to display the corresponding view for the alarm. For example, double-clicking a card alarm takes you to card view. In network view, double-clicking a node alarm takes you to node view.

Alarms have specifically numbered VC object identifiers based upon the object TL1 access identifiers (AIDs). The port-based alarm numbering scheme is shown in Table 16-4. Figure 16-11 on page 16-56 shows an example of viewing all alarms reported for the current session in CTC.

Table 16-4 Port-Based Alarm Numbering Scheme

Object	VC AID	Port Number
MON object	VC-<Slot>-<Port>-<VC> For example, VC-6-1-6	Port=1

Figure 16-11 Viewing All Alarms Reported for Current Session



```
Node Addr :
Booted    : 8/24/06 2:51 AM
User      : CISCO15
Authority : Superuser
SW Version: 08.00
Defaults  : Factory Defaults
```

Date	Object	Eqpt Type	Slot	Port	Path Width	Sev	ST	SA	Cond	
08/24/06 20:45:02 PDT	FAC-11-2	STM64_4...	11	2		NA	T		T-MS-UAS	PM
08/24/06 20:45:02 PDT	FAC-11-3	STM64_4...	11	3		NA	T		T-MS-UAS	PM
08/24/06 20:45:02 PDT	FAC-11-4	STM64_4...	11	4		NA	T		T-MS-UAS	PM
08/24/06 20:45:01 PDT	FAC-11-2	STM64_4...	11	2		NA	T		T-RS-EB	PM
08/24/06 20:45:01 PDT	FAC-11-3	STM64_4...	11	3		NA	T		T-RS-EB	PM
08/24/06 20:45:01 PDT	FAC-11-4	STM64_4...	11	4		NA	T		T-RS-EB	PM
08/24/06 20:45:00 PDT	FAC-3-1	STM16_16	3	1		NA	T		T-OPRN-HWT	PM
08/24/06 20:45:00 PDT	FAC-14-13	STM16_16	14	13		NA	T		T-OPRN-HWT	PM
08/24/06 20:45:00 PDT	FAC-11-1	STM64_4...	11	1		NA	T		T-OPTN-LWT	PM

Step 8 Return to your originating procedure (NTP).

DLP-F197 View Conditions

Purpose	This task displays conditions (events with an NR severity) at the card, node, or network level. Conditions give you a record of changes or events that did not result in alarms.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 To view alarm history for the login node, go to Step 2.

If you want to view alarm history for the network, go to Step 3.

If you want to view alarm history for the card, go to Step 4.

Step 2 To display the node-level conditions:

a. Click the **Conditions** tab if you want to see only the conditions that apply to the node.

b. Go to Step 5.

Step 3 To view network-level conditions:

a. From the View menu, choose **Go to Network View**.

b. Click the **Conditions** tab if you want to see only the conditions that apply to the network.

Note If you are not in the node (default) CTC view, you can also click the Conditions tab in the card and network views to obtain the same results.

Step 4 To view card-level conditions:

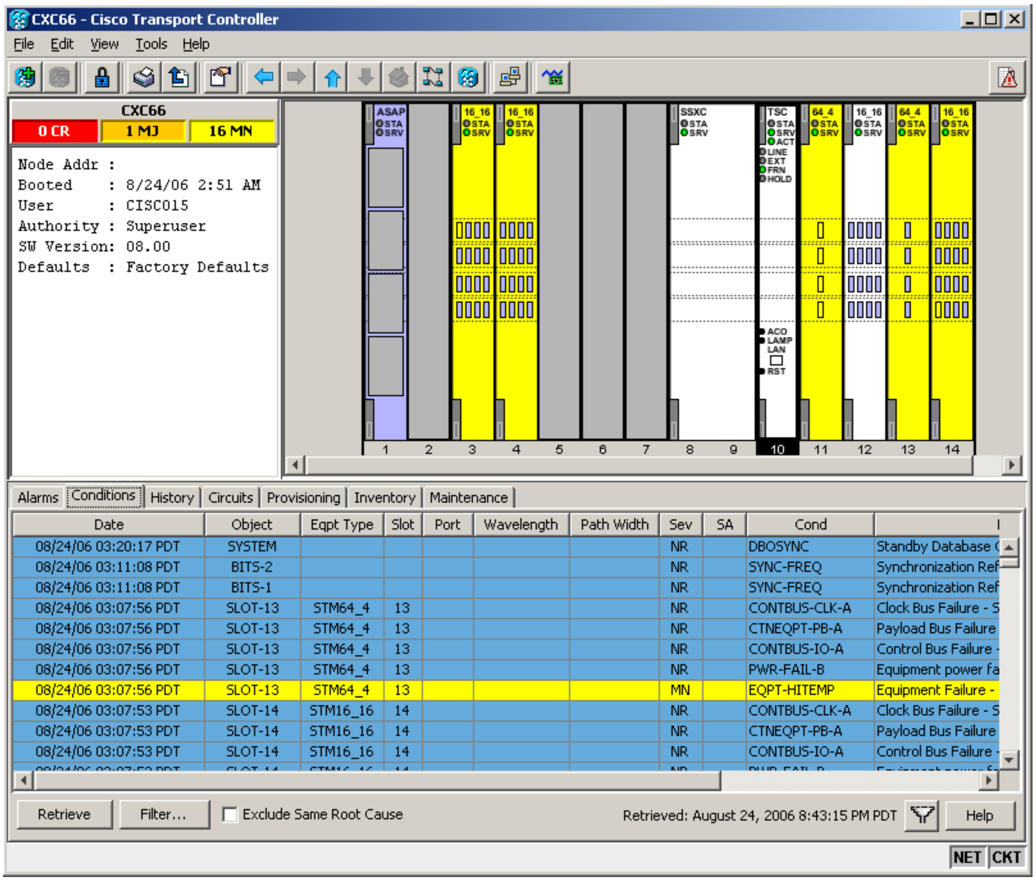
a. Double-click a card on the shelf graphic to display the card view.

b. Click the **Conditions** tab if you want to see only the conditions that apply to the card.

Step 5 Click **Retrieve**. (See Figure 16-12.)

Conditions include both alarms and events. Alarms are conditions with a severity of MN, MJ, or CR. Events are conditions with a severity of NA or NR.

Figure 16-12 Viewing Retrieved Fault Conditions in the Conditions Window



```
Node Addr :
Booted    : 8/24/06 2:51 AM
User      : CISCO15
Authority : Superuser
SW Version: 08.00
Defaults  : Factory Defaults
```

Date	Object	Eqpt Type	Slot	Port	Wavelength	Path Width	Sev	SA	Cond	
08/24/06 03:20:17 PDT	SYSTEM						NR		DBOSYNC	Standby Database (
08/24/06 03:11:08 PDT	BITS-2						NR		SYNC-FREQ	Synchronization Ref
08/24/06 03:11:08 PDT	BITS-1						NR		SYNC-FREQ	Synchronization Ref
08/24/06 03:07:56 PDT	SLOT-13	STM64_4	13				NR		CONTBUS-CLK-A	Clock Bus Failure - S
08/24/06 03:07:56 PDT	SLOT-13	STM64_4	13				NR		CTNEQPT-PB-A	Payload Bus Failure
08/24/06 03:07:56 PDT	SLOT-13	STM64_4	13				NR		CONTBUS-IO-A	Control Bus Failure -
08/24/06 03:07:56 PDT	SLOT-13	STM64_4	13				NR		PWR-FAIL-B	Equipment power fa
08/24/06 03:07:56 PDT	SLOT-13	STM64_4	13				MN		EQPT-HITEMP	Equipment Failure -
08/24/06 03:07:53 PDT	SLOT-14	STM16_16	14				NR		CONTBUS-CLK-A	Clock Bus Failure - S
08/24/06 03:07:53 PDT	SLOT-14	STM16_16	14				NR		CTNEQPT-PB-A	Payload Bus Failure
08/24/06 03:07:53 PDT	SLOT-14	STM16_16	14				NR		CONTBUS-IO-A	Control Bus Failure -

☐ Exclude Same Root Cause

Retrieved: August 24, 2006 8:43:15 PM PDT

Step 6 Return to your originating procedure (NTP).

DLP-F198 Display Events Using Each Node's Time Zone

Purpose	This task changes the time stamp for events to the time zone of the ONS node reporting the alarm. By default, the events time stamp is set to the time zone for the CTC workstation.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From the Edit menu, choose **Preferences**.

The CTC Preferences Dialog appears.

Step 2 Click the **Display Events Using Each Node's Time Zone** check box.

Step 3 Click **Apply** and **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-F199 Create Alarm Severity Profiles

Purpose	This task creates severity profiles for alarms by modifying the default severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

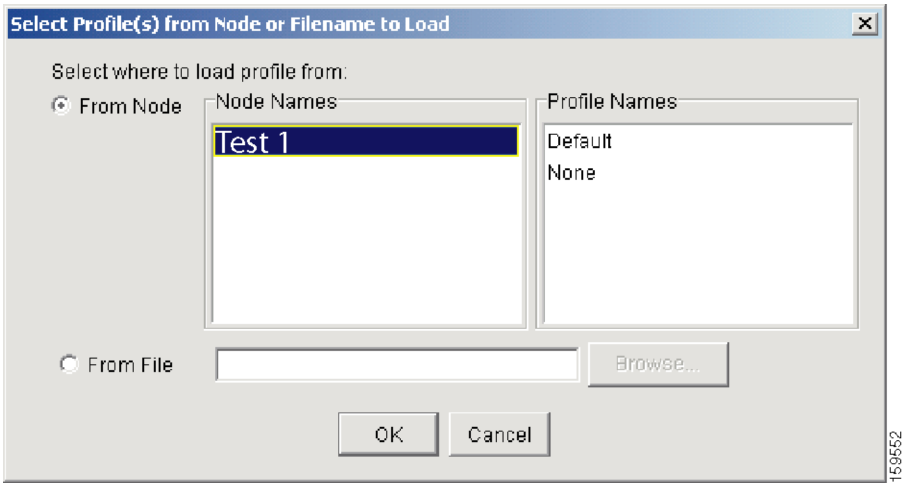
Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > Alarm Profiles** tabs.

Step 3 In the Node/Profile Ops area, click **Load**.

Step 4 Highlight the node name you are logged into in the Node Names field and highlight **Default** in the Profile Names field (Figure 16-13).

Figure 16-13 Select Profile(s) from Node or Filename to Load Dialog Box



Select Profile(s) from Node or Filename to Load

Select where to load profile from:

● From Node

Node Names: Test 1

Profile Names: Default, None

○ From File

Step 5 Click **OK**.

Step 6 Right-click in the Default column to display the profile editing shortcut menu.

Step 7 Choose **Clone** in the shortcut menu.

In the profile editing shortcut menu, any profile other than Inherited can be cloned.

Step 8 In the Clone Profile Default dialog box, type a name in the New Profile Name field.

Alarm profile names must be unique. If you try to import or name a profile that has the same name as another profile, CTC adds a suffix to create a new name.

Step 9 Click **OK**. A new alarm profile (named in Step 8) is created. This profile duplicates the severities of the default profile and appears as a new column on the right side.

Step 10 Modify the alarm profile:

a. In the new alarm profile column, left-click the alarm severity you want to change in the alarm profile column.

b. Select the desired severity from the drop-down list.

c. Repeat Steps a and b for each alarm severity that needs to be changed.

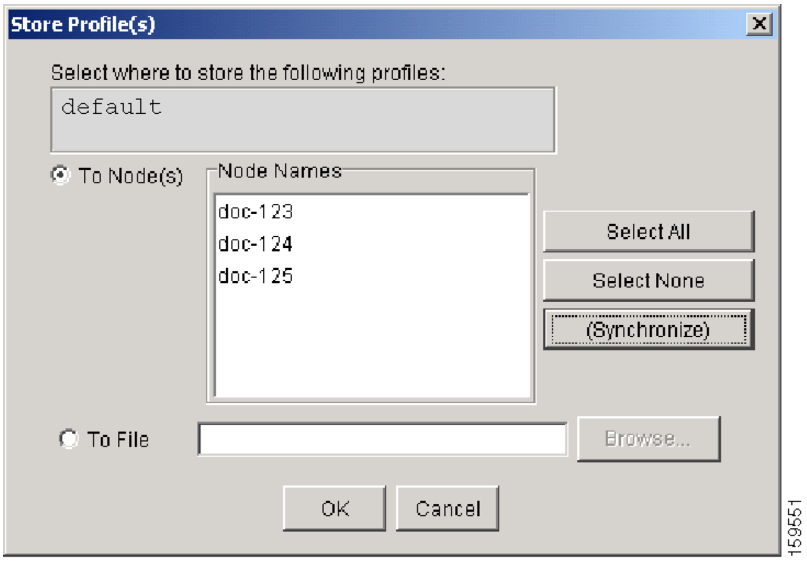
d. After you have chosen severities for your new alarm profile, click anywhere in new alarm profile column to highlight it.

e. Click **Store** in the Node/Profile Ops area or select Store from the shortcut menu.

Step 11 If you want to save the profile to one or more nodes, click the **To Node(s)** radio button (Figure 16-14) and choose the node(s) where you want to save the profile:

- If you want to save the profile to only one node, click the node in the Node Names list.
- If you want to save the profile to all nodes, click **Select All**.
- If you do not want to save the profile to any nodes, click **Select None**.
- If you want to update alarm profile information, click (**Synchronize)**.

Figure 16-14 Store Profiles Dialog Box



Store Profile(s)

Select where to store the following profiles:

default

● To Node(s)

Node Names

doc-123
doc-124
doc-125

Step 12 If you want to save the profile to a file:

a. Click the **To File** radio button.

b. Click **Browse** and navigate to the profile save location.

c. Enter a name in the File name field.

d. Click the **Select** button to choose this name and location.

Note Long file names are supported. CTC supplies a suffix of *.pfl to stored files.

Step 13 Click **OK** to store the profile.

Note Click the **Hide identical rows** check box to configure the Alarm Profiles window to display rows with dissimilar severities.

Note Click the **Hide reference values** check box to configure the Alarm Profiles window to display severities that do not match the Default profile.

Step 14 As needed, complete the "DLP-F200 Apply Alarm Profiles for Ports and Cards" task on page 17-1.

Step 15 As needed, complete the "DLP-F201 Apply Alarm Profiles to Cards and Nodes" task on page 17-3.

Step 16 Return to your originating procedure (NTP).

CHAPTER 17

DLPs F200 to F299

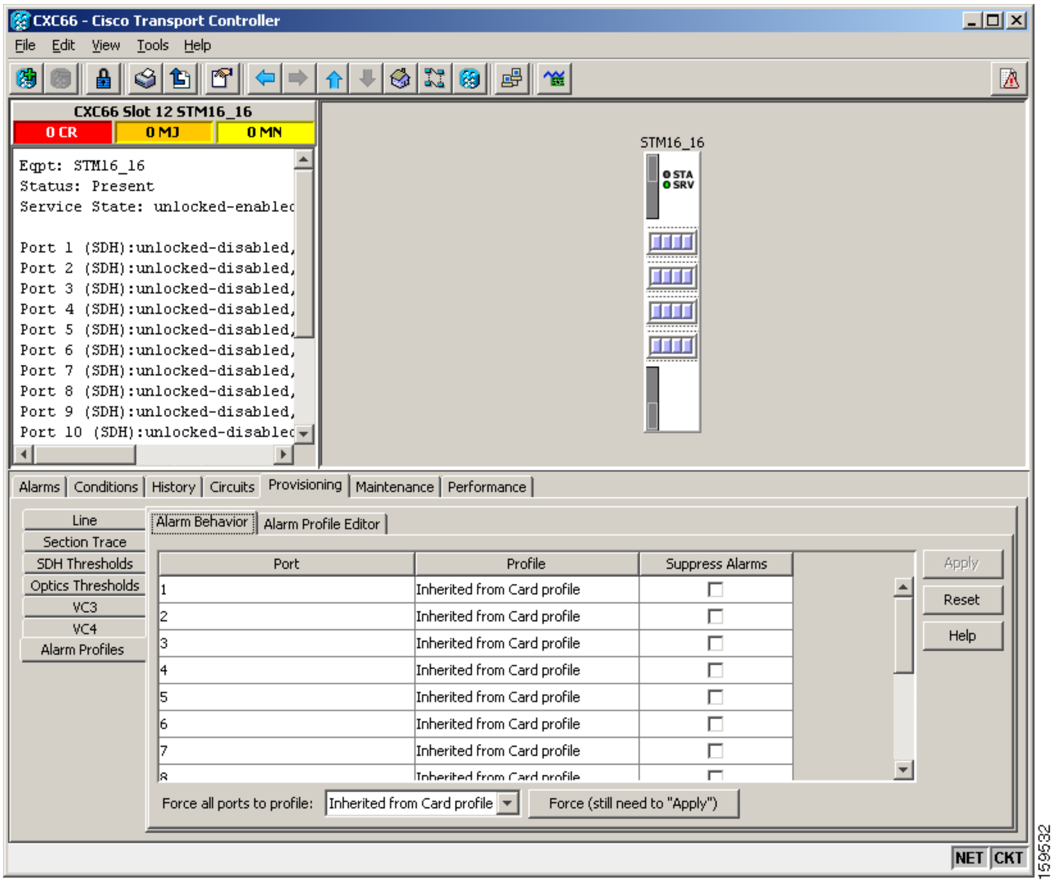
DLP-F200 Apply Alarm Profiles for Ports and Cards

Purpose	This task applies alarm severity profiles to a port or a card.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 DLP-F199 Create Alarm Severity Profiles, page 16-59
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the card graphic.

Step 2 Click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs (Figure 17-1).

Figure 17-1 Card View Alarm Profiles



```
Eqpt: STM16_16
Status: Present
Service State: unlocked-enablec

Port 1 (SDH):unlocked-disabled,
Port 2 (SDH):unlocked-disabled,
Port 3 (SDH):unlocked-disabled,
Port 4 (SDH):unlocked-disabled,
Port 5 (SDH):unlocked-disabled,
Port 6 (SDH):unlocked-disabled,
Port 7 (SDH):unlocked-disabled,
Port 8 (SDH):unlocked-disabled,
Port 9 (SDH):unlocked-disabled,
Port 10 (SDH):unlocked-disablec
```

Port	Profile	Suppress Alarms
1	Inherited from Card profile	□
2	Inherited from Card profile	□
3	Inherited from Card profile	□
4	Inherited from Card profile	□
5	Inherited from Card profile	□
6	Inherited from Card profile	□
7	Inherited from Card profile	□
8	Inherited from Card profile	□

Force all ports to profile: Inherited from Card profile

Step 3 To apply alarm profiles on a port-by-port basis:

a. Click the specific port row in the Profile column.

b. Choose the profile from the drop-down list.

You can select multiple port profiles.

c. Click **Apply**.

Step 4 To apply a profile for all the ports on a card:

a. Click the **Force all ports to profile** drop-down list at the bottom of the window.

b. Choose the profile.

c. Click **Force (still need to "Apply")**.

d. Click **Apply**.

Tip If you choose the wrong profile, click **Reset** to return to the previous profile setting.

Step 5 Return to your originating procedure (NTP).

DLP-F201 Apply Alarm Profiles to Cards and Nodes

Purpose	This task applies a custom or default alarm profile to cards or nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 DLP-F199 Create Alarm Severity Profiles, page 16-59
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

Step 2 To apply a profile to a card:

a. Click the Profile column row for the card.

b. Choose the profile from the drop-down list.

You can select multiple profiles for multiple cards.

c. Click **Apply**.

Step 3 To apply the profile to an entire node:

a. Click the **Node Profile** drop-down list.

b. Choose the profile.

c. Click **Apply**.

Tip If you choose the wrong profile, click **Reset** to return to the previous profile.

Step 4 Return to your originating procedure (NTP).

DLP-F202 Suppress Alarm Reporting

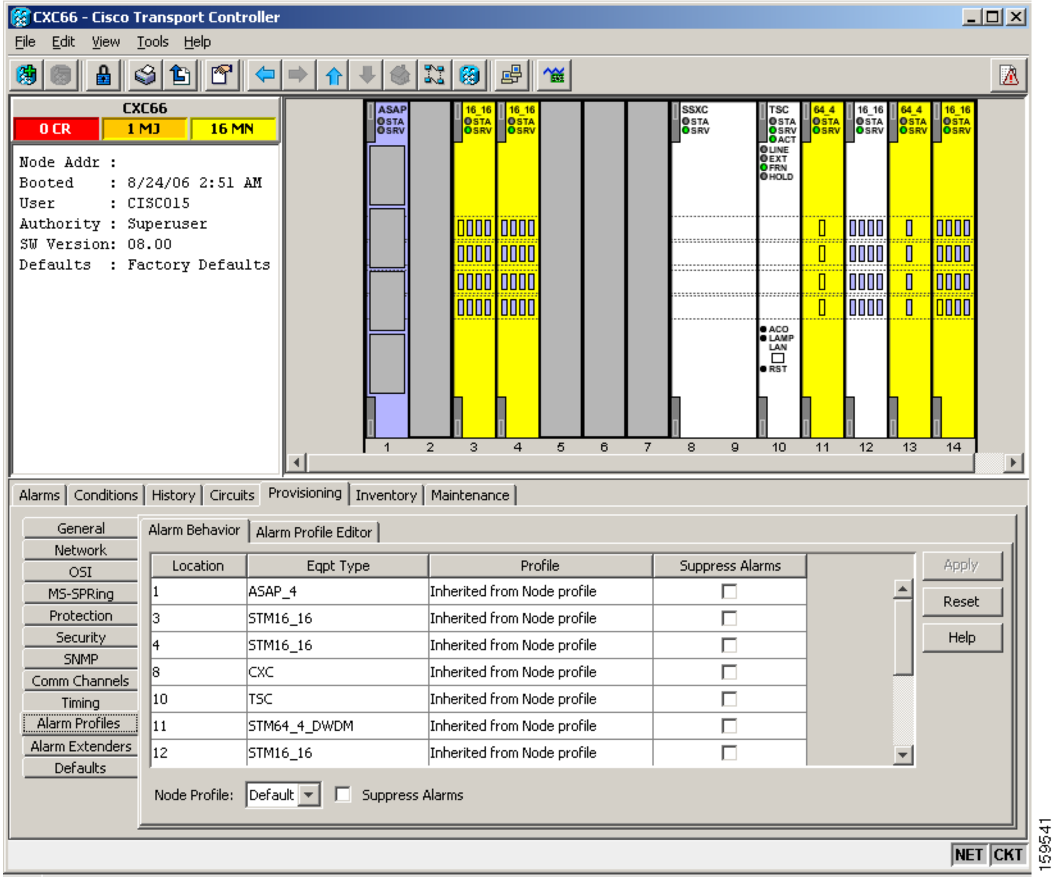
Purpose	This task suppresses the reporting of ONS 15600 SDH alarms at the port, card, or node level.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Use alarm suppression with caution. Suppressing alarms in one session suppresses the alarms in all other open CTC and TL1 sessions.

Step 1 In node or card view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs (Figure 17-2).

Note Suppressing alarms for a card or node causes the alarms to appear on the CTC Conditions window instead of the Alarms window. The suppressed alarms on the Conditions window appear there with their alarm severities, color codes, and service-affecting status. But as conditions, their severities are overridden as NR severity. Suppressed alarms do not appear on the History window or in the Alarms window of any other clients.

Figure 17-2 Suppress Alarms Check Box



```
Node Addr :
Booted    : 8/24/06 2:51 AM
User      : CISCO15
Authority : Superuser
SW Version: 08.00
Defaults  : Factory Defaults
```

Location	Eqpt Type	Profile	Suppress Alarms
1	ASAP_4	Inherited from Node profile	☐
3	STM16_16	Inherited from Node profile	☐
4	STM16_16	Inherited from Node profile	☐
8	CXC	Inherited from Node profile	☐
10	TSC	Inherited from Node profile	☐
11	STM64_4_DWDM	Inherited from Node profile	☐
12	STM16_16	Inherited from Node profile	☐

Node Profile: Default ☐ Suppress Alarms

Step 2 To suppress alarms, perform the following action, as needed:

- To suppress alarms for the entire node in the node view, check the **Suppress Alarms** check box next to the Node Profile drop-down list.
- To suppress alarms for a card in the node view, check the **Suppress Alarms** check box for the card you want to suppress.
- To suppress alarms for a port in the card view, check the **Suppress Alarms** check box for ports you want to suppress.

Step 3 Click **Apply**.

The node sends out autonomous messages to clear any raised alarms.

Step 4 Return to your originating procedure (NTP).

DLP-F203 Restore Alarm Reporting

Purpose	This task removes the alarm suppression command on a port, card, or node.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 DLP-F202 Suppress Alarm Reporting, page 17-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view or card view, depending on where the alarms were suppressed, click the **Provisioning > Alarm Profiles > Alarm Behavior** tab.

Note Suppressed alarm reporting must be restored in the same view where it was suppressed.

Step 2 In node view, uncheck the **Suppress Alarms** check box next to the Node Profile drop-down list, or uncheck the slot row for a card.

Step 3 In card view, uncheck the **Suppress Alarms** check box for the ports you want to stop suppressing.

Step 4 Click **Apply**. The node sends out autonomous messages to raise any actively suppressed alarms.

Step 5 Return to your originating procedure (NTP).

DLP-F204 Provision External Alarms and Virtual Wires

Purpose	This task creates, enables, and sets severities for up to 16 alarms caused by external events (such as a low battery, fire detector failure, or low temperature).
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 DLP-F392 Install Alarm Wires on the CAP/CAP2, page 18-108
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Alarm Extenders > External Alarms** tabs.

Step 2 Complete the following fields for each external device wired to the ONS 15600 SDH backplane:

- Enabled—Check the check box for the alarm input number that you want to configure.

- Alarm Type—Choose an alarm type, such as Low temp or Misc, from the drop-down list.
- Severity—Choose an alarm severity (CR, MJ, MN, NA, or NR) from the drop-down list. The severity determines how the alarm appears in the CTC Alarms and History windows and whether the LEDs are activated in the software.

Note When virtual wires are assigned in mixed ONS 15454 SDH and ONS 15600 SDH networks, only the last four virtual wires (13 through 16) are visible from the ONS 15454 SDH nodes.

- Virtual Wire—From the drop-down list, choose a virtual wire (1 through 16) for the alarm. If you choose None, the alarm is not activated in CTC.
- Raised When—From the drop-down list, choose the contact condition (open or closed) that will trigger the alarm in CTC.
- Description—Default descriptions are provided for each alarm. To change the description, which is how the alarm is identified in CTC, double-click the field and edit as necessary.

Step 3 To provision additional devices, complete Step 2 for each additional device.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-F205 Provision External Controls for External Alarms and Virtual Wires

Purpose	This task configures the external control outputs. An external control governs an external alarm.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
	DLP-F392 Install Alarm Wires on the CAP/CAP2, page 18-108
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Alarm Extenders > External Controls** tabs.

Step 2 Complete the following fields for each external control wired to the ONS 15600 SDH backplane:

- Enabled—Check this check box for the alarm control output number that you want to configure.
- Control Type—In the drop-down list, choose the type of control, such as Engine or Heat. For example, if you set up a virtual wire in the "DLP-F204 Provision External Alarms and Virtual Wires" task on page 17-5 as alarm type Low Temp, you would choose a control type in the External Controls tab such as "Heat."
- Trigger Type—Choose a means for triggering the alarm from the drop-down list, such as a local or remote alarm of a particular severity or association with a particular virtual wire.
- Description—Enter a description to be shown in the Alarms window.

Step 3 To provision additional controls, complete Step 2 for each additional device.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-F206 View Optical STM-N PM Parameters

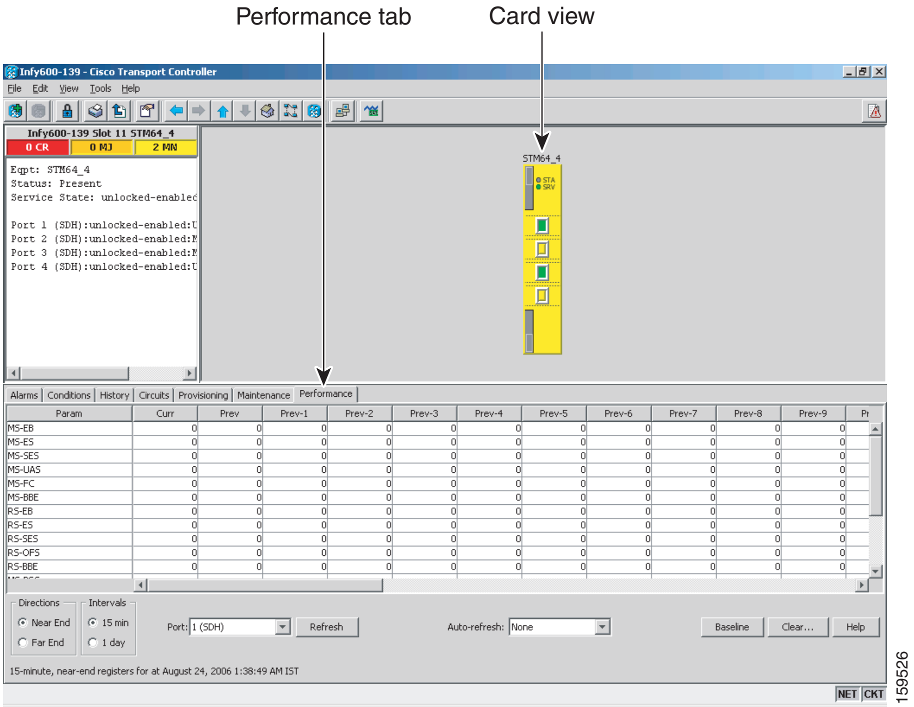
Purpose	This task enables you to view performance monitoring (PM) counts on a selected STM-N card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an STM-N card. The card view appears.

Step 2 Click the **Performance** tab (Figure 17-3).

Note The performance window defaults to Port 1 (SDH), VC3/VC4 PM counts. You must select the specific port and/or VC where you want to view PM counts. See the "DLP-F207 Refresh PM Counts for a Selected Port and VC" task on page 17-8.

Figure 17-3 Viewing Optical STM-N Performance Monitoring Information



```
Eqpt: STM64_4
Status: Present
Service State: unlocked-enablec

Port 1 (SDH):unlocked-enabled:U
Port 2 (SDH):unlocked-enabled:M
Port 3 (SDH):unlocked-enabled:M
Port 4 (SDH):unlocked-enabled:U
```

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9	Pr
MS-EB	0	0	0	0	0	0	0	0	0	0	0	
MS-ES	0	0	0	0	0	0	0	0	0	0	0	
MS-SES	0	0	0	0	0	0	0	0	0	0	0	
MS-UAS	0	0	0	0	0	0	0	0	0	0	0	
MS-FC	0	0	0	0	0	0	0	0	0	0	0	
MS-BBE	0	0	0	0	0	0	0	0	0	0	0	
RS-EB	0	0	0	0	0	0	0	0	0	0	0	
RS-ES	0	0	0	0	0	0	0	0	0	0	0	
RS-SES	0	0	0	0	0	0	0	0	0	0	0	
RS-OFS	0	0	0	0	0	0	0	0	0	0	0	
RS-BBE	0	0	0	0	0	0	0	0	0	0	0	

Directions: ● Near End ○ Far End

Intervals: ● 15 min ○ 1 day

Port: 1 (SDH)

Auto-refresh: None

15-minute, near-end registers for at August 24, 2006 1:38:49 AM IST

Step 3 The PM parameter names appear on the left portion of the window in the Param column. The parameter values appear on the right portion of the window in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions refer to the "Performance Monitoring" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Step 4 Return to your originating procedure (NTP).

DLP-F207 Refresh PM Counts for a Selected Port and VC

Purpose	This task changes the window view to display PM counts for a selected optical (STM-N) card port and virtual container (VC).
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From node view, double-click an STM-N or Ethernet port. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the Port drop-down list and choose the desired port.

Step 4 Click **Refresh**. All PM counts occurring for the selected port appear. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Step 5 Return to your originating procedure (NTP).

DLP-F208 Refresh PM Counts at Fifteen-Minute Intervals

Purpose	This task changes the window view to display PM counts in 15-minute intervals.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an STM-N or Ethernet port. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **15 min** radio button.

Step 4 Click **Refresh**. The PM parameters appear in 15-minute intervals that are synchronized with the time of day.

Step 5 View the Current column to find PM counts for the current 15-minute interval.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 15-minute interval, a threshold crossing alert (TCA) is raised. The number represents the counter value for each specific performance monitoring parameter.

Step 6 View the Prev-*n* columns to find PM counts for the preceding 15-minute intervals.

Note If a complete 15-minute interval count is not possible, the value has a yellow background. An incomplete or incorrect count can be caused by monitoring for less than 15 minutes after the counter started, changing node timing settings, changing the time zone settings, changing the count by using the clear function, replacing a card, resetting a card, or changing port states. When the problem is corrected, the subsequent 15-minute interval appears with a white background.

Step 7 Return to your originating procedure (NTP).

DLP-F209 Refresh PM Counts at One-Day Intervals

Purpose	This task changes the window view to display PM counts in one-day intervals.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an STM-N or Ethernet port. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **1 day** radio button.

Step 4 Click **Refresh**. The PM parameters display in one-day (24-hour) intervals that are synchronized with the time of day. For PM parameter definitions refer to the "Performance Monitoring" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Step 5 View the Current column to find PM counts for the current one-day interval.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular one-day interval, a TCA is raised. The number represents the counter value for each specific performance monitoring parameter.

Step 6 View the Prev-*n* columns to find PM counts for the preceding one-day intervals.

Note If a complete count over a one-day interval is not possible, the value has a yellow background. An incomplete or incorrect count can be caused by monitoring for less than 24 hours after the counter started, changing node timing settings, changing the time zone settings, replacing a card, resetting a card, changing port states, or adjusting and clearing the counter. When the problem is corrected, the subsequent one-day interval appears with a white background.

Step 7 Return to your originating procedure (NTP).

DLP-F210 Monitor Near-End PM Counts

Purpose	This task changes the window view to show near-end PM counts for the selected card, port, and VC.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an STM-N or Ethernet port. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Near End** radio button.

Step 4 Click **Refresh**. All PM counts recorded by the near-end node for the incoming signal on the selected card/port/VC appear. For PM parameter definitions refer to the "Performance Monitoring" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Step 5 Return to your originating procedure (NTP).

DLP-F211 Monitor Far-End PM Counts

Purpose	This task changes the window view to show far-end PM counts for the selected card, port, and VC.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an STM-N or Ethernet port. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Far End** radio button.

Step 4 Click **Refresh**. All PM counts that are recorded by the far-end node for the outgoing signal on the selected card/port/VC appear. For PM parameter definitions refer to the "Performance Monitoring" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Step 5 Return to your originating procedure (NTP).

DLP-F212 Reset Current PM Counts

Purpose	This task uses the Baseline button to clear the PM count shown in the current time interval, but it does not clear the cumulative PM count. This allows you to see how quickly the PM counts rise.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From node view, double-click an STM-N or Ethernet port. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click **Baseline**.

Note The Baseline button clears the PM count shown in the Current column, but does not clear the PM counts on the card. When the current time interval expires or the window view changes, the total number of PM counts on the card and on the window appear in the appropriate column. The baseline values are discarded if you change views to a different window and then return to the Performance tab window.

Step 4 View the Current column to observe changes to PM counts for the current time interval.

Step 5 Return to your originating procedure (NTP).

DLP-F213 Clear Selected PM Counts

Purpose	This task uses the Clear button to clear specified PM counts depending on the selected option.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Caution The Clear button can mask problems if used incorrectly. This button is commonly used for testing purposes.

Step 1 In node view, double-click an STM-N or Ethernet port. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click **Clear**.

Step 4 In the Clear Statistics menu, choose one of the following options:

- **Displayed statistics**: This option erases from the window display all PM counts that currently appear in the Performance tab window.
- **All statistics for port *n***: This option erases from the window display and card memory all PM counts associated with the selected port. This means the 15-minute/one-day and near-end/far-end PM counts for the selected port are cleared from the card and the window display.
- **All statistics for card**: This option erases from the window display and card memory all PM counts associated with the selected card. This means the 15-minute/one-day and near-end/far-end PM counts for the selected card are cleared from the card and the window display.
- **All statistics for selected parameters**: This option erases from the window display and card memory all PM counts associated with the selected parameters. For example, if the 15 min and the Near End radio buttons are selected, all near-end PM counts in the current 15-minute interval are erased from the card and the window display.

Step 5 Click **Yes** to clear the selected statistics.

Step 6 Verify that the selected PM counts have been cleared.

Step 7 Return to your originating procedure (NTP).

DLP-F214 Search for Circuits

Purpose	This task searches for an ONS 15600 SDH circuit at the network, node, or card level.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate CTC view:

- To search the entire network, from the View menu choose **Go To Network View**.
- To search for circuits that originate, terminate, or pass through a specific node, from the View menu choose **Go To Other Node**, then choose the node you want to search and click **OK**.
- To search for circuits that originate, terminate, or pass through a specific card, double-click the card on the shelf graphic in node view to display the card in card view.

Step 2 Click the **Circuits** tab.

Step 3 If you are in node or card view, choose the scope for the search (**Network** or **Node**) from the Scope drop-down list.

Step 4 Click **Search**.

Step 5 In the Circuit Name Search dialog box, complete the following:

- Find What—Enter the text of the circuit name you want to find.
- Match Whole Word Only—Check this box to instruct CTC to select circuits only if the entire word matches the text in the Find What field.
- Match Case—Check this box to instruct CTC to select circuits only when the capitalization matches the capitalization entered in the Find What field.
- Direction—Choose the direction for the search. Searches are conducted up or down from the currently selected circuit.

Step 6 Click **Find Next**.

Step 7 Repeat Steps 5 and 6 until you are finished, then click **Cancel**.

Step 8 Return to your originating procedure (NTP).

DLP-F215 Filter the Display of Circuits

Purpose	This task filters the display of circuits in the ONS 15600 SDH network, node, or card view Circuits window based on circuit name, size, type, direction, and other attributes.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate CTC view:

- To filter network circuits, from the View menu choose **Go To Network View**.
- To filter circuits that originate, terminate, or pass through a specific node, from the View menu choose **Go To Other Node**, then choose the node you want to search and click **OK**.
- To filter circuits that originate, terminate, or pass through a specific card, double-click the card on the shelf graphic in node view to display the card in card view.

Step 2 Click the **Circuits** tab.

Step 3 Set the attributes for filtering the circuit display:

a. Click the **Filter** button.

b. In the Circuit Filter dialog box, complete the following, as applicable:

Note You can use all of the Filter dialog box options, partial options, or a single option to create a filter.

- Name—Enter a complete or partial circuit name to filter circuits based on circuit name; otherwise leave the field blank.
- Direction—Choose one: **Any** (CTC will not use direction to filter circuits), **1-way** (CTC displays only one-way circuits), or **2-way** (CTC displays only two-way circuits).
- OCHNC Wlen—(DWDM OCHNCs only; refer to the *Cisco ONS 15454 DWDM Procedure Guide*) Choose an optical channel network connection (OCHNC) wavelength to filter the circuits. For example, choosing 1530.33 will display channels provisioned on the 1530.33-nm wavelength.
- Status—Choose a circuit status to filter the circuits. For more information about circuit statuses, see Table 18-3 on page 18-53.
- State—Choose one: **Locked** (display only out-of-service circuits), **Unlocked** (display only in-service circuits; optical channel network connections have Unlocked status only), or **Locked-PARTIAL** (display only circuits with cross-connects in mixed service states).
- Protection—Choose the protection type from the drop-down list. For more information about protection types, see Table 18-2 on page 18-52.
- Slot—Enter a slot number to filter circuits based on source or destination slot; otherwise leave the field blank.

- Port—Enter a port number to filter circuits based on source or destination port; otherwise leave the field blank.
- Type—Choose one:

  Any (CTC will not use circuit type to filter circuits)

  VC_HO_PATH_CIRCUIT (CTC displays only high-order path circuits)

  VC_LO_PATH_CIRCUIT (CTC displays only low-order path circuits)

  VC_LO_PATH_TUNNEL (CTC displays only low-order tunnel circuits)

  VC_LO_PATH_AGGREGATION (CTC displays only low-order path aggregation circuits)

  VC_HO_PATH_VCAT_CIRCUIT (CTC displays only high-order path VCAT circuits)

  VC_LO_PATH_VCAT_CIRCUIT (CTC displays only low-order path VCAT circuits)

  OCHNC (CTC displays only OCHNC circuits)

  OCHTRAIL (CTC displays only OCHTRAIL circuits)

  OCHCC (CTC displays only OCHCC circuits)
- Size—Click the appropriate check boxes to filter circuits based on size: Equipped non-specific, VC3, VC4-8c, VC11, 2.5 Gb/s No FEC, 10 Gb/s No FEC, VC4-6c, VC4-2c, VC4-32c, VC4-64c, VC4-16c, VC4-3c, 10 Gb/s FEC, VC4, VC12, OCHCC, VC4-4c, 2.5 Gb/s FEC, VC4-12c, and/or Multi-rate.

Step 4 To set the filter for ring, node, link, and source and drop type, click the **Advanced** tab and complete the following. If you do not want to make advanced filter selections, continue with Step 5.

a. If you made selections on the General tab, click **Yes** in the confirmation box to apply the settings.

b. In the Advanced tab of the Circuit Filter dialog box, set the following filter attributes as necessary:

- Ring—Choose the ring from the drop-down list.
- Node—Click the check boxes by each node in the network to filter circuits based on node.
- Link—Choose the desired link in the network.
- Source/Drop—Choose one of the following to filter circuits based on whether they have one or multiple sources and drops: **One Source and One Drop Only** or **Multiple Sources or Multiple Drops**.

Step 5 Click **OK**. Circuits matching the attributes in the Filter Circuits dialog box appear in the Circuits window.

Step 6 To turn filtering off, click the Filter icon in the lower right corner of the Circuits window. Click the icon again to turn filtering on.

Step 7 Return to your originating procedure (NTP).

DLP-F216 View Circuits on a Span

Purpose	This task views circuits on an ONS 15600 SDH span.
Tools/Equipment	None
Prerequisite Procedures	Chapter 6, “Create Circuits”
	DLP-F181 Log into CTC, page 16-34

Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From the View menu, choose **Go To Network View**. If you are already in network view, continue with Step 2.

Step 2 Right-click the green line (span) containing the circuits you want to view and choose one of the following:

- Circuits—To view MS-SPRing, SNCP, 1+1, or unprotected circuits on the span.
- PCA Circuits—To view circuits routed on an MS-SPRing protected channel. (This option does not appear if the span you right-clicked is not an MS-SPRing span.)

In the Circuits on Span dialog box, you can view the following information for all circuits provisioned on the span:

- VC—Displays VCs used by the circuits.
- SNCP—Indicates whether the circuit is in an SNCP.
- Circuit—Displays the circuit name.
- Switch State—(SNCP span only) Displays the switch state of the circuit, that is, whether any span switches are active. For SNCP spans, switch types include: CLEAR (no spans are switched), MANUAL (a Manual switch is active), FORCE (a Force switch is active), and LOCKOUT OF PROTECTION (a span lockout is active).

Note You can complete other procedures from the Circuits on Span dialog box. If the span is in an SNCP, you can switch the span traffic. See "DLP-F193 SNCP Protection Switching Test" task on page 16-51 for instructions. If you want to edit a circuit on the span, double-click the circuit. See the "DLP-F264 Edit SNCP Circuit Path Selectors" task on page 17-55 for instructions.

Step 3 Return to your originating procedure (NTP).

DLP-F217 Edit a Circuit Name

Purpose	This task edits a circuit name.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **Circuits** tab.

Step 2 Click the circuit you want to rename, then click **Edit**.

Step 3 In the General tab, click the **Name** field, and edit or rename the circuit. Names can be up to 48 alphanumeric and/or special characters.

Step 4 Click **Apply**.

Step 5 From File menu, choose **Close**.

Step 6 In the Circuits window, verify that the circuit was correctly renamed.

Step 7 Return to your originating procedure (NTP).

DLP-F218 Change Active and Standby Span Color

Purpose	This task changes the color of active (working) and standby (protect) circuit spans that appear on the detailed circuit map of the Edit Circuit window. By default, working spans are green and protect spans are purple.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **Circuit** tab.

Step 3 Complete one or more of the following steps, as required:

- To change the color of the active (working) span, continue with Step 4.
- To change the color of the standby (protect) span, continue with Step 5.
- To return active and standby spans to their default colors, continue with Step 6.

Step 4 Change the color of the active span:

a. In the Span Colors area, click the colored square located near the word Active.

b. In the Pick a Color dialog box, click the color for the active span. Click the **Reset** button if you want the active span to display the last applied (saved) color.

c. Click **OK** to close the Pick a Color dialog box.

d. If you want to change the standby span color, continue with Step 5. If not, click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box open.

Step 5 Change the color of the standby span:

a. In the Span Colors area, click the colored square located near the word Standby.

b. In the Pick a Color dialog box, click the color for the standby span. Click the **Reset** button if you want the standby span to display the last applied (saved) color.

c. Click **OK** to close the Pick a Color dialog box.

d. Click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box open.

Step 6 If you want to return the active and standby spans to their default colors:

a. From the Edit menu, choose **Preferences**.

b. In the Preferences dialog box, click the **Circuit** tab.

c. Click the **Reset to Defaults** button.

d. Click **Apply** and click **OK** to close the Preferences dialog box.

Step 7 Return to your originating procedure (NTP).

DLP-F219 Change IP Settings

Purpose	This task changes the IPv4 address, subnet mask, default router, DHCP access, firewall Internet Inter-ORB Protocol (IIOP) listener port, LCD IP display, IPv6 Address, Prefix Length, IPv6 Default Router, and SOCKS proxy server settings for the ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 DLP-F185 Provision IP Settings, page 16-38
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning** > **Network > General** tabs.

Step 2 Change any of the following:

- Node Address
- Default Router
- IPv6 Configuration
  - IPv6 Address
  - Prefix Length
  - IPv6 Default Router
- Subnet Mask Length
- Forward DHCP Request To
- TSC CORBA (IIOP) Listener Port
- Gateway Settings

See the "DLP-F185 Provision IP Settings" task on page 16-38 for detailed field descriptions.

Step 3 Click **Apply**.

If you changed any network fields that will cause the node to reboot, the Change Network Configuration confirmation dialog box appears. If you changed a Gateway Setting, a confirmation appropriate to the gateway field appears. Change in IPv6 configuration such as IPv6 Address, Prefix Length and IPv6 Default Router does not cause the node to reboot.

Step 4 If a confirmation dialog box appears, click **Yes**.

If you changed an IPv4 address, subnet mask length, or TCC CORBA (IIOP) Listener Port, both ONS TSC cards will reboot, one at a time. A TSC reboot causes a temporary loss of connectivity to the node, but traffic is unaffected.

Step 5 Confirm that the changes appear on the Provisioning > Network > General tab. If the changes do not appear, repeat the task.

Step 6 Return to your originating procedure (NTP).

DLP-F220 Modify a Static Route

Purpose	This task modifies a static route on the ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 DLP-F186 Create a Static Route, page 16-41
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network > Static Routing** tabs.

Step 2 Click the static route you want to edit.

Step 3 Click **Edit.**

Step 4 In the Edit Selected Static Route dialog box, enter the following:

- Mask
- Next Hop
- Cost

See the "DLP-F186 Create a Static Route" task on page 16-41 for detailed field descriptions.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-F221 Delete a Static Route

Purpose	This task deletes a static route from the ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** > **Static Routing** tabs.

Step 2 Click the static route you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-F222 Disable OSPF

Purpose	This task disables the OSPF routing protocol process for the LAN on the ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 DLP-F187 Set Up or Change Open Shortest Path First Protocol, page 16-42
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If the ONS 15600 SDH has interfaces (DCC or LAN) in multiple OSPF areas, at least one ONS 15600 SDH interface (DCC or LAN) must be in the backbone area 0.0.0.0.

Note When you are logged into a ONS 15600 SDH node, CTC will not allow both a DCC interface and a LAN interface in the same nonzero OSPF area.

Note Cisco recommends limiting the number of link-state packets (LSPs) that will be forwarded over the DCC interfaces.

Step 1 In node view, click the **Provisioning** > **Network** > **OSPF** tabs.

Step 2 In the OSPF on LAN area, uncheck **OSPF active on LAN**.

Step 3 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Note Disabling OSPF can cause the TSCs to reboot. This results in a temporary loss of connectivity to the node, but traffic is unaffected.

Step 4 Return to your originating procedure (NTP).

DLP-F223 Change the Network View Background Color

Purpose	This task changes the network view background color and the domain view background color (the area displayed when you open a domain).
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note If you modify background colors, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Right-click the network view or domain map area and choose **Set Background Color** from the shortcut menu.

Step 3 In the Choose Color dialog box, select a background color.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-F224 Change the Default Network View Background Map

Purpose	This task changes the default map of the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If you modify the background image, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

Step 1 From the Edit menu, choose **Preferences > Map** and check the **Use Default Map** check box.

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

Step 3 In the Defaults Selector area, choose **CTC** and then **network**.

Step 4 Click the **Default Value** field and choose a default map from the drop-down list. Map choices are: Germany, Japan, Netherlands, South Korea, United Kingdom, and the United States (default).

Step 5 Click **Apply**. The new default network map appears.

Step 6 Click **OK**.

Step 7 If the ONS 15600 SDH icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until the ONS 15600 SDH icons are visible. (You can also choose **Fit Graph to Window**.)

Step 8 If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.

Step 9 If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15600 SDH icons are displayed at the magnification you want.

Step 10 Return to your originating procedure (NTP).

DLP-F225 Apply a Custom Network View Background

Purpose	This task changes the background image of the CTC network view on your login workstation.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You can replace the network view background image with any JPEG or GIF image that is accessible on a local or network drive. If you want to position nodes on the map based on the node coordinates, you will need the longitudes and latitudes for the edges of the map. You can obtain the longitude and latitude for cities and zip codes from the U.S. Census Bureau U.S. Gazetteer website (www.census.gov/cgi-bin/gazetteer). If you will use your mouse to position nodes, coordinates for the image edges are not necessary. The change does not affect other CTC users.

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Right-click the network or domain map and choose **Set Background Image**.

Step 3 Click **Browse**. Navigate to the graphic file that you want to use as a background.

Step 4 Select the file. Click **Open**.

Step 5 Click **Apply** and then click **OK**.

Step 6 If the ONS 15600 SDH icons are not visible, right-click the network view and choose **Zoom Out**. Repeat this step until all the ONS 15600 SDH icons are visible.

Tip If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.

Step 7 If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15600 SDH icons are displayed at the magnification you want.

Step 8 At the network view, use the CTC toolbar Zoom buttons (or right-click the graphic area and select a Zoom command from the shortcut menu) to set the area of the image you want to view.

Step 9 Return to your originating procedure (NTP).

DLP-F226 Create Domain Icons

Purpose	This task creates a domain icon, which can be used to group ONS 15600 SDH icons in CTC network view for all users.
Tools/Equipment	None
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note Domains are visible to all users who log into the network.

Note To allow users of any security level to create local domains, that is, domains that are visible on the home CTC session only, Superusers can change the CTC.network.LocalDomainCreationAndViewing NE default value to TRUE. A TRUE value means that any user can maintain the domain information in his or her Preferences file, which means that domain changes will not affect other CTC sessions. (The default value is FALSE, meaning domain information affects all CTC sessions and only Superusers can create a domain or put a node into a domain.) See the "NTP-F244 Edit Network Element Defaults" procedure on page 14-34 to change NE default values.

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Right-click the network map and choose **Create New Domain** from the shortcut menu.

Step 3 When the domain icon appears on the map, click the map name and type the domain name.

Step 4 Press **Enter**.

Step 5 Return to your originating procedure (NTP).

DLP-F227 Manage Domain Icons

Purpose	This task manages CTC network view domain icons, including moving, renaming, and removing domains.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 DLP-F226 Create Domain Icons, page 17-23
Required/As needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Superuser

Note All domain changes, such as added or removed nodes, are visible to all users who log into the network.

Note To allow users of any security level to create local domains, that is, domains that are visible on the home CTC session only, Superusers can change the CTC.network.LocalDomainCreationAndViewing NE default value to TRUE. A TRUE value means that any user can maintain the domain information in his or her Preferences file, which means that domain changes will not affect other CTC sessions. (The default value is FALSE, meaning domain information affects all CTC sessions and only Superusers can create a domain or put a node into a domain.) See the "NTP-F244 Edit Network Element Defaults" procedure on page 14-34 to change NE default values.

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Locate the domain action you want in Table 17-1 and complete the appropriate steps.

Table 17-1 Managing Domains

Domain Action	Steps
Move a domain	Press **Ctrl** and drag and drop the domain icon to the new location.
Rename a domain	Right-click the domain icon and choose **Rename Domain** from the shortcut menu. Type the new name in the domain name field.
Add a node to a domain	Drag and drop the node icon on the domain icon.
Move a node from a domain to the network map	Open the domain and right-click a node. Select **Move Node Back to Parent View**.
Open a domain	Double-click the domain icon, right-click the domain, and choose **Open Domain**.
Return to network view	Right-click the domain view area and choose **Go To Parent View** from the shortcut menu.
Preview domain contents	Right-click the domain icon and choose **Show Domain Overview**. The domain icon shows a small preview of the nodes in the domain. To turn off the domain overview, right-click the overview and select **Show Domain Overview**.
Remove domain	Right-click the domain icon and choose **Remove Domain**. Any nodes residing in the domain are returned to the network map.

Step 3 Return to your originating procedure (NTP).

DLP-F228 Modify a 1+1 Protection Group

Purpose	This task modifies a 1+1 protection group for any optical port.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Protection** tabs.

Step 2 In the Protection Groups list, click the 1+1 protection group that you want to modify.

Step 3 In the Selected Group area, you can modify the following:

- Name
- Bidirectional switching
- Revertive
- Reversion time

Note The bidirectional switching and revertive settings must be identical at each end of the span.

See the "NTP-F138 Create a 1+1 Protection Group" procedure on page 4-10 for field descriptions.

Step 4 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-F229 Delete a 1+1 Protection Group

Purpose	This task deletes a 1+1 protection group for any optical port.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From node view, click the **Provisioning** > **Protection** tabs.

Step 2 In the Protection Groups list, click the 1+1 protection group that you want to delete.

Step 3 Click **Delete**. The Delete Protection Group window appears.

Step 4 Click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-F230 Change the Node Timing Source

Purpose	This task changes the SDH timing source for the ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution The following procedure might be service affecting; complete during a scheduled maintenance window.

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 In the General Timing area, change any of the following information:

- Timing Mode
- Revertive
- Revertive Time

For detailed descriptions of these fields, see the "NTP-F137 Set Up Timing" procedure on page 4-9.

Step 3 In the Reference Lists area, you can change the NE Reference.

Step 4 Click the **BITS Facilities** tab. In the BITS In area, you can change the following information:

Note The BITS Facilities area sets the parameters for your BITS1 and BITS2 timing references. Many of these settings are determined by the timing source manufacturer.

- Facility Type
- BITS State
- Coding
- Framing
- Sync. Messaging
- Admin SSM
- Sa Bit
- Cable Type

Step 5 In the BITS Out area, you can change the following information:

- Facility Type
- BITS State
- Coding

- Framing
- AIS Threshold
- Sa Bit
- Cable Type

Step 6 Click **Apply**.

Note Both TSCs must acquire the new clock. The UNPROT-SYNCCLK alarm will occur for 700 seconds, and both TSCs will report the FSTSYNC alarm for the same period of time. This is normal.

Step 7 Return to your originating procedure (NTP).

DLP-F231 Delete a User from a Single Node

Purpose	This task deletes an existing user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 DLP-F269 Change User Password and Security Levels for a Single Node, page 17-61
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, select the **Provisioning** > **Security > Users** tabs.

Step 2 Choose the user you want to delete.

Step 3 Click **Delete**. The Delete User dialog box appears.

Step 4 Verify that you selected the correct user to delete and click **OK**.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-F232 Delete a User From Multiple Nodes

Purpose	This procedure deletes an existing user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 DLP-F270 Change User and Security Settings for Multiple Nodes, page 17-62

Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note Users who are logged in when you delete them will not be logged out. The delete user action will take effect after the user logs out. To log out a user while they are logged in, complete the "DLP-F272 Log Out a User on Multiple Nodes" task on page 17-63.

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Provisioning** > **Security > Users** tabs.

Step 3 Choose the user that you want to delete.

Step 4 Click **Delete**. The Delete User dialog box appears.

Step 5 In the Select Applicable Nodes area, uncheck any nodes where you do not want to delete this user.

Step 6 Click **OK**. The User Deletion Results confirmation dialog box appears.

Step 7 Click **OK**. Confirm that the changes appear; if not, repeat the task.

Step 8 Return to your originating procedure (NTP).

DLP-F233 Modify SNMP Trap Destinations

Purpose	This task modifies Simple Network Management Protocol (SNMP) trap destinations on an ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **SNMP** tabs.

Step 2 Click a trap in the Trap Destinations list box.

For a description of SNMP traps, refer to the "SNMP" chapter of the *Cisco ONS 15600 SDH Reference Manual*.

Step 3 In the Selected Destination area, complete as needed:

- Type the SNMP community name in the Community Name field.

  Note The community name is a form of authentication and access control. The community name assigned to the ONS 15600 SDH is case-sensitive and must match the community name of the network management system (NMS).

Note The default UDP port for SNMP is 162.

- Set the Trap Version field to either SNMPv1 or SNMPv2.

  Refer to your NMS documentation to determine whether to use SNMPv1 or SNMPv2.

Step 4 If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If this box is not checked, SET requests are rejected.

Step 5 Click **Apply**. SNMP settings are now configured.

Step 6 To view SNMP information for each node, click the node IP address in the Trap Destinations list.

Step 7 Return to your originating procedure (NTP).

DLP-F234 Delete SNMP Trap Destination

Purpose	This task deletes an SNMP trap destination on an ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **SNMP** tabs.

Step 2 Click the trap that you want to delete in the Trap Destination list box.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Confirm that the changes are correct and click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-F235 Switch All SNCP Circuits on a Span

Purpose	This task applies a FORCE external switching command to all circuits on an SNCP span. The FORCE switches the traffic to another span.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go To Network View.**

Step 2 Right-click the span where you want to switch SNCP traffic.

Step 3 Choose **Circuits** from the shortcut menu.

Step 4 In the Circuits on Span dialog box, select **Force**.

⚠ **Caution** The FORCE command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

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

In the Circuits on Span dialog box, the Switch State listed for all circuits is FORCE.

Step 6 Return to your originating procedure (NTP).

DLP-F236 Clear a Switch for all SNCP Circuits on a Span

Purpose	This task clears a Force traffic switch for all circuits on an SNCP span.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Right-click the span where you want to clear the switch.

Step 3 Choose **Circuits** from the shortcut menu.

Step 4 In the Circuits on Span dialog box, select **CLEAR** to remove a previously set switch command.

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

In the Circuits on Span dialog box, the Switch State listed for all circuits is CLEAR.

Step 6 Return to your originating procedure (NTP).

DLP-F237 Verify Timing in a Reduced Ring

Purpose	This task verifies timing in a reduced ring.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite/remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 Observe the Timing Mode field to see the type of timing (Line, External) that has been set for that node.

Step 3 Scroll down to the Reference Lists and observe the NE Reference fields to see the timing references provisioned for that node.

Step 4 If the removed node was the BITS timing source, perform the following:

a. Look for another node on the ring that can be used as a BITS source and set that node's Timing Mode to **External**. Choose that node as the primary timing source for all other nodes in the ring. See the "DLP-F230 Change the Node Timing Source" task on page 17-26.

b. If no node in the reduced ring can be used as a BITS source, choose one node to be your internal timing source. Set that node's Timing Mode to **External** and set the BITS 1 and 2 State to **Locked**. Then choose line timing for all other nodes in the ring. This will force the first node to be their primary timing source. See the "DLP-F230 Change the Node Timing Source" task on page 17-26.

Note This type of timing conforms to Stratum 3E requirements and is not considered optimal.

Step 5 If the removed node was not the BITS timing source, provision the adjacent nodes to line timing using SDH links (east and west) as timing sources, traceable to the node with external BITS timing.

Step 6 Return to your originating procedure (NTP).

DLP-F238 Initiate a Manual Switch on a Port in a 1+1 Protection Group

Purpose	This procedure applies the Manual external switching command to a 1+1 protection scheme.
Tools/Equipment	Installed optical (STM-N) cards
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Group area, select the protection group with the port you want to switch.

In the Selected Group area each port is identified as Working or Protect. Each port also has a status:

- Active—The port is carrying traffic.
- Standby—The port is not carrying traffic.
- [MANUAL TO WORKING]—A Manual switch has moved traffic to the Working port.
- [MANUAL TO PROTECT]—A Manual switch has moved traffic to the Protect port.
- [FORCE TO WORKING]—A Force switch has moved traffic to the Working port.
- [FORCE TO PROTECT]—A Force switch has moved traffic to the Protect port.

The normal assignment status is for one port assignment to say Working/Active and for the other to say Protect/Standby.

Step 3 In the Selected Group, click the port that you want to switch. For example, if you want to switch traffic from the working port to the protect port, click the working port.

Step 4 Click **Manual**.

If the Manual switch is successful, CTC shows both ports as [MANUAL TO PROTECT] (or [MANUAL TO WORKING]). This indicates that the ONS 15600 SDH system has been able to carry out the switch request and has moved traffic from one port to the other.

If the Bidirectional switching check box is checked, both the near-end and far-end nodes switch to the designated protection ports. For example, if the near-end node has a loss of signal (LOS), it switches to the protect port and transmits a switch request to the far-end node to switch to the protect port also. This ensures that both nodes process traffic from the same span.

If the Bidirectional switching check box is not selected, the near-end and far-end nodes switch independently of each other. For example, if the near-end node has an LOS on its working port, it switches to the protect port. If the far-end node does not have a LOS, traffic remains on the working port.

If the Manual switch is not successful, CTC continues to show the ports as active and standby, and an alarm such as FAILTOSWS is raised. This failure occurs because the target port is not available and troubleshooting is required. For information about troubleshooting, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Step 5 Click the **Conditions** tab and click **Retrieve** to see new events. The switch procedure raises a MANUAL-REQ-SPAN condition that is visible in the window unless Not Alarmed conditions have been filtered out from the view.

Step 6 Click the **Alarms** tab.

If any traffic loss alarms occur or if a switching failure alarm such as FAILTOSWS occurs, troubleshoot the problems that have prevented the switch and attempt the switch procedure again.

Step 7 Return to your originating procedure (NTP).

DLP-F239 Initiate a Force Switch on a Port in a 1+1 Protection Group

Purpose	This task applies the Force external switching command to a 1+1 protection scheme.
Tools/Equipment	Installed STM-N cards
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Group area, select the protection group with the port you want to switch.

In the Selected Group area, each port is identified as Working or Protect. Each port also has a status:

- Active—The port is carrying traffic.

- Standby—The port is not carrying traffic.
- [MANUAL TO WORKING]—A Manual switch has moved traffic to the working port.
- [MANUAL TO PROTECT]—A Manual switch has moved traffic to the protect port.
- [FORCE TO WORKING]—A Force switch has moved traffic to the working port.
- [FORCE TO PROTECT]—A Force switch has moved traffic to the protect port.

The normal status is for one port to be Working/Active and the other to be Protect/Standby.

Step 3 In the Selected Group area, select the port that you want to switch. For example, if you want to switch traffic from the working port to the protect port, click the working port.

Step 4 Click **Force**.

If the Force switch is successful, Cisco Transport Controller (CTC) shows both ports as [FORCE TO PROTECT] (or [FORCE TO WORKING]). This indication is shown whether or not the ONS 15600 SDH system has been able to move traffic from one port to the other.

If the Bidirectional switching check box is checked, both the near-end and far-end nodes switch to the designated protection ports. For example, if the near-end node has a loss of signal (LOS), it switches to the protection port and transmits a switch request to the far-end node to switch to the protection port also. This ensures that both nodes process traffic from the same span.

If the Bidirectional switching check box is not selected, the near-end and far-end nodes switch independently of each other. For example, if the near-end node has an LOS on its working port, it switches to the protection port. If the far-end node does not have a LOS, traffic remains on the working port.

If the Force switch is unsuccessful, clear the switch immediately using the "DLP-F295 Clear a Manual or Force Switch in a 1+1 Protection Group" task on page 17-86, and then troubleshoot the problems preventing the switch by referring to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Step 5 Click the **Conditions** tab and click **Retrieve** to see new events. The switch procedure raises a FORCED-REQ-SPAN condition that is visible in the window unless Not Alarmed conditions have been filtered out from the view.

Step 6 Click the **Alarms** tab.

No new traffic loss alarms or failure-to-switch alarms should appear.

Step 7 Return to your originating procedure (NTP).

DLP-F240 Apply a Lock On in a 1+1 Group

Purpose	This task locks traffic onto a working port to prevent traffic from switching to the protect port in a protection group.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note A lock on can be applied to a working port only.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, select the protection group where you want to apply a lock-on.

Step 3 If you determine that the protect port is in standby and you want to apply the lock-on to the protect port, make the protect port active:

- **a.** In the Selected Group field, click the protect port.
- **b.** In the Switch Commands field, click **Force**.

Step 4 In the Selected Group area, choose the active port where you want to lock on traffic.

Step 5 In the Inhibit Switching field, click **Lock On**.

Step 6 Click **Yes** in the confirmation dialog box.

The lock on has been applied and traffic cannot be switched from that port. See the "DLP-F296 Clear a Lock On or Lockout in a 1+1 Protection Group" task on page 17-86 as needed.

Step 7 Return to your originating procedure (NTP).

DLP-F241 Apply a Lockout in a 1+1 Group

Purpose	This task locks traffic out of a protect port in a 1+1 protection group, which prevents traffic from switching to that port.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note A lockout can be applied to a protect port only.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups field, click the protection group that contains the card you want to lock out.

Step 3 In the Selected Group area, select the card you want to lock out.

Step 4 In the Inhibit Switching field, click **Lock Out**.

Step 5 Click **Yes** in the confirmation dialog box.

The lock out has been applied and traffic is switched to the opposite card. To clear the lockout, see the "DLP-F296 Clear a Lock On or Lockout in a 1+1 Protection Group" task on page 17-86.

Step 6 Return to your originating procedure (NTP).

DLP-F242 Initiate a Manual Switch on an SNCP Circuit

Purpose	This task switches traffic to the protect SNCP path using a Manual switch. A Manual switch will switch traffic if the path has an error rate less than the signal degrade.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Circuits > Circuits** tabs.

Step 2 Click the path you want to switch and then click **Edit**.

Step 3 In the Edit Circuit window, click the **SNCP Selectors** tab.

Step 4 In the Switch State column, click the row for the path you want to switch and select **Manual to Protect** or **Manual to Working** as appropriate.

Step 5 Click **Apply**.

Step 6 To verify that the switch has occurred, view the SNCP Selectors tab Switch State column. The row for the circuit you switched will show a MANUAL status.

Traffic switches from the working SNCP path to the protect path. If the path is configured for revertive switching, the traffic reverts to the working path when the Manual switch is cleared. See the "DLP-F298 Clear a Switch or Lockout on an SNCP Circuit" task on page 17-88 as needed.

Step 7 Return to your originating procedure (NTP).

DLP-F243 Initiate a Force Switch to an SNCP Circuit

Purpose	This task switches traffic to the working SNCP circuit using a Force switch. 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.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Circuits > Circuits** tabs.

Step 2 Click the path you want to switch and click **Edit**.

Step 3 In the Edit Circuit window, click the **SNCP Selectors** tab.

Step 4 In the Switch State column, click the row for the path you want to switch and select **Force to Working** or **Force to Protect** as appropriate.

Step 5 Click **Apply**.

Step 6 To verify that the switch has occurred, view the SNCP Selectors tab Switch State column. The circuit row shows a FORCE status.

Traffic switches from the protect path to the working path. Protection switching cannot occur until the Force switch is cleared. See the "DLP-F298 Clear a Switch or Lockout on an SNCP Circuit" task on page 17-88 as needed.

Step 7 Return to your originating procedure (NTP).

DLP-F244 Create a DCC Tunnel

Purpose	This task creates a data communications channel (DCC) tunnel to transport traffic from third-party SDH equipment across ONS 15600 SDH networks. Tunnels can be created on the RS-DCC channel (D1-D3) (if not used by a node as a terminated DCC), or any MS-DCC channel (D4-D6, D7-D9, or D10-D12).
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 NTP-F144 Verify Node Turn-Up, page 5-2 NTP-F209 Modify or Delete Communications Channel Terminations, page 11-8, as needed
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The ONS 15600 SDH can support up to 64 DCC tunnels. Terminated RS-DCCs cannot be used as DCC tunnel endpoints, and an RS-DCC that is used as a DCC tunnel endpoint cannot be terminated. You must delete the terminated RS-DCCs in a path before creating a DCC tunnel. All DCC tunnel connections are bidirectional.

Step 1 In network view, click the **Provisioning > Overhead Circuits** tabs.

Step 2 Click **Create**.

Step 3 In the Circuit Creation dialog box, provision the DCC tunnel:

- Name—Type the tunnel name.
- Type—Choose one:
  - **DCC Tunnel - D1-D3**—Allows you to choose either the RS-DCC (D1-D3) or a MS-DCC (D4-D6, D7-D9, or D10-D12) as the source or destination endpoints.
  - **DCC Tunnel - D4-D12**—Provisions the full MS-DCC as a tunnel.

Step 4 In the Source area, complete the following:

- Node—Choose the source node.

- Slot—Choose the source slot.
- Port—Choose the source port.
- Channel—Shown if you chose DCC Tunnel-D1-D3 as the tunnel type. Choose one of the following:
  - **DCC1 (D1-D3)**—RS-DCC
  - **DCC2 (D4-D6)**—MS-DCC 1
  - **DCC3 (D7-D9)**—MS-DCC 2
  - **DCC4 (D10-D12)**—MS-DCC 3

  DCC options do not appear if they are used by the ONS 15600 SDH (DCC1) or other tunnels.

Step 5 In the Destination area, complete the following:

- Node—Choose the destination node.
- Slot—Choose the destination slot.
- Port—Choose the destination port.
- Channel—Shown if you chose DCC Tunnel-D1-D3 as the tunnel type. Choose one of the following:
  - **DCC1 (D1-D3)**—RS-DCC
  - **DCC2 (D4-D6)**—MS-DCC 1
  - **DCC3 (D7-D9)**—MS-DCC 2
  - **DCC4 (D10-D12)**—MS-DCC 3

  DCC options do not appear if they are used by the ONS 15600 SDH (DCC1) or other tunnels.

Step 6 Click **Finish**.

Step 7 Put the ports that are hosting the DCC tunnel in service. See the "DLP-F254 Change the Service State for a Port" task on page 17-48 for instructions.

Step 8 Return to your originating procedure (NTP).

DLP-F245 Clean Fiber Connectors

Purpose	This task cleans the fiber connectors.
Tools/Equipment	Inspection microscope (suggested: Westover FBP-CIS-1) Desktop hand tool Scrub tool 3M high-performance fiber-optic wipes Compressed air/duster
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note Replace all dust caps whenever the equipment will be unused for 30 minutes or more.

Step 1 Remove the dust cap from the fiber connector.

Step 2 To use the desktop hand tool:

a. Advance the 3M high-performance fiber-optic wipe in the desktop hand tool to access the unused wipe area.

Note To replace the fiber-optic wipe in the desktop hand tool, remove the frame cover. Put a new wipe over the base of the desktop hand tool with the stitching of the wipe aligned lengthwise with the tool. Place the frame cover on the tool and press firmly to reattach.

b. Place the connector tip at the top of the slot at a slight angle. In a single stroke, move the connector down the wipe without lifting the connector from the wipe. Before lifting the connector from the wipe, straighten the connector.

c. Repeat the single stroke motion on each side of the alignment pins to clean the entire connector face.

d. Blow off any wipe lint left on the fiber connector using the compressed air.

Step 3 To use the scrub tool:

a. Connect the grounding strap to the scrub tool and to suitable ground.

b. Install or replace the scrub wipe in the scrub tool with a new wipe. Avoid handling the wipe excessively.

c. Scrub between the alignment pins of the fiber connector, and then wipe around the outside of each alignment pins.

Step 4 Inspect the connector for cleanliness. Repeat Steps 2 and 3 as necessary.

Step 5 Replace the dust cap on the fiber connector until ready for use.

Step 6 Return to your originating procedure (NTP).

DLP-F246 Clean the Fiber Adapters

Purpose	This task cleans the fiber adapters.
Tools/Equipment	Inspection microscope (suggested: Westover FBP-CIS-1) Scrub tool Grounding strap Wipes Rinse tool HFE-based cleaning fluid and pump head assembly Replacement scrub tool wipes Replacement rinse tool absorbent pads Empty disposable container
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Remove the dust plugs from the fiber adapter.

Step 2 To remove stubborn particles from the fiber adapter:

a. Connect the grounding strap to the scrub tool and to suitable ground.

b. Install or replace the scrub wipe in the scrub tool with a new wipe. Avoid handling the wipe excessively.

c. Insert the scrub tool tip into the fiber adapter.

d. Remove and insert the scrub tool tip several times to clean the fiber adapter.

Step 3 To remove loose particles from the fiber adapter:

a. Remove the dust cap from the rinse tool.

Note If the absorbent pad on the rinse tool needs replacement, slide the old pad and mesh retainer off of the rinse tool tube. Slide the new absorbent pad and mesh retainer over the rinse tip onto the rinse tool tube. Roll the absorbent pad and mesh retainer between your hands until the opening on the absorbent pad is closed. Discard the old absorbent pad and mesh retainer.

b. Connect the grounding strap to the rinse tool and to suitable ground.

c. Connect the rinse tool to the HFE-based cleaning fluid bottle and pump head assembly.

d. Turn the aluminum nozzle on the pump one-half turn counterclockwise and squirt the cleaning fluid into an empty container to soak the rinse tool.

e. Remove the dust cover from the fiber adapter.

f. Insert the rinse tool tip into the fiber adapter with the bent part of the handle pointing downwards. Squirt twice.

g. Remove the rinse tool and replace the dust cover on the adapter. Replace the dust cap on the rinse tool.

h. Turn the aluminum nozzle on the pump clockwise until it is tight and disconnect the HFE bottle from the pump.

Step 4 Inspect the fiber adapter to ensure it is clean. If it is not clean, repeat Steps 2 and 3.

Step 5 Replace the dust plug in the fiber adapter until ready for use.

Step 6 Return to your originating procedure (NTP).

DLP-F247 Verify that a 1+1 Working Port is Active

Purpose	This task verifies that a working slot in a 1+1 protection scheme is active (and that the protect slot is in standby).
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Selected Group area, verify that the working slot/port is shown as Working/Active. If so, this task is complete.

Step 3 If the working slot says Working/Standby, perform a Manual switch on the working port:

a. In the Selected Group area, choose the Protect/Active port.

b. In the Switch Commands field, choose **Manual**.

c. Click **Yes** in the confirmation dialog box.

Step 4 Verify that the working slot is carrying traffic (Working/Active).

Note If the slot is not active, look for conditions or alarms that might be preventing the card from carrying working traffic. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for procedures to clear alarms.

Step 5 When the working port is carrying traffic, clear the Manual switch:

a. In the Switch Commands field, choose **Clear**.

b. Click **Yes** in the confirmation dialog box.

Step 6 Verify that the working port does not revert to Standby, which might indicate a problem on the working span.

Step 7 Return to your originating procedure (NTP).

DLP-F248 Drill Holes to Anchor and Provide Access to the Bay Assembly

Purpose	This task describes how to use the floor template to locate and drill the appropriate holes that are needed to anchor and provide additional access to the bay assembly at your site.
Tools/Equipment	Floor template (53-2141-XX) Marking pen Concrete drill Reciprocating saw
Prerequisite Procedures	NTP-F108 Unpack and Inspect the ONS 15600 SDH Bay Assembly, page 1-4
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note If the bay will use wide cable routing modules (CRMs) for cable routing, you need to use 900-mm (35.4-in) spacing between bays.

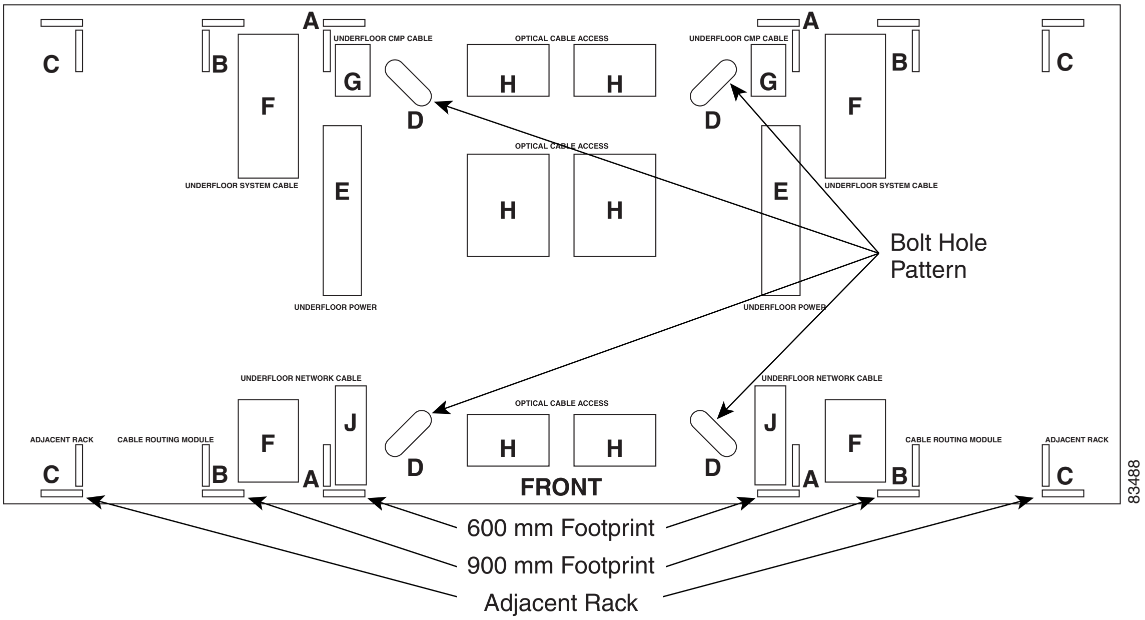
Step 1 Determine the proper location of your bay:

a. For a 900-mm (35.4-inch) wide bay, position the floor template so that corner indicators “B” fall where you want the corners of the bay to reside (Figure 17-4).

b. For a 600-mm (23.6-inch) wide bay, position the floor template so that corner indicators “A” fall where you want the corners of the bay to reside (Figure 17-4).

Note If space allows, Cisco recommends you reserve an additional 1/4 inch (6.35 mm) of space on each side of the bay assembly you are installing.

Figure 17-4 Floor Template



Step 2 Use the corner indicators "C" to determine the closest recommended position of an adjacent 900-mm (35.4-inch) bay assembly.

Step 3 Use a marking pen to mark the floor with the corner indicators appropriate to your installation.

Step 4 At the four locations marked "D," drill floor bolt holes according to the bolt manufacturer's recommendation for bolt hole size.

Step 5 If you will use under-floor power, use the drill and saw to cut out the rectangular floor areas marked "E."

Step 6 If you will route optical cables in a 900-mm (35.4-inch) bay from under the floor, use the drill and saw to cut out the rectangular floor areas marked "F."

Step 7 If you will route optical cables in a 600-mm (23.6-inch) bay from under the floor, use the drill and saw to cut out the rectangular floor areas marked "J."

Step 8 If you will route any timing, alarm, or LAN cables through the floor to the customer access panel (CAP), use the drill to cut out the floor areas marked "G."

Step 9 (Optional.) If you want to create other access holes for under-floor access (for AC power, for example), use the reciprocating saw to cut sufficient holes within any of the locations marked "H."

Step 10 Return to your originating procedure (NTP).

DLP-F249 Assign a Name to a Port

Purpose	This task assigns a name to a port on any ONS 15600 SDH card.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 NTP-F131 Verify Card Installation, page 4-2

Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Double-click the card that has the port you want to provision.

Step 2 Click the **Provisioning** tab.

Step 3 Click the **Port Name** column for the port number you are assigning a name to and enter the desired port name.

The port name can be up to 32 alphanumeric/special characters and is blank by default.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-F250 Provision SNCP Selectors During Circuit Creation

Purpose	This task provisions SNCP selectors during circuit creation. Use this task only if the circuit will be routed on an SNCP.
Tools/Equipment	None
Prerequisite Procedures	You must have the Circuit Creation wizard open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Provisioning signal degrade–path (SD-P) or signal fail–path (SF-P) thresholds in the Circuit Attributes page of the Circuit Creation wizard sets the values only for SNCP-protected spans. The circuit source and destination use the node default values of 10E-4 for SD-P and 10E-6 for SF-P for unprotected circuits and for the source and drop of SNCP circuits.

Step 1 In the Circuit Attributes area of the Circuit Creation wizard, set the SNCP path selectors:

- Provision working go and return on primary path—Check this box to route the working path on one fiber pair and the protect path on a separate fiber pair. This feature only applies to bidirectional SNCP circuits.
- Revertive—Check this box if you want traffic to revert to the working path when the conditions that diverted it to the protect path are repaired. If you do not choose Revertive, traffic remains on the protect path after the switch.
- Reversion time—If Revertive is checked, click the Reversion time field and choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working path. Traffic can revert when conditions causing the switch are cleared.
- SF threshold—For high-order circuits, set the SNCP path-level signal failure bit error rate (BER) thresholds.
- SD threshold—For high-order circuits, set the SNCP path-level signal degrade BER thresholds.

- Switch on PDI-P—For high-order circuits, check this box if you want traffic to switch when a high-order payload defect indication–path is received. Unavailable for low-order circuits.

Step 2 Return to your originating procedure (NTP).

DLP-F251 Provision a Half Circuit Source and Destination on an MS-SPRing or 1+1 Protection Group

Purpose	This task provisions a half circuit source and destination for MS-SPRings and 1+1 protection groups.
Tools/Equipment	None
Prerequisite Procedures	NTP-F168 Create a Half Circuit on an MS-SPRing or 1+1 Node, page 6-17
	The Source page of the Circuit Creation wizard must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Node drop-down list, choose the node that will contain the half circuit.

Step 2 From the Slot drop-down list, choose the slot containing the card where the circuit will originate.

Step 3 From the Port drop-down list, choose the port where the circuit will originate.

Step 4 Click **Next**.

Step 5 From the Node drop-down list, choose the node chosen in Step 1.

Step 6 From the Slot drop-down list, choose the STM-N card to map the STM-N high-order circuit to a virtual container (VC).

Step 7 Choose the destination VC from the additional drop-down lists that appear based on your choices.

Step 8 Return to your originating procedure (NTP).

DLP-F252 Provision a Half Circuit Source and Destination on an SNCP

Purpose	This task provisions a half circuit source and destination for an SNCP ring. This task is used to create SNCP selectors on the node. Depending on the specific network configuration, the SNCP selector can be created on the source side (two sources, one destination); the destination side (one source, two destinations); or both (two sources, two destinations). Selectors are required on both the source and destination sides when two VC SNCP paths (rings) are interconnected at a single node.
Tools/Equipment	None
Prerequisite Procedures	NTP-F169 Create a Half Circuit on an SNCP Node, page 6-19 The Source page of the Circuit Creation wizard must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Node drop-down list, choose the node that will contain the half circuit.

Step 2 From the Slot drop-down list, choose the slot containing the card where the circuit will originate.

Step 3 From the Port drop-down list, choose the port where the circuit will originate. This field might not be available, depending on the card chosen in Step 2.

Step 4 Complete one of the following:

- For low-order VC12 circuits, choose VC4, TUG3, TUG2, and VC12.
- For low-order VC11 circuits, choose VC4, TUG3, TUG2, and VC11.
- For low-order VC3 circuits, choose VC4 and VC3.
- For high-order circuits, choose VC4.

Step 5 If you want to create an SNCP ring with two sources, click **Use Secondary Source** and repeat Steps 1 through 4. If not, skip this step and continue with Step 6.

Step 6 Click **Next**.

Step 7 From the Node drop-down list, choose the node chosen in Step 1.

Step 8 From the Slot drop-down list, choose the optical (STM-N) card to map the low-order VC3, VC11, or VC12 circuit for optical transport or to map the VC4 circuit to a synchronous transport module (STM).

Step 9 From the Port drop-down list, choose the destination port.

Step 10 If applicable, choose the destination VC.

Step 11 If you want to create an SNCP ring with two destinations, click **Use Secondary Destination** and repeat Steps 7 through 10.

Step 12 Return to your originating procedure (NTP).

DLP-F253 Provision RS-DCC Terminations

Purpose	This task creates SDH RS-DCC terminations required for alarms, administration data, signal control information, and messages.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Comm Channels > RS-DCC** tabs.

Step 2 In the RS-DCC Terminations area, click **Create**.

Step 3 In the Create RS-DCC Terminations dialog box, click the ports where you want to create the DCC termination. To select more than one port, press the **Shift** key or the **Ctrl** key.

Note RS-DCC refers to the regenerator-section DCC, which is used for ONS 15600 SDH DCC terminations. You can provision the SDH MS-DCCs and RS-DCC (when not used as a DCC termination by the ONS 15600 SDH) as DCC tunnels. See the "DLP-F244 Create a DCC Tunnel" task on page 17-36.You can provision RS-DCCs and MS-DCCs on different ports in the same node. In the Port Admin State area, click **Set to unlocked** to put the port in service. When RS-DCC is provisioned, an MS-DCC termination is allowed on the same port, but is not recommended. Changing configuration of a port having RS-DCC termination to MS-DCC termination is allowed. During this upgrade both MS-DCC and RS-DCC terminations can be present on the same port. Once the MS-DCC termination is configured see "DLP-F314 Provision MS-DCC Terminations" task on page 18-14, delete the RS-DCC terminations as specified in"DLP-F321 Delete an RS-DCC Termination" task on page 18-20, and enable the OSPF on MS-DCC termination if not enabled see "DLP-F320 Change an MS-DCC Termination" task on page 18-19

Step 4 Verify that the Disable OSPF on RS-DCC Link is unchecked.

Step 5 If the RS-DCC termination is to include a non-ONS node, check the **Far End is Foreign** check box. This automatically sets the far-end node IP address to 0.0.0.0, which means that any address can be specified by the far end. To change the default to a specific the IP address, see the "DLP-F319 Change an RS-DCC Termination" task on page 18-19.

Step 6 In the Layer 3 area, perform one of the following:

- Check the IP box only—If the RS-DCC is between the ONS 15600 SDH and another ONS node and only ONS nodes reside on the network. The RS-DCC will use Point-to-Point Protocol (PPP).
- Check the IP and OSI boxes—If the RS-DCC is between the ONS 15600 SDH and another ONS node and third party NEs that use the Open System Interconnection (OSI) protocol stack are on the same network. The RS-DCC will use PPP.
- Check OSI box only—If the RS-DCC is between an ONS node and a third party NE that uses the OSI protocol stack. The RS-DCC will use the Link Access Protocol on the D Channel (LAP-D) protocol.

Note If OSI is checked and IP is not checked (LAP-D), no network connections will appear in network view.

Step 7 If you checked OSI, complete the following steps. If you checked IP only, continue with Step 9.

a. Click **Next**.

b. Provision the following fields:

- Router—Choose the OSI router.
- ESH—Sets the End System Hello (ESH) propagation frequency. End system NEs transmit ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- ISH—Sets the Intermediate System Hello (ISH) PDU propagation frequency. Intermediate system NEs send ISHs to other ESs and ISs to inform them about the IS NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- IIH—Sets the Intermediate System to Intermediate System Hello (IIH) PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
- Metric—Sets the cost for sending packets on the LAN subnet. The IS-IS protocol uses the cost to calculate the shortest routing path. The default metric cost for LAN subnets is 20. It normally should not be changed.

Step 8 If the OSI and IP boxes are both checked, continue with Step 9. If only the OSI is checked, click **Next** and provision the following fields:

- Mode
  - AITS—(Acknowledged Information Transfer Service) (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.
  - UITS—(Unacknowledged Information Transfer Service) Transfers frames containing user data with no acknowledgement. The service does not guarantee that the data presented by one user will be delivered to another user, nor does it inform the user if the delivery attempt fails. It does not provide any flow control or error control mechanisms.
- Role—Set to the opposite of the mode of the NE at the other end of the RS-DCC.
- MTU—(Maximum transmission unit) Sets the maximum number of octets in a LAP-D information frame. The range is 512 to 1500 octets. The default is 512. You normally should not change it.
- T200— Sets the time between Set Asynchronous Balanced Mode (SABME) frame retransmissions. The default is 0.2 seconds. The range is 0.2 to 20 seconds.
- T203—Provisions the maximum time between frame exchanges, that is, the trigger for transmission of the LAP-D “keep-alive” Receive Ready (RR) frames. The default is 10 seconds. The range is 4 to 120 seconds.

Step 9 Click **Finish**.

Step 10 Return to your originating procedure (NTP).

DLP-F254 Change the Service State for a Port

Purpose	This task puts a port in service or removes a port from service.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the card with the port(s) you want to put in or out of service. The card view appears.

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

Step 3 In the Admin State column for the target port, choose one of the following from the drop-down list:

- **Unlocked**—Puts the port in the Unlocked-enabled service state.
- **Locked,disabled**—Puts the port in the Locked-enabled,disabled service state. In this service state, traffic is not passed on the port until the service state is changed to Unlocked-enabled; Locked-enabled,maintenance; or Unlocked-disabled,automaticInService.
- **Locked,maintenance**—Puts the port in the Locked-enabled,maintenance service state. This service state does not interrupt traffic flow and loopbacks are allowed, but alarm reporting is suppressed. Raised fault conditions, whether or not their alarms are reported, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command. Use the Locked-enabled,maintenance service state for testing or to suppress alarms temporarily. A port must be in this service state before you can apply a loopback. Change to the Unlocked-enabled or Unlocked-disabled,automaticInService when testing is complete.
- **Unlocked,automaticInService**—Puts the port in the Unlocked-disabled,automaticInService service state. In this service state, alarm reporting is suppressed, but traffic is carried and loopbacks are allowed. After the soak period passes, the port changes to Unlocked-enabled. Raised fault conditions, whether their alarms are reported or not, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command.

Note CTC will not allow you to change a port service state from Unlocked-enabled to Locked-enabled,disabled. You must first change a port to the Locked-enabled,maintenance service state before putting it in the Locked-enabled,disabled service state.

For more information about service states, refer to the “Administrative and Service States” appendix of the *Cisco ONS 15600 SDH Reference Manual*.

Step 4 If the port is in loopback (Locked-enabled,loopback & maintenance) and you set the Admin State to Unlocked-enabled, a confirmation window appears indicating that the loopback will be released and that the action could be service affecting. To continue, click **Yes**.

Step 5 If you set Admin State to Unlocked,automaticInService, set the soak period time in the AINS Soak field. This is the amount of time that the port will stay in Unlocked-disabled,automaticInService service state after the signal is continuously received before changing to Unlocked-enabled.

Step 6 Click **Apply**.

Step 7 As needed, repeat this task for each port.

Step 8 Return to your originating procedure (NTP).

DLP-F255 Remap the K3 Byte

Purpose	This task provisions the K3 byte. Do not remap the K3 byte unless specifically required to run an ONS 15600 SDH MS-SPRing through third-party equipment. This task is unnecessary for most users.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution If you remap the K3 byte, remap to the same extended byte (Z2, E2, or F1) on either side of the span.

Step 1 In node view, double-click the card that connects to the third-party equipment.

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

Step 3 Click **MS-SPRing Ext Byte** and choose the alternate byte: Z2, E2, or F1.

Step 4 Click **Apply**.

Step 5 Repeat Steps 1 through 4 at the node and card on the other end of the MS-SPRing span.

Note The extension byte set in Step 3 should match at both ends of the span.

Step 6 Return to your originating procedure (NTP).

DLP-F256 Set Auto-Refresh Interval for Displayed PM Counts

Purpose	This task changes the window auto-refresh intervals for updating the PM counts.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an STM-N or Ethernet port. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 From the **Auto-refresh** drop-down list choose one of the following options:

- **None**: This option disables the auto-refresh feature.
- **15 Seconds**: This option sets the window auto-refresh to 15-second time intervals.
- **30 Seconds**: This option sets the window auto-refresh to 30-second time intervals.
- **1 Minute**: This option sets the window auto-refresh to one-minute time intervals.
- **3 Minutes**: This option sets the window auto-refresh to three-minute time intervals.
- **5 Minutes**: This option sets the window auto-refresh to five-minute time intervals.

Step 4 Click **Refresh**. The PM counts for the new time interval appear.

Depending on the selected auto-refresh interval, the PM counts shown automatically update when each refresh interval is complete. If the auto-refresh interval is set to None, the PM counts are not updated unless you click the Refresh button.

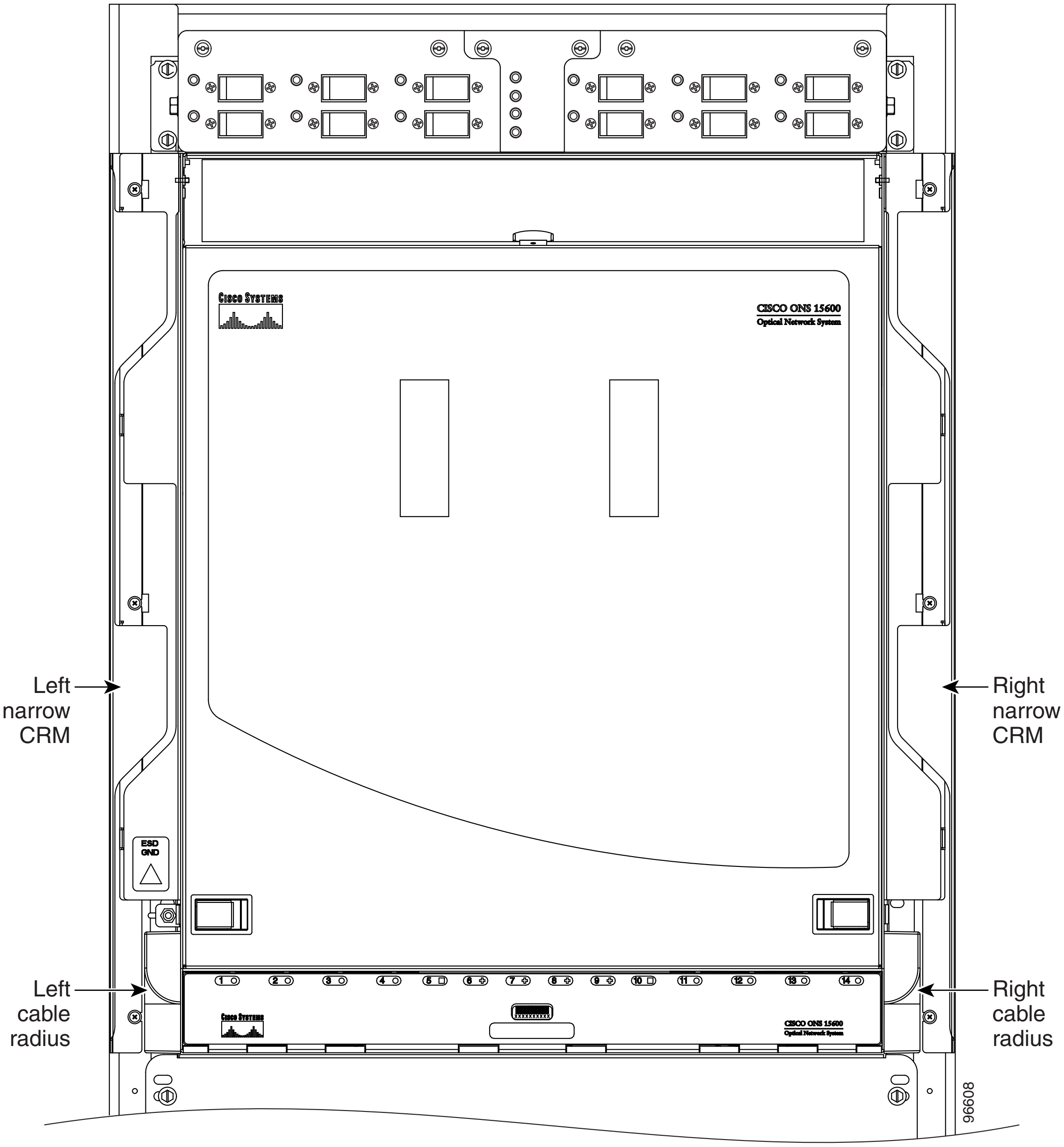
Step 5 Return to your originating procedure (NTP).

DLP-F257 Remove the Narrow CRMs

Purpose	This task removes existing narrow CRMs on the ONS 15600 SDH bay so that you can install the wide CRMs.
Tools/Equipment	Phillips screwdriver, 6 inches long Retaining screws
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Use a Phillips screwdriver to loosen the three screws (approximately five revolutions each) on the existing cable routers (Figure 17-5).

Figure 17-5 Narrow CRMs



Step 2 Lift the cable router slightly and pull it away from the bay.

Step 3 Repeat this procedure for the router on the other side.

Step 4 Unscrew and remove the cable radius pieces at the lower right and left sides of the shelf.

Step 5 Return to your originating procedure (NTP).

DLP-F258 Replace the Existing 600-mm Kick Plates with 900-mm Kick Plates

Purpose	This task removes the existing 600-mm (23.6-inch) kick plates so you can install the 900-mm (35.4-inch) kick plates. You should install 900-mm (35.4-inch) kick plates if you plan to install the wide CRMs.
Tools/Equipment	900-mm kick plate kit (53-2178-XX) Screwdriver Retaining screws
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Using the screwdriver, remove the five screws located on the 600-mm (23.6-inch) kick plate on the front of the bay.

Step 2 Repeat Step 1 for the kick plate at the rear of the bay.

Step 3 Place a 900-mm (35.4-inch) kick plate (700-16756-XX) at the front of the bay and use a screwdriver to install the five screws.

Step 4 On the right side of the bay, install the side kick plate (700-16758-XX) using the two appropriate screws.

Note Make sure the side kick plate's larger flange is on the floor.

Step 5 Repeat Step 4 for the left and rear kick plates.

Step 6 Return to your originating procedure (NTP).

DLP-F259 Manual Switch the Node Timing Reference

Purpose	This task commands the network element (NE) to switch to the timing reference you have selected if the synchronization status message (SSM) quality of the requested reference is not less than the current reference.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance** > **Timing > Source** tabs. The Timing source window appears.

Step 2 In the Reference drop-down list for the desired Clock, choose the desired reference.

Step 3 In the Operation drop-down list, choose **Manual**.

This operation commands the node to switch to the reference you have selected if the SSM quality of the reference is not lower than the current timing reference.

Step 4 Click **Apply**.

Step 5 Click **Yes** in the confirmation dialog box. If the selected timing reference is an acceptable valid reference, the node switches to the selected timing reference.

Step 6 If the selected timing reference is invalid, a warning dialog box appears. Click **OK**; the timing reference does not revert.

Step 7 Return to your originating procedure (NTP).

DLP-F260 Clear a Manual Switch on a Node Timing Reference

Purpose	This task clears a Manual switch on a node timing reference and reverts the timing reference to its provisioned reference.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance** > **Timing > Source** tabs. The Timing source window appears.

Step 2 Find the Clock reference that is currently set to Manual in the Operation menu.

Step 3 In the Operation drop-down list, choose **Clear**.

Step 4 Click **Apply**.

Step 5 Click **Yes** in the confirmation dialog box. If the normal timing reference is an acceptable valid reference, the node switches back to the normal timing reference as defined by the system configuration.

Step 6 If the normal timing reference is invalid or has failed, a warning dialog box appears. Click **OK**; the timing reference does not revert.

Step 7 Return to your originating procedure (NTP).

DLP-F261 Set the Optical Power Received Nominal Value

Purpose	This task sets the optical power received (OPR) threshold for each optical card. The ONS 15600 SDH node uses the value set as a performance monitoring parameter to determine if the power level has degraded.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the optical (STM-N) card that you want to provision. The card view appears.

Step 2 Click the **Provisioning > Optics Thresholds** tabs.

Step 3 From the Types list, choose **TCA or Alarm** and click **Refresh**.

Step 4 For Port 1, click **Set** in the Set OPR column. The OPR is set automatically. In the confirmation dialog box, click **OK**.

Step 5 Repeat Step 4 for each port on the card.

Step 6 Repeat this task for each optical card.

Step 7 Return to your originating procedure (NTP).

DLP-F262 Provision the IIOP Listener Port on the ONS 15600 SDH

Purpose	This task provisions the IIOP listener port on the ONS 15600 SDH, which enables you to access ONS 15600 SDHs that reside behind a firewall.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If the Enable Proxy Server on port 1080 check box is checked, CTC will use Port 1080 and ignore the configured IIOP port setting. If Enable Proxy Server is subsequently unchecked, the configured IIOP listener port is used.

Step 1 Click the **Provisioning** > **Security > Access** subtabs.

Step 2 In the TSC CORBA (IIOP) Listener Port area, choose a listener port option:

- **Default - TSC Fixed**—(Default) Uses Port 57790 to connect to ONS 15600 SDHs on the same side of the firewall or if no firewall is used. This option can be used for access through a firewall if Port 57790 is open.
- **Standard Constant**—Uses Port 683, the CORBA default port number.

- Other Constant—If Port 683 is not used, type the IIOP port specified by your firewall administrator.

Step 3 Click **Apply**.

Step 4 When the Change Network Configuration message appears, click **Yes**.

Both TSCs reboot, one at a time. The reboot will take approximately 15 minutes.

Step 5 Return to your originating procedure (NTP).

DLP-F263 Provision the IIOP Listener Port on the CTC Computer

Purpose	This task selects the IIOP listener port on CTC. You must perform this procedure if the computer running CTC resides behind a firewall.
Tools/Equipment	IIOP listener port number from LAN or firewall administrator
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2 DLP-F181 Log into CTC, page 16-34
Required/As Needed	Required if the computer running CTC resides behind a firewall
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **Firewall** tab.

Step 3 In the CTC CORBA (IIOP) Listener Port area, choose a listener port option:

- **Default - Variable**—(Default) Use to connect to ONS 15600 SDHs from within a firewall or if no firewall is used.
- **Standard Constant**—Use Port 683, the CORBA default port number.
- **Other Constant**—If Port 683 is not used, enter the IIOP port defined by your administrator.

Step 4 Click **Apply**. A warning appears telling you that the port change will apply during the next CTC login.

Step 5 Click **OK**.

Step 6 In the Preferences dialog box, click **OK**.

Step 7 To access the ONS 15600 SDH using the IIOP port, log out of CTC then log back in. (To log out, choose **Exit** from the File menu.)

Step 8 Return to your originating procedure (NTP).

DLP-F264 Edit SNCP Circuit Path Selectors

Purpose	This task changes the SNCP SF and SD thresholds, the reversion time, and PDI-P settings.
Tools/Equipment	None

Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 NTP-F152 Provision SNCP Nodes, page 5-13
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Circuits** tab.

Step 3 In the Circuits tab, click the SNCP circuit that you want to edit. To change the settings for multiple circuits, press the **Shift** key (to choose adjoining circuits) or the **Ctrl** key (to choose nonadjoining circuits) and click each circuit you want to change.

Step 4 From the Tools menu, choose **Circuits > Set Path Selector Attributes**.

Note Alternatively, for single circuits, you can click Edit, then click the SNCP Selectors tab in the Edit Circuits window.

Step 5 In the Path Selectors Attributes dialog box, edit the following SNCP selectors, as needed:

- Revertive—If checked, traffic reverts to the working path when conditions that diverted it to the protect path are repaired. If not checked, traffic does not revert.
- Reversion Time (Min)—If Revertive is checked, sets the amount of time that will elapse before traffic reverts to the working path. The range is 0.5 to 12 minutes in 0.5 minute increments.

Step 6 In the VC Circuits Only area, set the following thresholds:

- (Low-order circuits only) In the VC LO Circuits Only area, set the following thresholds:
  - SF threshold—Sets the SNCP signal failure BER threshold.
  - SD threshold—Sets the SNCP signal degrade BER threshold.
- (High-order circuits only) In the VC4 Circuits Only area, set the following thresholds:
  - SF Ber Level—Sets the SNCP signal failure BER threshold.
  - SD Ber Level—Sets the SNCP signal degrade BER threshold.
  - Switch on PDI-P—When checked, traffic switches if a VC4 payload defect indication is received.

Step 7 Click **OK** and verify that the changed values are correct.

Step 8 Return to your originating procedure (NTP).

DLP-F265 Change the Node Name, Date, Time, and Contact Information

Purpose	This task changes basic node information such as node name, date, time, and contact information.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34

Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Changing the date, time, or time zone might invalidate node performance monitoring counters.

Step 1 In node view, click the **Provisioning > General** tabs.

Step 2 Change any of the following:

- General: Node Name/TID
- General: Contact
- Location: Latitude
- Location: Longitude
- Location: Description

Note To see changes to longitude or latitude on the network map, you must go to network view and right-click the specified node, then click Reset Node Position.

- Time: Use NTP/SNTP Server
- Time: Date (M/D/Y)
- Time: Time (H:M:S)
- Time: Time Zone
- Time: Use Daylight Saving Time

See the "NTP-F133 Set Up Date, Time, and Contact Information" procedure on page 4-4 for detailed field descriptions.

Step 3 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 4 Return to your originating procedure (NTP).

DLP-F266 Enable Dialog Box Do-Not-Display Option

Purpose	This task enables or disables the "Do not show this dialog again" dialog box preference for subsequent sessions or disables the do-not-display option.
Tools/Equipment	None
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If any user who has rights to perform an operation (for example, creating a circuit) selects the "Do not show this dialog again" check box on a dialog box, the dialog box is not displayed for any other users who perform that operation on the network unless the command is overridden using the following task.

Step 1 From the Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **General** tab.

The Preferences Management area field lists all dialog boxes where "Do not show this dialog again" was checked.

Step 3 Choose one of the following:

- Don't Show Any—Hides all do-not-display check boxes.
- Show All—Overrides do-not-display check box selections and displays all dialog boxes.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-F267 Change Security Policy on a Single Node

Purpose	This task changes the security policy for a single node, including idle user timeouts, user lockouts, password changes, and concurrent login policies.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning** > **Security** > **Policy** tabs.

Step 2 If you want to modify the idle user timeout period, click the hour (H) and minute (M) arrows in the Idle User Timeout area for the security level you want to provision: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. The idle period time range is 0 and 16 hours, and 0 and 59 minutes. The user is logged out after the idle user timeout period is reached.

Step 3 In the User Lockout area, you can modify the following:

- Failed Logins Before Lockout—Choose the number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
- Manual Unlock by Superuser—Check this box if you want to allow a user with Superuser privileges to manually unlock a user who has been locked out from a node. The user will remain locked out until a Superuser manually unlocks the user.
- Automatic Unlock After—Choose the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).

Step 4 In the Password Change area, you can modify the following:

- Prevent Reusing Last [nn] Password(s)—Choose a value between 1 and 10 to set the number of different passwords the user must create before they can reuse a password.
- New Password must Differ from the Old Password by [nn] Characters—Choose a value between 1 and 5 to determine how many characters must change between the old and new passwords.
- Cannot Change New Password for [nn] Days—If checked, prevents users from changing their password for the specified period. Choose a value between 20 and 95 days.
- Require Password Change on First Login to New Account—Check the check box to require all new users to change their password the first time they log into their account.

Note "Require [nn] password change on first login to new account" or "Cannot change new password for [nn] days" is an OR statement, meaning that either one of the two conditions that you set can be satisfied for a password to be reused.

Step 5 In the Password Aging area, check the Enforce Password Aging check box to require users to change their password at periodic intervals. If checked, provision the following parameters:

- Aging Period—Sets the amount of time that must pass before the user must change his or her password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, and SUPERUSER. The range is 20 to 95 days.
- Warning—Sets the number of days the user will be warned to change their password for each security level. The range is 2 to 20 days.

Step 6 In the Other area, you can provision the following:

- Single Session Per User**—**If checked, limits users to one login session at one time.
- Disable Inactive User—If checked, disables users who do not log into the node for the period of time specified in the Inactive Duration box. The Inactive Duration range is 0 to 99 days.

Note If you advance the node date to a date beyond the threshold in the Inactive Duration box, the user account is disabled. User accounts are not reenabled if you revise the node date backwards, and the account has already been disabled.

Step 7 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 8 Return to your originating procedure (NTP).

DLP-F268 Change Security Policy on Multiple Nodes

Purpose	This task changes the security policy for multiple nodes including idle user timeouts, user lockouts, password change, and concurrent login policies.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Provisioning > Security > Policy** tabs. A read-only table of nodes and their policies appears.

Step 3 Click a node in the table that you want to modify, then click **Edit**.

Step 4 In the Idle User Timeout area, you can modify the timeout values for each security level by clicking the hour (H) and minute (M) arrows. You can choose values between 0 and 16 hours and 0 and 59 minutes.

Step 5 In the User Lockout area, you can modify the following:

- Failed Logins Allowed Before Lockout—Choose the number failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
- Manual Unlock by Superuser—Check this box if you want to allow a user with Superuser privileges to manually unlock a user who has been locked out from a node. The user will remain locked out until a Superuser manually unlocks the user.
- Automatic Unlock After—Choose the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).

Step 6 In the Password Change area, you can modify the following:

- Prevent Reusing Last [nn] Password(s)—Choose a value between 1 and 10 to set the number of different passwords the user must create before they can reuse a password.
- New Password must Differ from the Old Password by [nn] Characters—Choose a value between 1 and 5 to determine how many characters must change between the old and new passwords.
- Cannot Change New Password for [nn] Days—If checked, prevents users from changing their password for the specified period. Choose a value between 20 and 95 days.
- Require Password Change on First Login to New Account—Check the check box to require all new users to change their password the first time they log into their account.

Note “Require [nn] password change on first login to new account” or “Cannot change new password for [nn] days” is an OR statement, meaning that either one of the two conditions that you set can be satisfied for a password to be reused.

Step 7 In the Password Aging area, check the Enforce Password Aging check box to require users to change their password at periodic intervals. If checked, provision the following parameters:

- Aging Period—Sets the amount of time that must pass before the user must change his or her password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, and SUPERUSER. The range is 20 to 95 days.
- Warning—Sets the number of days the user will be warned to change their password for each security level. The range is 2 to 20 days.

Step 8 In the Other area, you can provision the following:

- Single Session Per User**—**If checked, limits users to one login session at one time.
- Disable Inactive User—If checked, disables users who do not log into the node for the period of time specified in the Inactive Duration box. The Inactive Duration range is 0 to 99 days.

Note If you advance the node date to a date beyond the threshold in the Inactive Duration box, the user account is disabled. User accounts are not reenabled if you revise the node date backwards, and the account has already been disabled.

Step 9 In the Select applicable nodes list dialog box, uncheck any nodes where you do not want to change the user's settings (all network nodes are selected by default).

Step 10 Click **OK**. The Security Policy Change Results dialog box appears.

Step 11 Confirm that the changes are correct and click **OK**.

Step 12 Return to your originating procedure (NTP).

DLP-F269 Change User Password and Security Levels for a Single Node

Purpose	This task changes settings for an existing user at one node. Use this procedure to change a user's password, modify the user's security level, lock out the user, disable the user, or require the user to change their password on next login.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning** > **Security** > **Users** tabs.

Step 2 Click the user whose settings you want to modify, then click **Edit**.

Step 3 In the Edit User dialog box, you can modify:

- New Password
- Security Level
- Lock Out
- Disable
- Change Password on Next Login

See the "DLP-F269 Change User Password and Security Levels for a Single Node" task on page 17-61 and the "DLP-F270 Change User and Security Settings for Multiple Nodes" task on page 17-62 for field descriptions.

Step 4 Click **Apply**.

Note User settings that you changed during this task will not appear until that user logs off and logs back in again.

Step 5 Return to your originating procedure (NTP).

DLP-F270 Change User and Security Settings for Multiple Nodes

Purpose	This task changes an existing user's settings for multiple nodes. Use this procedure to change passwords, modify security levels, lock out users, disable users, or require users to change their passwords on next login.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Step 1 From the View menu, choose **Go To Network View**. Verify that all the nodes where you want to add users are accessible in network view.

Step 2 Click the **Provisioning > Security > Users** tabs. Click the user's name whose settings you want to change.

Step 3 Click **Edit**. The Change User window appears.

Step 4 In the Change User dialog box, you can:

- New Password
- Security Level
- Lock Out
- Disable
- Change Password on Next Login

See the "DLP-F269 Change User Password and Security Levels for a Single Node" task on page 17-61 and "DLP-F270 Change User and Security Settings for Multiple Nodes" task on page 17-62 for field descriptions.

Step 5 In the Select applicable nodes list dialog box, uncheck any nodes where you do not want to change the user's settings (all network nodes are selected by default).

Step 6 Click **OK**. The User Change Results confirmation dialog box appears.

Step 7 Click **OK**. Confirm that the changes appear; if not, repeat the task.

Step 8 Return to your originating procedure (NTP).

DLP-F271 Log Out a User on a Single Node

Purpose	This task logs out a user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning** > **Security** > **Active Logins** tabs.

Step 2 Choose the user you want to log out.

Step 3 Click **Logout**.

Step 4 In the Logout User dialog box, check **Lockout before Logout** if you want to lock the user out before logout. This prevents the user from logging in after logout based on parameters set under User Lockouts in the Policy tab. Either a manual unlock by a Superuser is required, or the user is locked out for the amount of time specified in the Lockout Duration field. See the "DLP-F267 Change Security Policy on a Single Node" task on page 17-58 for more information.

Step 5 Click **OK**. A confirmation dialog box appears.

Step 6 Click **OK**. Confirm that the changes appear; if not, repeat the task.

Step 7 Return to your originating procedure (NTP).

DLP-F272 Log Out a User on Multiple Nodes

Purpose	This task logs out a user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 From the View menu, chose **Go To Network View**.

Step 2 Click the **Provisioning** > **Security** > **Active Logins** tabs.

Step 3 Choose the user you want to log out.

Step 4 Click **Logout**.

Step 5 In the Logout User dialog box, uncheck the nodes where you do not want to log out the user.

Step 6 Check **Lockout before Logout** if you want to lock the user out before logout. This prevents the user from logging in after logout based on parameters set under User Lockouts in the Policy tab. Either a manual unlock by a Superuser is required, or the user is locked out for the amount of time specified in the Lockout Duration field. See the "DLP-F267 Change Security Policy on a Single Node" task on page 17-58 for more information.

Step 7 Click **OK**. A confirmation dialog box appears.

Step 8 Click **OK**.

Step 9 Return to your originating procedure (NTP).

DLP-F273 Check the Network for Alarms and Conditions

Purpose	This task verifies that no alarms or conditions exist on the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	Retrieve or higher

Step 1 From the View menu, choose **Go To Network View**. Verify that all affected spans on the network map are green.

Step 2 Verify that the affected spans do not have active switches on the network map. Span ring switches are graphically displayed on the span with the letters L for lockout ring, F for Force ring, M for manual ring, and E for Exercise ring.

Another way you can verify that no active switches exist is to click the **Conditions** tab, and click **Retrieve**. Make sure the Filter button is not selected.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 for instructions.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for procedures.

Step 4 Return to your originating procedure (NTP).

DLP-F274 Disable Proxy Service Using Internet Explorer (Windows)

Purpose	This task disables proxy service for PCs running Internet Explorer. It is required if your computer is connected to a network computer proxy server and your browser is Internet Explorer.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required if your computer is connected to a network computer proxy server and your browser is Internet Explorer.
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 From the Start menu, select **Settings > Control Panel**.

Note If your computer is running Windows XP, you can select Control Panel directly from the Start menu. Make sure that you are in Classic View before continuing with this procedure.

Step 2 In the Control Panel window, choose **Internet Options**.

Step 3 From the Internet Properties dialog box, click **Connections** > **LAN Settings**.

Step 4 In the LAN Settings dialog box, complete one of the following tasks:

- Uncheck **Use a proxy server** to disable the service.
- Leave **Use a proxy server** selected and click **Advanced**. In the Proxy Setting dialog box under Exceptions, enter the IP addresses of ONS 15600 SDH nodes that you will access. Separate each address with a semicolon. You can insert an asterisk for the host number to include all the ONS nodes on your network. Click **OK** to close each open dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-F275 Disable Proxy Service Using Netscape (Windows and UNIX)

Purpose	This task disables proxy service for PCs and UNIX workstations running Netscape. It is required if your computer is connected to a network computer proxy server and your browser is Netscape.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required if your computer is connected to a network computer proxy server and your browser is Netscape.
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Open Netscape.

Step 2 From the Edit menu, choose **Preferences**.

Step 3 In the Preferences dialog box under Category, choose **Advanced > Proxies**.

Step 4 In the right side of the Preferences dialog box under Proxies, perform one of the following options:

- Choose **Direct connection to the Internet** to bypass the proxy server.
- Choose **Manual proxy configuration** to add exceptions to the proxy server, then click **View**. In the Manual Proxy Configuration dialog box under Exceptions, enter the IP addresses of the ONS 15600 SDH nodes that you will access. Separate each address with a comma. Click **OK** to close each open dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-F416 Disable Proxy Service Using Mozilla Firefox (Windows and UNIX)

Purpose	This task disables proxy service for PCs and UNIX workstations running Mozilla Firefox.
Tools/Equipment	None
Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1
Required/As Needed	As Needed
Onsite/Remote	Onsite or remote
Security Level	None

Note You must perform this task if your computer is connected to a network computer proxy server and your browser is Mozilla Firefox.

Step 1 Open Mozilla Firefox.

Step 2 From the Tools menu, choose **Options**.

Step 3 In the Options dialog box under the Network tab, click **Settings**.

Step 4 In the Connection Settings dialog box, perform one of the following options, as applicable:

- Choose the **No Proxy** radio button to disable the proxy service.
- Choose **Manual proxy configuration** to add exceptions to the proxy server. In the **No Proxy for** option under the Manual Proxy Configuration, enter the IP addresses of the ONS 15454 nodes that you access. Separate each address with a comma. Click **OK** to close each open dialog box.

Note For ONS 15454 nodes that have TCC2P cards installed with the TCC2P secure mode option enabled, enter the backplane LAN port IP addresses. If the node is in secure mode and the configuration has been locked, you will not be able to change the IP address unless the lock is disabled by Cisco Technical Support. See the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual* for additional information about secure mode.

Step 5 Return to your originating procedure (NTP).

DLP-F276 Install the Narrow CRMs

Purpose	This task installs narrow CRMs on the ONS 15600 SDH bay.
Tools/Equipment	Narrow CRM kit (53-2193-01) (optional) • Fiber radiuses (2 left and 2 right) • Narrow CRMs (2 left and 2 right) • 6x32 panhead screws for fiber radiuses (4) • 8x32 panhead screws for narrow CRMs (6) Phillips screwdriver, 6 inches long Retaining screws
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 On the bottom left and bottom right, install the cable radius (2 screws).

Step 2 Lift the right-side narrow CRM and align it with the three screw holes you will use to mount the CRM.

Step 3 Use a Phillips screwdriver to tighten the three screws, starting with the bottom screw and moving up (Figure 17-5 on page 17-51).

Step 4 Repeat this procedure for the router on the other side.

Step 5 Return to your originating procedure (NTP).

DLP-F277 Install the Wide CRMs

Purpose	This task installs the wide CRMs.
Tools/Equipment	Wide CRM kit (53-2181-XX) (optional) • Latch catches (2 left and 2 right) • Velcro tie-wrap (26) • Wide CRMs (2 left and 2 right) • 6x32 panhead screws for latch catches (8) • 8x32 panhead screws for wide CRMs (10) Screwdriver Retaining screws
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note If you are installing CRMs on more than one shelf, it is easiest to install the lowest CRMs first.

Note If your site uses under-floor cabling, mount the CRMs on the sides of the bay directly next to the shelf below the node for which you want to route cables. (For instance, if you are routing cables that originate in the top shelf, mount the CRMs that will route those cables on the sides of the bay at the middle shelf level.)

Step 1 To install the lower latch bracket for the right-side CRM, line up the holes with the holes on the shelf where you removed the plastic cable radius.

Step 2 Screw the two screws through the brackets into the shelf.

Step 3 Repeat for the right-side CRM’s top latch bracket.

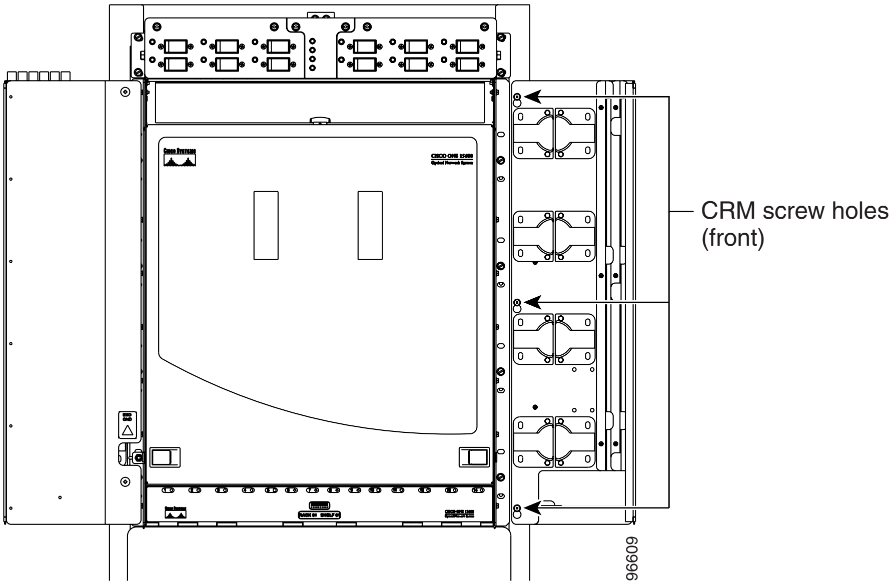
Step 4 Repeat Steps 1 through 3 for the left-side latch brackets.

Step 5 On the front right edge of the bay, locate the three screw holes that will be used to secure the right-side CRM to the bay. Insert a #8 screw in the top hole and turn five revolutions. Do not tighten the screw completely, but make sure it is started enough so that it is secure in the bay (Figure 17-6).

Note Only the left-side CRM front door has the cutout and label for the ESD jack.

Step 6 Repeat for the two remaining screws on that side of the bay.

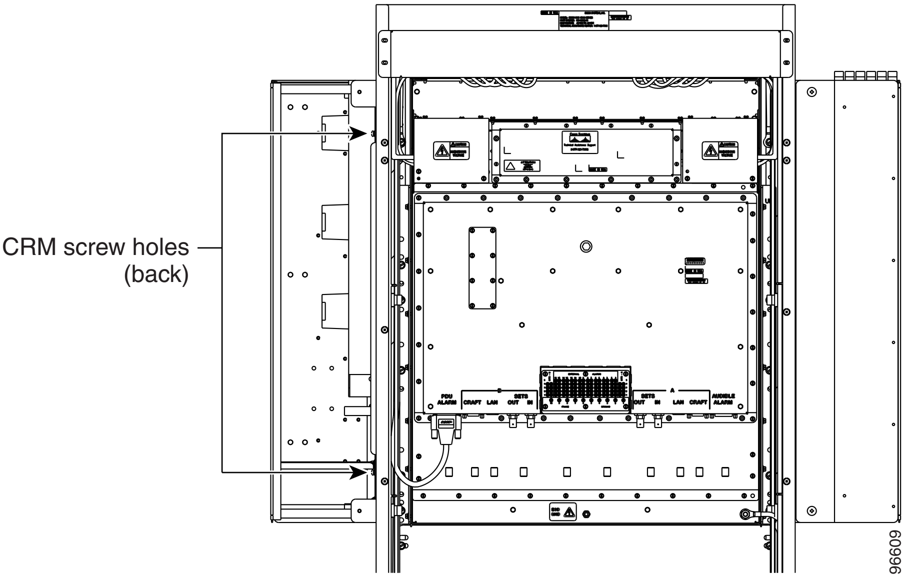
Figure 17-6 CRM Screw Holes (Front)



Step 7 Align the front of the CRM keyholes with the screws and carefully slide the CRM down so it rests on the screws. Tighten the screws, starting with the bottom screw and proceeding up to the middle and top screws.

Step 8 Locate the two screw holes on the side of the shelf toward the rear of the bay and make sure they are aligned with the holes on the CRM. Install and tighten the bottom screw and then the top screw (Figure 17-7).

Figure 17-7 CRM Screw Holes (Back)



Step 9 Repeat Steps 5 through 8 for the left-side CRM.

Step 10 Return to your originating procedure (NTP).

DLP-F278 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)

Purpose	This task reinitializes the ONS 15600 SDH using the CTC reinitialization (reinit) tool on a Windows computer. Reinitialization uploads a new software package to the TSC cards, clears the node database, and restores the factory default parameters.
Tools/Equipment	ONS 15600 SDH System Software CD, Version 8.0 JRE 5.0 must be installed on the computer to log into the node at the completion of the reinitialization. The reinitialization tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 5.0.
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note Restoring a node to the factory configuration deletes all cross-connects on the node.

Step 1 Insert the ONS 15600 SDH System Software CD, Version 8.0, into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.

Step 2 From the Windows Start menu, choose **Run**. In the Run dialog box, click **Browse** and navigate to the CISCO15600SDH folder on the software CD.

Step 3 In the Browse dialog box Files of Type field, choose All Files.

Step 4 Choose the RE-INIT.jar file and click Open. The NE Reinitialization window appears.

Step 5 Complete the following fields:

- GNE IP—If the node you are reinitializing is accessed through another node configured as a gateway network element (GNE), enter the GNE IP address. If you have a direct connection to the node, leave this field blank.
- Node IP—Enter the node name or IP address of the node that you are reinitializing.
- User ID—Enter the user ID needed to access the node.
- Password—Enter the password for the user ID.
- Upload Package—Check this box to send the software package file to the node. If unchecked, the software stored on the node is not modified.
- Force Upload—Check this box to send the software package file to the node even if the node is running the same software version. If unchecked, reinitialization will not send the software package if the node is already running the same version.
- Activate/Revert—Check this box to activate the uploaded software (if the software is a later than the installed version) or revert to the uploaded software (if the software is earlier than the installed version) as soon as the software file is uploaded. If unchecked, the software is not activated or reverted after the upload, allowing you to initiate the functions later from the node view Maintenance > Software tab.
- Confirm—Check this box if you want a warning message displayed before any operation is performed. If unchecked, reinitialization does not display a warning message.
- Database restore—Check this box if you want to send a new database to the node and to restore node provision values. (This is equivalent to the CTC database restore with the "Complete Database" check box unchecked.)
- Complete database restore—Check this option to send a new database to the node and to restore node provision and system values. (This is equivalent to the CTC database restore with the "Complete Database" check box checked.)
- No database restore—Check this box if you do not want the node database to be modified.
- Search Path—Enter the path to the CISCO 15600 SDH folder on the CD drive.

Step 6 Click **Go**.

Caution Before continuing with the next step, verify that the database to upload is correct. You cannot reverse the upload process after you click Yes.

Step 7 Review the information on the Confirm NE Re-Initialization dialog box, then click **Yes** to start the reinitialization.

The reinitialization begins. After the software is downloaded and activated, and the database is uploaded to the TSC cards, “Complete” appears in the status bar and the TSC cards will reboot. Wait a few minutes for the reboot to complete.

Step 8 After the reboot is complete, log into the node using the "DLP-F181 Log into CTC" task on page 16-34.

Step 9 Complete the "NTP-F133 Set Up Date, Time, and Contact Information" procedure on page 4-4.

Step 10 Return to your originating procedure (NTP).

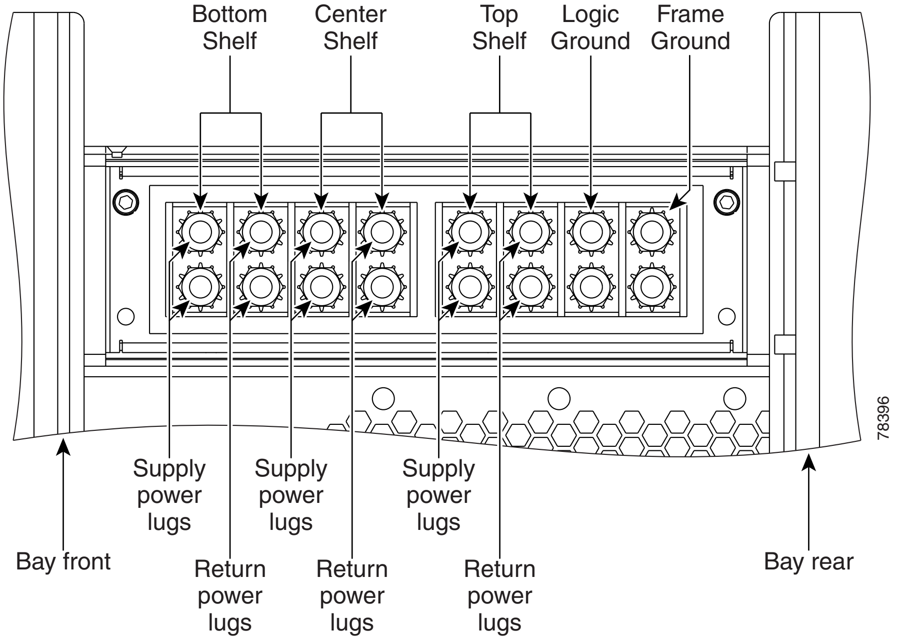
DLP-F279 Connect the PDU Ground Cables to the PDU

Purpose	This task connects the preinstalled power distribution unit (PDU) ground cables to the PDU.
Tools/Equipment	Screwdriver 7/16-inch (11.11 mm) socket Torque wrench calibrated to inch-pounds 9/64-inch (3.57 mm) Allen wrench
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Locate the PDU ground cables (Figure 16-3 on page 16-8). Remove the PDU safety cover on the right side and install the free end of the green terminal closest to the rear of the rack. This terminal is labeled "Frame Ground" in Figure 17-8.

Note A shunt is preinstalled between logic and frame ground to bond the two grounds. If you are providing a separate logic ground, remove this shunt on both sides before installing the PDU frame ground.

Figure 17-8 Power Terminal Block (Right Side Shown)



Step 2 Tighten the nuts to 36 in-lb.

Step 3 Repeat Steps 1 and 2 for the left side of the PDU.

Step 4 Replace the PDU safety covers.

Step 5 Return to your originating procedure (NTP).

DLP-F280 Install Isolated Logic Ground

Purpose	This task isolates logic ground from frame ground if required by site specifications. The ONS 15600 SDH ships with the frame ground strapped to the logic ground with metal shunts at the PDU input terminals.
Tools/Equipment	Screwdriver Ground wire Two-hole power lugs, 0.625-inch hole spacing, 0.25-inch bolt holes (2) (Panduit LCCF2-14AZFW-E)
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Remove the PDU safety cover on the right side.

Step 2 Remove the metal shunt connecting the frame ground to the logic ground terminals. Terminal designations are marked on the top of the PDU.

Step 3 Replace the green ground wire on the frame ground terminals and secure the wire with two Kepnuts torqued to 36 in-lb.

Step 4 Repeat Steps 1 through 3 for the left side of the bay.

Step 5 Build a 36-inch-long logic ground strap with two-hole lugs on each side. Use AWG #2 cable with green insulation and crimp lugs on the terminals at each end.

Note Lugs must be no wider than 0.60 inches (15.24 mm) to fit on the PDU terminals.

Step 6 Put one end of the strap on the left-side PDU logic ground terminals and secure the strap with two Kepnuts torqued to 36 in-lb.

Step 7 Put the other end of the ground strap on the right-side PDU logic ground terminals.

Step 8 Put the two-hole lug from the office logic ground cable on the right-side PDU logic ground terminals and secure it with two Kepnuts torqued to 36 in-lb.

Step 9 Secure the other end of the office logic ground cable to the office logic ground bar.

Step 10 Return to your originating procedure (NTP).

DLP-F281 Check MS-SPRing or SNCP Alarms and Conditions

Purpose	This task checks an MS-SPRing or an SNCP for alarms and conditions before performing any major administrative change to the ring such as adding and removing nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From the View menu, choose **Go to Network View**. Verify that all MS-SPRing or SNCP spans on the network map are green.

Step 2 Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms or conditions, such as loss of signal (LOS), loss of frame alignment (LOF), alarm indication signal–line (AIS-L), SF, and SD. In an MS-SPRing, these facility conditions might be reported as minor alarms. Make sure the Filter button in the lower right corner of the window is off (not indented).

Step 3 Click the **Conditions** tab and click **Retrieve.** Verify that no ring switches are active. Make sure the Filter button in the lower right corner of the window is off (not indented).

Step 4 Return to the originating procedure (NTP).

DLP-F282 Clear an MS-SPRing Force Ring Switch

Purpose	This task removes a Force switch from an MS-SPRing port.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > MS-SPRing** tabs.

Step 3 Select the MS-SPRing and click **Edit**.

Note If node icons overlap, drag and drop the icons to a new location or return to network view and change the positions of the network node icons. MS-SPRing node icons are based on the network view node icon positions.

Step 4 To clear a Force switch on the west line:

a. Right-click the MS-SPRing west port where you want to clear the protection switch and choose **Set West Protection Operation**. Ports with a Force switch applied are marked with an F.

b. In the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down list. Click **OK**.

c. In the Confirm MS-SPRing Operation dialog box, click **Yes**.

Step 5 To clear a Force switch on the east line:

a. Right-click the MS-SPRing east port where you want to clear the protection switch and choose **Set East Protection Operation**. Ports with a Force switch applied are marked with an F.

b. In the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down list. Click **OK**.

c. In the Confirm MS-SPRing Operation dialog box, click **Yes**.

On the MS-SPRing network graphic, a green and a purple span line connects each node. This is normal for MS-SPRings when protection operations are not invoked.

Step 6 From the File menu, choose **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-F283 Install Public-Key Security Certificate

Purpose	This task installs the ITU Recommendation X.509 public-key security certificate. The public-key certificate is required to run Software Release 1.1 or later.
Tools/Equipment	None

Prerequisite Procedures	This task is performed during the "DLP-F181 Log into CTC" procedure on page 16-34. You cannot perform it outside of this task.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 If the Java Plug-in Security Warning dialog box appears, choose one of the following options:

- **Yes (Grant This Session)**—Installs the public-key certificate to your PC only for the current session. After the session is ended, the certificate is deleted. This dialog box will appear the next time you log into the ONS 15600 SDH.
- **No (Deny)**—Denies permission to install certificate. If you choose this option, you cannot log into the ONS 15600 SDH.
- **Always (Grant Always)—**Installs the public-key certificate and does not delete it after the session is over. Cisco recommends this option.
- **More Details (View Certificate)**—Allows you to view the public-key security certificate.

Step 2 If the Login dialog box appears, continue with Step 3. If the Change Java Policy File dialog box appears, complete this step. The Change Java Policy File dialog box appears if CTC finds a modified Java policy file (.java.policy) on your PC. In Software Release 1.0, the Java policy file was modified to allow CTC software files to be downloaded to your PC. The modified Java policy file is not needed in Software R1.1 and later, so you can remove it. Choose one of the following options:

- **Yes**—Removes the modified Java policy file from your PC. Choose this option only if you will log into ONS 15600 SDHs running Software R1.4 (the first ONS 15600 SDH release) or later.
- **No**—Does not remove the modified Java policy file from your PC. If you choose No, this dialog box will appear every time you log into the ONS 15600 SDH. If you do not want it to appear, check the **Do not show the message again** check box.

Step 3 Return to your originating procedure (NTP).

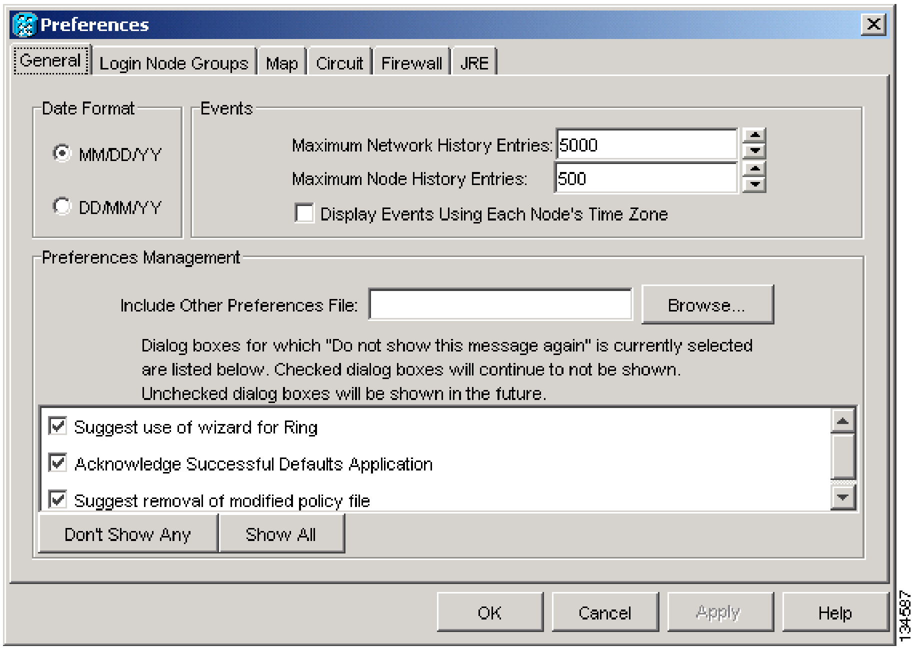
DLP-F284 Changing the Maximum Number of Session Entries for Alarm History

Purpose	This task changes the maximum number of session entries included in the alarm history. Use this task to extend the history list in order to save information for future reference or troubleshooting.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu, choose **Preferences**.

The CTC Preferences Dialog box appears (Figure 17-9).

Figure 17-9 CTC Preferences Dialog Box



Date Format

● MM/DD/YY

○ DD/MM/YY

Events

Maximum Network History Entries: 5000

Maximum Node History Entries: 500

□ Display Events Using Each Node's Time Zone

Preferences Management

Include Other Preferences File:

Dialog boxes for which "Do not show this message again" is currently selected are listed below. Checked dialog boxes will continue to not be shown. Unchecked dialog boxes will be shown in the future.

☑ Suggest use of wizard for Ring

☑ Acknowledge Successful Defaults Application

☑ Suggest removal of modified policy file

Step 2 Click the up or down arrow buttons next to the Maximum History Entries field to change the entry.

Step 3 Click **Apply** and **OK**.

Note Setting the Maximum History Entries value to the high end of the range uses more CTC memory and could impair CTC performance.

Note This task changes the maximum history entries recorded for CTC sessions. It does not affect the maximum number of history entries viewable for a network, node, or card.

Step 4 Return to your originating procedure (NTP).

DLP-F285 Delete Alarm Severity Profiles

Purpose	This task deletes a custom or default alarm severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 3 Click the column heading for the profile column you want to delete.

The selected alarm profile name appears in the Description field.

Step 4 Click **Delete**.

The Select Node/Profile Combination for Delete dialog box appears.

Step 5 Click the node name(s) in the Node Names list to highlight the profile location.

Tip If you hold the Shift key down, you can select consecutive node names. If you hold the Ctrl key down, you can select any combination of nodes.

Step 6 Click the profile name(s) that you want to delete in the Profile Names list.

Step 7 Click **OK**.

The Delete Alarm Profile confirmation dialog box appears.

Step 8 Click **Yes** for each Delete Alarm Profile confirmation dialog box.

Note If you delete a profile from a node, it is still displayed in the network view Provisioning > Alarm Profiles > Alarm Profile Editor window unless you remove it by choosing Remove.

Step 9 To remove the alarm profile from the Provisioning > Alarm Profiles > Alarm Profile Editor window, right-click the column of the profile you deleted and choose **Remove** from the shortcut menu.

Note If a node and profile combination is selected but does not exist, a warning appears: “One or more of the profile(s) selected do not exist on one or more of the node(s) selected.” For example, if Node A has only Profile 1 and the user tries to delete both Profile 1 and Profile 2 from Node A, this warning appears. However, the operation still removes Profile 1 from Node A.

Note The Default and Inherited special profiles cannot be deleted and do not appear in the Select Node/Profile Combination for Delete window.

Step 10 Return to your originating procedure (NTP).

DLP-F286 Enable Alarm Filtering

Purpose	This task filters the display of alarms, history, or conditions on the login workstation.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed

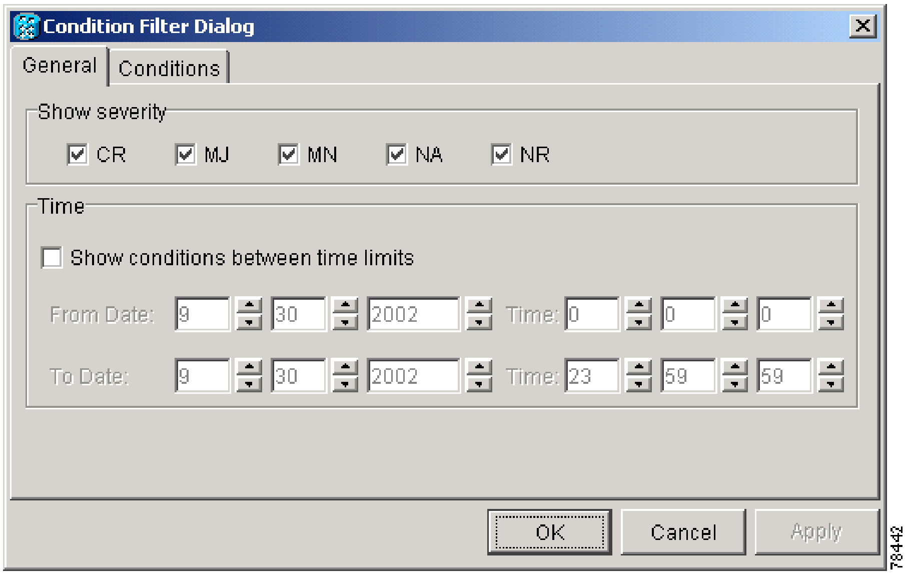
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note The Filter button in the Alarms, History, and Conditions windows allows you to display data that meets a certain severity level, time frame, and/or condition. CTC retains user filter activation. The filter button remains active when the user logs out and logs back in.

Step 1 In the node view Alarms, History, or Conditions windows, click **Filter**.

Step 2 In the Filter Dialog window, click the **General** tab. The Filter Dialog box appears (Figure 17-10).

Figure 17-10 Conditions Window Filter Dialog Box



Condition Filter Dialog

General | Conditions

Show severity

☑ CR ☑ MJ ☑ MN ☑ NA ☑ NR

Time

☐ Show conditions between time limits

From Date: 9 30 2002 Time: 0 0 0

To Date: 9 30 2002 Time: 23 59 59

Step 3 In the Show Severity area, alarm severities appear. All of the applicable severities are checked by default. If a severity is checked, it appears in the alarm list.

Note The Alarms window and History window have Critical (CR), Major (MJ), Minor (MN), and Not Alarmed (NA) severities available. The Conditions window also has the Not Reported (NR) severity.

Uncheck a severity to prevent it from appearing in the alarm list.

Step 4 In the Time area:

a. Check the **Enable Time** check box to establish time as a parameter in the filter.

b. Click the **From Date** and **To Date** up and down arrows to set the date range for the filter.

c. Click the **From Time** and **To Time** up and down arrows to set the time range for the filter.

Step 5 To set conditions, click the **Conditions** tab.

Step 6 In the Available list, double-click the desired conditions to move them to the Selected list.

Step 7 Click **OK**.

Step 8 Return to your originating procedure (NTP).

DLP-F287 Modify Alarm and Condition Filtering Parameters

Purpose	This task modifies alarm and condition reporting in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-F286 Enable Alarm Filtering, page 17-77 DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In the node, network, or card view, click the **Alarms** tab.

Step 2 Click the **Filter** button at the lower-left of the bottom toolbar.

The Alarm Filter Dialog box appears, showing the General tab.

In the General tab Show Severity area, you can choose which alarm severities will show through the alarm filter and provision a time period during which filtered alarms show through the filter. To change the alarm severities shown in the filter, go to Step 3. To change the time period filter for the alarms, go to Step 4.

Step 3 In the Show Severity area, click the check boxes for the severities [Critical (CR), Major (MJ*)*, Minor (MN), or Not Alarmed (NA)] that you want to be reported at the network level. Leave severity check boxes unchecked to prevent them from appearing.

When alarm filtering is disabled, all alarms show.

Step 4 In the Time area, click the **Show alarms between time limits** check box to enable it; then click the up and down arrows in the From Date, To Date, and Time fields to modify the period of alarms shown.

To modify filter parameters for conditions, continue with Step 5. If you do not need to modify them, continue with Step 6.

Step 5 Click the **Conditions** tab.

When alarm filtering is enabled, conditions in the Show list are visible and conditions in the Hide list are invisible.

- To move conditions individually from the Show list to the Hide list, click the **>** button.
- To move conditions individually from the Hide list to the Show list, click the **<** button.
- To move conditions collectively from the Show list to the Hide list, click the **>>** button.
- To move conditions collectively from the Hide list to the Show list, click the **<<** button.

Note Conditions include alarms.

Step 6 Click **Apply** and **OK**.

Alarm and condition filtering parameters are enforced when alarm filtering is enabled (see the "DLP-F286 Enable Alarm Filtering" task on page 17-77), and are not enforced when alarm filtering is disabled (see the "DLP-F288 Disable Alarm Filtering" task on page 17-80).

Step 7 Return to your originating procedure (NTP).

DLP-F288 Disable Alarm Filtering

Purpose	This task turns off specialized alarm filtering in all network nodes so that all severities are reported in CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-F286 Enable Alarm Filtering, page 17-77 DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In the node, network, or card view, click the **Alarms** tab.

Step 2 Click the **Filter** tool at the lower-right side of the bottom toolbar.

Alarm filtering is enabled if the tool is selected and disabled if the tool is raised (not selected).

Step 3 If you want alarm filtering disabled when you view conditions, click the **Conditions** tab and repeat Step 2.

Step 4 If you want alarm filtering disabled when you view alarm history, click the **History** tab and repeat Step 2.

Step 5 Return to your originating procedure (NTP).

DLP-F289 Manually Lock or Unlock a User on a Single Node

Purpose	This task manually locks out or unlocks a user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning** > **Security** > **Users** tabs.

Step 2 Choose the user you want to lock out or unlock.

Step 3 Click **Edit**.

Step 4 Complete one of the following:

- To lock a user out so the user cannot log into the node, check the **Locked out** check box.
- If the user is currently locked out, uncheck the **Locked out** check box.

  See the "DLP-F267 Change Security Policy on a Single Node" task on page 17-58 for more information about manual lockouts and lockout duration.

Step 5 Click **OK**. A confirmation dialog box appears.

Step 6 Click **OK**.

Step 7 Return to your originating procedure (NTP).

DLP-F290 Manually Lock or Unlock a User on Multiple Nodes

Purpose	This task manually locks out or unlocks a user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 From the View menu, chose **Go To Network View**.

Step 2 Click the **Provisioning** > **Security > Users** tabs.

Step 3 Click the user you want to lock out or unlock.

Step 4 Click **Edit**.

Step 5 Complete one of the following:

- To lock a user out so the user cannot log into nodes on the network, check the **Locked out** check box.
- If the user is currently locked out, uncheck the **Locked out** check box.

  See the "DLP-F267 Change Security Policy on a Single Node" task on page 17-58 for more information about manual lockouts and lockout duration.

Step 6 Click **OK**. A confirmation dialog box appears.

Step 7 Click **OK**. Confirm that the changes appear; if not, repeat the task.

Step 8 Return to your originating procedure (NTP).

DLP-F291 Verify MS-SPRing Extension Byte Mapping

Purpose	This task verifies that the extension byte mapping is the same on MS-SPRing trunk (span) cards that will be connected after a node is removed from an MS-SPRing. K3 extension byte mapping is supported on all ONS 15600 SDH STM-16 and STM-64 line cards, as well as the ONS 15454 SDH STM-16 card.
Tools/Equipment	STM-N cards must be installed at one or both ends of the MS-SPRing span that will be connected.
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In network view, double-click one of the MS-SPRing nodes with STM-N trunk cards that will be reconnected after an MS-SPRing node removal.

Step 2 Double-click one STM-N MS-SPRing trunk card to open the card view.

Step 3 Click the **Provisioning > Line** tab.

Step 4 Record on paper the byte in the MS-SPRing Ext Byte column.

Step 5 Repeat Steps 2 through 4 for the second STM-N trunk card.

Step 6 If the trunk cards on each end of the new span are not mapped to the same MS-SPRing extension byte, remap the extension byte of the trunk card at one of the nodes. See the "DLP-F255 Remap the K3 Byte" task on page 17-49.

Step 7 Return to your originating procedure (NTP).

DLP-F292 Single Shelf Control Card Switch Test

Purpose	This task tests the SSXC diagnostics and the switching functionality of the TSC and SSXC cards.
Tools/Equipment	The test set specified by the acceptance test procedure, connected and configured as specified in the acceptance test procedure.
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Test the SSXC card switch functionality:

a. Connect the test set to an STM-N slot/port on the node.

b. Create a one-way VC4-16c or VC4-64c circuit (based on the STM-N card connected in Step a) to monitor with the test set. See Chapter 6, "Create Circuits."

c. Verify that the test set is alarm and error free.

d. In node view, click the **Maintenance > Preferred Copy** tabs.

e. From the Set Preferred drop-down list, choose **Copy B**. Click **Apply**.

f. Remove the SSXC card from Slot 8. (The SSXC card faceplate extends to cover Slot 9.)

g. Verify that the traffic switches to Copy A. You will experience an interruption of less than 50 ms, and after that the test set should remain error free. If not, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide.*

h. Replace the SSXC card and allow it to recover.

i. Remove the SSXC card from Slot 6. (The SSXC card faceplate extends to cover Slot 7.)

j. Verify that the traffic switches to Copy B. You will experience an interruption of less than 50 ms, and after that the test set should remain error free. If not, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

k. Replace the SSXC card and allow it to recover.

l. From the Set Preferred drop-down list, choose **Copy A**. Click **Apply.**

Step 2 Test the TSC card switch functionality:

a. Make a note of which TSC card is active and which is standby by moving the mouse over the TSC cards on the CTC shelf graphic and viewing the tooltips. TSC cards are installed in Slot 5 and Slot 10.

b. On the shelf graphic, right-click the active TSC card and choose **Soft-reset Card** from the shortcut menu.

c. In the Resetting Card confirmation dialog box, click **Yes**. After 20 to 40 seconds, a “lost node connection, changing to network view” message appears.

d. Click **OK**. On the network view map, the node with the reset TSC card will be gray.

e. After the node icon turns yellow (from 1 to 2 minutes), double-click it. The node will remain yellow because of the UNPROT-SYNCCLK alarm for about 12 minutes. Move the mouse over the TSC cards on the shelf graphic and observe the following in the tooltips:

- The previous standby TSC card is active.
- The previously active TSC card is now standby.

f. Verify that the traffic on the test set connected to the node is still running. If a traffic interruption occurs, do not continue. Refer to your next level of support.

g. Repeat Steps b through f to return the active/standby TSC cards to their configuration at the start of the procedure.

h. Verify that the TSC cards appear as they did in Step a.

Step 3 Return to your originating procedure (NTP).

DLP-F293 Delete Circuits

Purpose	This task deletes circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34

Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "NTP-F221 Back Up the Database" procedure on page 14-4.

Step 2 Investigate all network alarms and resolve any problems that could be affected by the circuit deletion. If necessary, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Step 3 Verify that traffic is no longer carried on the circuit and that the circuit can be safely deleted.

Step 4 Click the **Circuits** tab.

Step 5 Choose the circuit you want to delete, then click **Delete**.

Step 6 In the Delete Circuits confirmation dialog box, check one or both of the following, as needed:

- Check **Change drop port admin state** and choose **Locked,disabled** from the drop-down list to put the circuit source and destination ports out of service if the circuit is the same size as the port or is the only circuit using the port. If the circuit is not the same size as the port or the only circuit using the port, CTC will not change the port state.
- If you check **Notify when completed**, the CTC Alerts confirmation dialog box indicates when all circuit source/destination ports are in the Locked,disabled service state and the circuit is deleted. During this time, you cannot perform other CTC functions. If you are deleting many circuits, waiting for confirmation can take a few minutes. Circuits are deleted whether or not this check box is checked.

Note The CTC Alerts dialog box does not automatically open to show a deletion error unless you checked All alerts or Error alerts only in the CTC Alerts dialog box. For more information, see the "DLP-F309 Configure the CTC Alerts Dialog Box for Automatic Popup" task on page 18-11. If the CTC Alerts dialog box is not set to open automatically with a notification, a red triangle inside the CTC Alerts toolbar icon indicates that a notification exists.

Step 7 Complete one of the following:

- If you checked "Notify when completed," the CTC Alerts dialog box appears. If you want to save the information, continue with Step 8. If you do not want to save the information, continue with Step 9.
- If you did not check "Notify when completed," the Circuits window appears. Continue with Step 10.

Step 8 If you want to save the information in the CTC Alerts dialog box, complete the following steps. If you do not want to save, continue with the next step.

a. Click **Save**.

b. Click **Browse** and navigate to the directory where you want to save the file.

c. Type the file name using a TXT file extension, and click **OK**.

Step 9 Click **Close** to close the CTC Alerts dialog box.

Step 10 Complete the "NTP-F221 Back Up the Database" procedure on page 14-4, if needed.

Note If a schedule is established for database backup, you do not need to complete a backup after every circuit addition and deletion.

Step 11 Return to your originating procedure (NTP).

DLP-F294 Change an STM-N Card

Purpose	This task describes how to change an optical (STM-N) card. To change a card, you must first delete all circuits, DCCs, and timing references on the card.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Physically removing an STM-N card can cause a loss of working traffic.

Note Do not use this procedure to replace a card with an identical card. Instead, use the "DLP-F174 Delete a Card from CTC" task on page 16-17.

Step 1 If the card the active card in a 1+1 protection group, switch traffic away from the card:

- **a.** Log into a node on the network. If you are already logged in, go to Step b.
- **b.** Display the CTC node (login) view.
- **c.** Click the **Maintenance > Protection** tabs.
- **d.** Double-click the protection group that contains the reporting card.
- **e.** Click the active card of the selected group.
- **f.** Click **Switch** in the Confirmation dialog box.
- **g.** Click **Yes** in the Confirmation dialog box.

Step 2 Delete all circuits, DCCs, and timing references on the card.

Step 3 In CTC, right-click the card that you want to remove and choose **Change Card**.

Step 4 From the Change Card drop-down list, choose the desired card type and click **OK**. A Mismatched Equipment Alarm (MEA) appears until you replace the card.

Step 5 Physically remove the card:

- **a.** Open the card latches/ejectors.
- **b.** Use the latches/ejectors to pull the card forward and away from the shelf.

Step 6 Complete the "NTP-F119 Install the STM-N Cards" procedure on page 2-4.

Step 7 Return to your originating procedure (NTP).

DLP-F295 Clear a Manual or Force Switch in a 1+1 Protection Group

Purpose	For ports configured for revertive switching, this task clears the Manual or Force switch and restores traffic to the pre-switch port. For nonrevertive ports, it clears the switch but does not revert traffic to the previous port.
Tools/Equipment	None
Prerequisite Procedures	DLP-F238 Initiate a Manual Switch on a Port in a 1+1 Protection Group, page 17-31 or DLP-F239 Initiate a Force Switch on a Port in a 1+1 Protection Group, page 17-32
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, choose the protection group that contains the card you want to clear.

Step 3 In the Selected Group area, choose the card you want to clear.

Step 4 In the Inhibit Switching area, click **Clear**.

Step 5 Click **Yes** in the confirmation dialog box.

The Manual or Force switch is cleared.

Step 6 Return to your originating procedure (NTP).

DLP-F296 Clear a Lock On or Lockout in a 1+1 Protection Group

Purpose	This task clears the lock on or lockout to resume normal protection switching capability.
Tools/Equipment	None
Prerequisite Procedures	DLP-F240 Apply a Lock On in a 1+1 Group, page 17-33 or DLP-F241 Apply a Lockout in a 1+1 Group, page 17-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, choose the protection group that contains the card you want to clear.

Step 3 In the Selected Group area, choose the card you want to clear.

Step 4 In the Inhibit Switching area, click **Unlock**.

Step 5 Click **Yes** in the confirmation dialog box.

The Lock On or Lock Out is cleared.

Step 6 Return to your originating procedure (NTP).

DLP-F297 Initiate a Lockout on an SNCP Path

Purpose	This task applies a lock out of protection to an SNCP circuit so that working traffic cannot switch to the protection path. Lockouts prevent traffic from switching under any circumstance and have a higher priority than Manual or Force switches.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Circuits > Circuits** tabs.

Step 2 Click the path you want to switch and click **Edit**.

Step 3 In the Edit Circuit window, click the **SNCP Selectors** tab.

Step 4 In the Switch State column, click the row for the path you want to switch and select **Lockout of Protection**.

Note Refer to the *Cisco ONS 15600 SDH Reference Manual* for a description of protection switching and switch state priorities.

Step 5 Click **Apply**.

Working traffic is prevented from switching to the protect path.To clear the SNCP path Lock Out, complete the "DLP-F298 Clear a Switch or Lockout on an SNCP Circuit" task on page 17-88.

Step 6 Return to your originating procedure (NTP).

DLP-F298 Clear a Switch or Lockout on an SNCP Circuit

Purpose	This task clears an external switching command on an SNCP circuit.
Tools/Equipment	None
Prerequisite Procedures	DLP-F242 Initiate a Manual Switch on an SNCP Circuit, page 17-35, or DLP-F243 Initiate a Force Switch to an SNCP Circuit, page 17-35, or DLP-F297 Initiate a Lockout on an SNCP Path, page 17-87
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **Circuits > Circuits** tabs.

Step 2 Click the path you want to switch and click **Edit**.

Step 3 In the Edit Circuit window, click the **SNCP Selectors** tab.

Step 4 In the Switch State column, click the row for the path you want to switch and select **Clear**.

Step 5 Click **Apply**.

Note This task does revert traffic unless ports are configured for revertive switching.

Step 6 Return to your originating procedure (NTP).

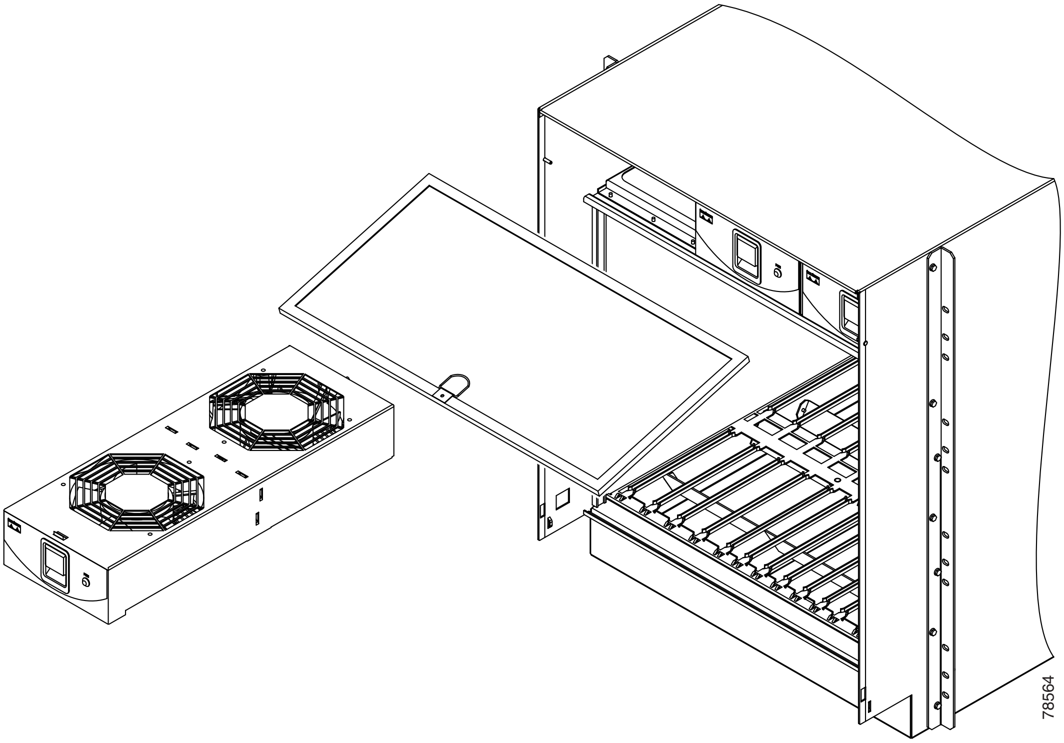
DLP-F299 Verify Fan Operation

Purpose	This task verifies that all fans are working before you insert the cards. Insufficient cooling by the fans can damage the equipment.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **Voltage is present on the backplane when the system is operating. To reduce risk of an electric shock, keep hands and fingers out of the power supply bays and backplane areas.** Statement 166

Step 1 Locate the three fan trays at the front of the bay. Figure 17-11 shows an unpopulated ONS 15600 SDH with one of the three fan trays and the fan-tray air filter removed.

Figure 17-11 ONS 15600 SDH Shelf with One Fan Tray and Air Filter Removed



Step 2 To ensure the three front fans are operating, carefully place your hand in the card cage two to three inches (50 to 76 mm) from the top of the cage, palm up, to feel for air flow from each fan. If you do not feel air flow from one or more fans, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* and make sure all fans work before you install any cards.

Step 3 To ensure the three rear fans are operating, at the back of the bay carefully place your hand in the fan outlet area above the CAP and place your palm face down on the grate to feel for air flow from each fan. If you do not feel air flow from one or more fans, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* and make sure all fans work before you install any cards.

Step 4 Return to your originating procedure (NTP).

CHAPTER 18

DLPs F300 to F400

DLP-F300 Install Fiber-Optic Cables for SNCP Configurations

Purpose	This task installs the fiber-optic cables to the SNCP ports at each node. See Chapter 5, “Turn Up a Network.” to provision and test SNCP configurations.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-F119 Install the STM-N Cards, page 2-4
	NTP-F231 Clean Fiber Connectors and Adapters, page 14-16
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution To avoid loss of traffic, do not create an SNCP using two ports on the same card. You can create an SNCP on different ports on the same side of the shelf, but Cisco recommends using one port on one side of the shelf and another port on the opposite side.

Note See Table 16-1 on page 16-19 and Table 16-2 on page 16-19 for OGI connector pinouts of STM-16 and STM-64 cards.

Step 1 Plug the fiber into the transmit (Tx) connector of an STM-N card at one node and plug the other end of the fiber into the receive (Rx) connector of an STM-N card at the adjacent node. The card will display an SF LED if the transmit and receive fibers are mismatched (one fiber connects a receive port on one card to a receive port on another card, or the same situation with transmit ports).

Step 2 Repeat Step 1 until you have configured the ring.

Step 3 Return to your originating procedure (NTP).

DLP-F301 Edit SNCP Dual-Ring Interconnect Circuit Hold-Off Timer

Purpose	This task changes the amount of time a path selector switch is delayed for circuits routed on an SNCP dual-ring interconnect (DRI) topology. Setting a switch hold-off time (HOT) prevents unnecessary back and forth switching when a circuit is routed through multiple SNCP selectors.
Tools/Equipment	None
Prerequisite Procedures	NTP-F152 Provision SNCP Nodes, page 5-13 DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Cisco recommends that you set the DRI port HOT value to zero and the circuit path selector HOT value to a number equal to or greater than zero.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Circuits** tab.

Step 3 Click the SNCP circuit you want to edit, then click **Edit**.

Step 4 In the Edit Circuit window, click the **SNCP Selectors** tab.

Step 5 Create a hold-off time for the circuit source and destination ports:

a. In the Hold-Off Timer area, double-click the cell of the circuit source port (top row), then type the new hold-off time. The range is 0 to 10,000 ms in increments of 100.

b. In the Hold-Off Timer area, double-click the cell of the circuit destination port (bottom row), then type the hold-off time entered in Step a.

Step 6 Click **Apply**, then close the Edit Circuit window by choosing **Close** from the File menu.

Step 7 Return to your originating procedure (NTP).

DLP-F302 Change Tunnel Type

Purpose	This task converts a traditional DCC tunnel to an IP-encapsulated tunnel or an IP-encapsulated tunnel to a traditional DCC tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-F244 Create a DCC Tunnel, page 17-36 DLP-F166 Create an IP-Encapsulated Tunnel, page 16-9
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > Overhead Circuits** tabs.

Step 3 Click the circuit tunnel that you want to convert.

Step 4 Click **Edit**.

Step 5 In the Edit Circuit window, click the **Tunnel** tab.

Step 6 In the Attributes area, complete the following:

- If you are converting a traditional DCC tunnel to an IP-encapsulated tunnel, check the **Change to IP Tunnel** check box and type the percentage of total DCC bandwidth used in the Maximum Bandwidth field (the minimum percentage is 10 percent).
- If you are converting an IP tunnel to a traditional DCC tunnel, check the **Change to RS-DCC Tunnel** check box.

Step 7 Click **Apply**.

Step 8 In the confirmation dialog box, click **Yes** to continue.

Step 9 In the Circuit Changed status box, click **OK** to acknowledge that the circuit change was successful.

Step 10 Return to your originating procedure (NTP).

DLP-F303 Delete Overhead Circuits

Purpose	This task deletes overhead circuits. ONS 15600 SDH overhead circuits include DCC tunnels and IP-encapsulated tunnels.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

⚠ **Caution** Deleting overhead circuits is service affecting if the circuit ports are in service. To put circuit ports out of service, see the "DLP-F254 Change the Service State for a Port" task on page 17-48.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > Overhead Circuits** tabs.

Step 3 Click the overhead circuit that you want to delete.

Step 4 Click **Delete**.

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

Step 6 Return to your originating procedure (NTP).

DLP-F304 Repair an IP Tunnel

Purpose	This task repairs circuits that are in the PARTIAL status as a result of node IP address changes.
Tools/Equipment	None
Prerequisite Procedures	See Chapter 6, "Create Circuits." for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Obtain the original IP address of the node in question.

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

Step 3 From the Tools menu, choose **Overhead Circuits > Repair IP Circuits**.

Step 4 Review the text in the IP Repair wizard and click **Next**.

Step 5 In the Node IP address area, complete the following:

- Node—Choose the node that has a PARTIAL circuit.
- Old IP Address—Type the node's original IP address.

Step 6 Click **Next**.

Step 7 Click **Finish**.

Step 8 Return to your originating procedure (NTP).

DLP-F305 Provision Path Trace on Circuit Source and Destination Ports

Purpose	This task creates a path trace on VC circuit source ports and destination.
Tools/Equipment	ONS 15600 SDH cards capable of transmitting and receiving path trace must be installed at the circuit source and destination ports. See Table 18-1 for a list of cards.
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This task assumes you are setting up path trace on a bidirectional circuit and setting up transmit strings at the circuit source and destination.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Circuits** tab.

Step 3 For the VC circuit you want to monitor, verify that the source and destination ports are on a card that can transmit and receive the path trace string. Table 18-1 provides a list of cards that support path trace.

Table 18-1 ONS 15600 SDH Cards for Path Trace

J1 Function	Cards
Transmit and Receive	ASAP (Gigabit Ethernet ports)
Receive Only	ASAP (Optical ports) OC48/STM16 LR/LH 16 Port 1550 OC48/STM16 SR/SH 16 Port 1310 OC192/STM64 LR/LH 4 Port 1550 OC192/STM64 SR/SH 4 Port 1310 OC192/STM64 4 Port ITU C-Band

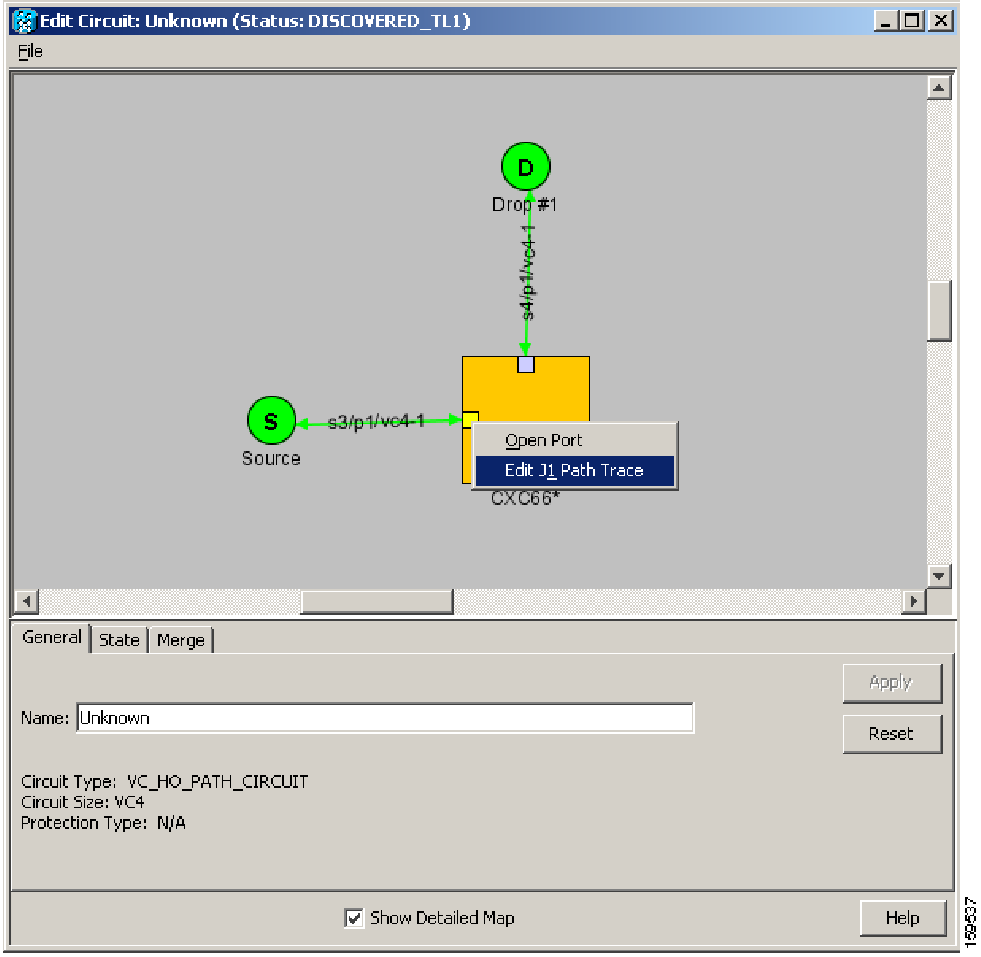
Step 4 Choose the VC circuit you want to trace, then click **Edit**.

Step 5 In the Edit Circuit window, click the **Show Detailed Map** check box at the bottom of the window. A detailed map of the source and destination ports appears.

Step 6 Provision the circuit source transmit string:

a. On the detailed circuit map, right-click the circuit source port (the square on the left or right of the source node icon) and choose **Edit J1 Path Trace (port)** from the shortcut menu. Figure 18-1 shows an example.

Figure 18-1 Selecting the Edit Path Trace Option



Name: Unknown

Circuit Type: VC_HO_PATH_CIRCUIT
Circuit Size: VC4
Protection Type: N/A

☑ Show Detailed Map

b. In the New Expected String field, enter the circuit source transmit string. Enter a string that makes the source port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Expected String field is left blank, the J1 transmits a string of null characters.

c. Click **Apply**, then click **Close**.

Step 7 Provision the circuit destination transmit string:

a. On the detailed circuit map, right-click the circuit destination port and choose **Edit Path Trace** from the shortcut menu (Figure 18-1).

b. In the New Expected String field, enter the string that you want the circuit destination to transmit. Enter a string that makes the destination port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Expected String field is left blank, the J1 transmits a string of null characters.

c. Click **Apply**.

Step 8 Provision the circuit destination expected string:

a. On the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down list:

- Auto—The first string received from the source port is automatically provisioned as the current expected string. An alarm is raised when a string that differs from the baseline is received.
- Manual—The string entered in the Current Expected String field is the baseline. An alarm is raised when a string that differs from the Current Expected String is received.

b. If you set the Path Trace Mode field to Manual, enter the string that the circuit destination should receive from the circuit source in the New Expected String field. If you set Path Trace Mode to Auto, skip this step.

c. Click the **Disable AIS and RDI if TIM-P is detected** check box if you want to suppress the alarm indication signal (AIS) and remote defect indication (RDI) when the VC Path Trace Identifier Mismatch Path (TIM-P) alarm appears. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for descriptions of alarms and conditions.

d. (Check box visibility depends on card selection.) Click the **Disable AIS on C2 Mis-Match** check box if you want to suppress the AIS when a C2 mismatch occurs.

e. Click **Apply**, then click **Close**.

Note It is not necessary to set the format (16 or 64 bytes) for the circuit destination expected string; the path trace process automatically determines the format.

Step 9 Provision the circuit source expected string:

a. In the Edit Circuit window (with Show Detailed Map chosen; see Figure 18-1 on page 18-6), right-click the circuit source port and choose **Edit Path Trace** from the shortcut menu.

b. In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down list:

- Auto—Uses the first string received from the port at the other path trace end as the baseline string. An alarm is raised when a string that differs from the baseline is received.
- Manual—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.

c. If you set the Path Trace Mode field to Manual, enter the string that the circuit source should receive from the circuit destination in the New Expected String field. If you set Path Trace Mode to Auto, skip this step.

d. Click the **Disable AIS and RDI if TIM-P is detected** check box if you want to suppress the AIS and RDI when the TIM-P alarm appears. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for descriptions of alarms and conditions.

e. (Check box visibility depends on card selection.) Click the **Disable AIS on C2 Mis-Match** check box if you want to suppress the AIS when a C2 mismatch occurs.

f. Click **Apply**.

Note It is not necessary to set the format (16 or 64 bytes) for the circuit source expected string; the path trace process automatically determines the format.

Step 10 After you set up the path trace, the received string appears in the Received field on the path trace setup window. The following options are available:

- Click **Hex Mode** to display path trace in hexadecimal format. The button name changes to ASCII Mode. Click it to return the path trace to ASCII format.
- Click the **Reset** button to reread values from the port.

- Click **Default** to return to the path trace default settings (Path Trace Mode is set to Off and the New Transmit and New Expected Strings are null).

Caution Clicking Default will generate alarms if the port on the other end is provisioned with a different string.

The expect and receive strings are updated every few seconds if the Path Trace Mode field is set to Auto or Manual.

Step 11 Click **Close**.

The detailed circuit window indicates path trace with an M (manual path trace) or an A (automatic path trace) at the circuit source and destination ports.

Step 12 Return to your originating procedure (NTP).

DLP-F306 Provision Path Trace on STM-N Ports

Purpose	This task monitors a path trace on STM-N ports within the circuit path.
Tools/Equipment	The STM-N ports you want to monitor must be on STM-N cards capable of receiving path trace. See Table 18-1 on page 18-5.
Prerequisite Procedures	DLP-F305 Provision Path Trace on Circuit Source and Destination Ports, page 18-4 DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Other Node**. In the Select Node dialog box, choose the node where path trace was provisioned on the circuit source and destination ports.

Step 2 Click **Circuits**.

Step 3 Choose the VC circuit that has path trace provisioned on the source and destination ports, then click **Edit**.

Step 4 In the Edit Circuit window, click the **Show Detailed Map** check box at the bottom of the window. A detailed circuit graphic showing source and destination ports appears.

Step 5 In the detailed circuit map right-click the circuit STM-N port (the square on the left or right of the source node icon) and choose **Edit Path Trace** from the shortcut menu.

Note The STM-N port must be on a receive-only card listed in Table 18-1 on page 18-5. If not, the Edit Path Trace menu item will not appear.

Step 6 In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down list:

- Auto—Uses the first string received from the port at the other path trace end as the current expected string. An alarm is raised when a string that differs from the baseline is received. For STM-N ports, Auto is recommended because Manual mode requires you to trace the circuit on the Edit Circuit window to determine whether the port is the source or destination path.
- Manual—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.

Step 7 If you set the Path Trace Mode field to Manual, enter the string that the STM-N port should receive in the New Expected String field. To do this, trace the circuit path on the detailed circuit window to determine whether the port is in the circuit source or destination path, then set the New Expected String to the string transmitted by the circuit source or destination. If you set the Path Trace Mode field to Auto, skip this step.

Step 8 Click **Apply**, then click **Close**.

Step 9 Return to your originating procedure (NTP).

DLP-F307 Create Login Node Groups

Purpose	This task creates a login node group to display ONS 15600 SDH nodes that have an IP connection but not a DCC connection to the login node.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 NTP-F129 Log into the ONS 15600 SDH GUI, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu in node view, choose **Preferences**.

Step 2 Click the **Login Node Group** tab.

Step 3 Click **Create Group**.

Step 4 In the Create Login Group Name dialog box, enter a name for the group.

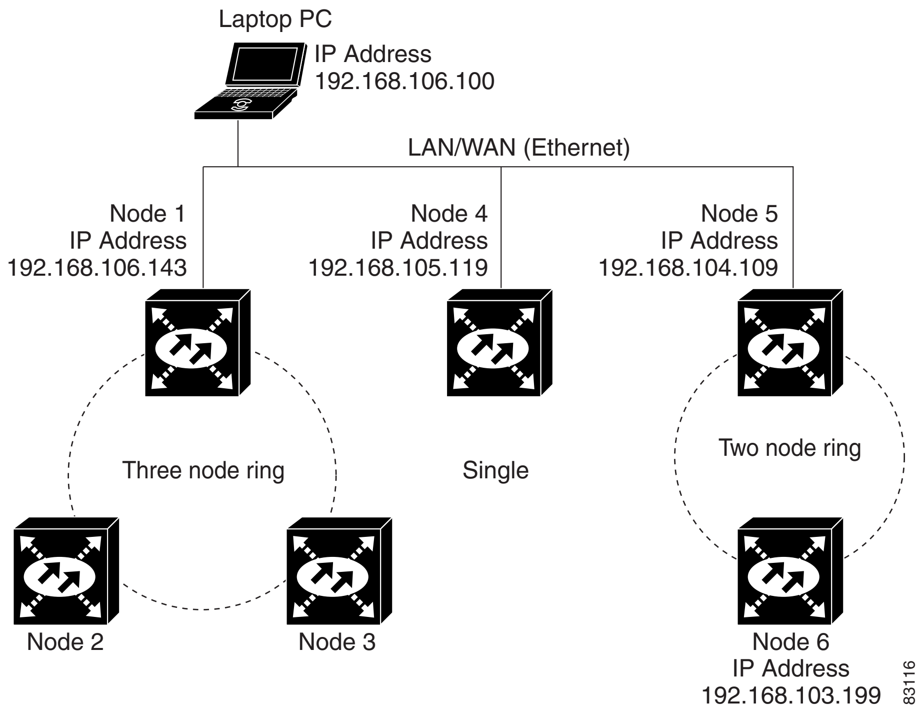
Step 5 Click **OK**.

Step 6 In the Members area, type the IP address (or node name) of a node you want to add to the group. Click **Add**. Repeat this step for each node that you want to add to the group.

Step 7 Click **OK**.

The next time you log into an ONS 15600 SDH, the login node group will be available in the Additional Nodes list of the Login dialog box. For example, in Figure 18-2, a login node group is created that contains the IP addresses for Nodes 1, 4, and 5. During login, if you choose this group from the Additional Nodes list and Disable Network Discovery is not selected, all nodes in the figure appear. If the login group and Disable Network Discovery are both selected, Nodes 1, 4, and 5 appear. You can create as many login groups as you need. The groups are stored in the CTC preferences file and are not visible to other users.

Figure 18-2 Login Node Group



Step 8 Return to your originating procedure (NTP).

DLP-F308 Delete a Node from the Current Session or Login Group

Purpose	This task removes a node from the current CTC session or login node group. To remove a node from a login node group that is not the current one, see "DLP-F312 Delete a Node from a Specified Login Node Group" task on page 18-13.
Tools	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the node that you want to delete.

Step 3 From the File menu, click **Delete Selected Node**.

After a few seconds, the node disappears from the network view map.

Step 4 Return to your originating procedure (NTP).

DLP-F309 Configure the CTC Alerts Dialog Box for Automatic Popup

Purpose	This task sets up the CTC Alerts dialog box to open for all alerts, for circuit deletion errors only, or never. The CTC Alerts dialog box displays information about network disconnection, Send-PDIP inconsistency, circuit deletion status, condition retrieval errors, and software download failure.
Tools	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the CTC Alerts toolbar icon.

Step 2 In the CTC Alerts dialog box, choose one of the following:

- **All alerts**—Sets the CTC Alerts dialog box to open automatically for all notifications.
- **Error alerts only**—Sets the CTC Alerts dialog box to open automatically for circuit deletion errors only.
- **Never**—Sets the CTC Alerts dialog box to never open automatically.

Step 3 Click **Close**.

Step 4 Return to your originating procedure (NTP).

DLP-F310 Change the JRE Version

Purpose	This task changes the Java Runtime Environment (JRE) version, which is useful if you would like to upgrade to a later JRE version from an earlier one without using the software CD. This does not affect the browser default version. After selecting the desired JRE version, you must exit CTC. The next time you log into a node, the new JRE version will be used.
Tools	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note JRE 5.0 is required to run Software R8.0.

Step 1 From the Edit menu, choose **Preferences**.

Step 2 Click the **JRE** tab. The JRE tab shows the current JRE version and the recommended version.

Step 3 Click the **Browse** button and navigate to the JRE directory on your computer.

Step 4 Choose the JRE version.

Step 5 Click **OK**.

Step 6 From the File menu, choose **Exit**.

Step 7 In the confirmation dialog box, click **Yes**.

Step 8 Return to your originating procedure (NTP).

DLP-F311 Remove Pass-through Connections

Purpose	This task removes pass-through connections from a node deleted from a ring.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into the deleted node.

Step 2 In the CTC Login dialog box, check the **Disable Network Discovery** check box.

Step 3 Choose **None** from the Additional Nodes drop-down list.

Step 4 Click the **Login** button.

Step 5 Click the **Circuits** tab. All internode circuits are shown as PARTIAL.

Step 6 Refer to the diagram or CTC printout you created in the "NTP-F215 Remove an MS-SPRing Node" procedure on page 13-5 or the "NTP-F217 Remove an SNCP Node" procedure on page 13-11. Find the circuits on the line cards of the removed node.

Step 7 Click the **Filter** button.

Step 8 Type the slot and port of a trunk card on the removed node.

Step 9 Click **OK**.

Step 10 In the Circuits tab, select all PARTIAL circuits that pass the filter and click the **Delete** button.

Note To select more than one circuit, press the **Shift** key and simultaneously click on all circuits to be deleted.

Step 11 Repeat Steps 6 through 10 for the other trunk card.

Step 12 Log out of CTC.

Step 13 Return to your originating procedure (NTP).

DLP-F312 Delete a Node from a Specified Login Node Group

Purpose	This task removes a node from a login node group.
Tools	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the CTC Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **Login Node Groups** tab.

Step 3 Click the login node group tab containing the node you want to remove.

Step 4 Click the node you want to remove, then click **Remove**.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-F313 Change a Circuit Service State

Purpose	This task changes the service state of a circuit.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Circuits** tab.

Step 3 Click the circuit with the state that you want to change.

Step 4 From the Tools menu, choose **Circuits > Set Circuit State**.

Step 5 In the Set Circuit State dialog box, choose the administrative state from the Target Circuit Admin State drop-down list:

- **Unlocked**—Puts the circuit cross-connects in the Unlocked-enabled service state.
- **Locked,disabled**—Puts the circuit cross-connects in the Locked-enabled,disabled service state. Traffic is not passed on the circuit.
- **Unlocked,automaticInService**—Puts the circuit cross-connects in the Unlocked-disabled,automaticInService service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to Unlocked-enabled.

- **Locked,maintenance**—Puts the circuit cross-connects in the Locked-enabled,maintenance service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use Locked,maintenance for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to Unlocked; Unlocked,automaticInService; or Locked,disabled when testing is complete.

Note Alternatively, you can choose the circuit on the Circuits tab, click the Edit button, then click the State tab on the Edit Circuits window.

For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Step 6 If you want to apply the state to the circuit source and destination ports, check the **Apply to Drop Ports** check box.

Note CTC will not allow you to change a drop port service state from Unlocked-enabled to Locked-enabled,disabled. You must first change a port to the Locked-enabled,maintenance service state before putting it in the Locked-enabled,disabled service state.

Step 7 Click **Apply**.

Step 8 If the Apply to Ports Results dialog box appears, view the results and click **OK**.

CTC will not change the service state of the circuit source and destination port in certain circumstances. For example, if a port is in loopback (Locked-enabled,loopback & maintenance), CTC will not change the port to Unlocked-enabled. In another example, if the circuit size is smaller than the port, CTC will not change the port service state from Unlocked-enabled to Locked-enabled,disabled. If CTC cannot change the port service state, you must change the port service state manually. For more information, see the "DLP-F254 Change the Service State for a Port" task on page 17-48.

Step 9 Return to your originating procedure (NTP).

DLP-F314 Provision MS-DCC Terminations

Purpose	This task creates the MS-DCC terminations required for alarms, administration, data, signal control information, and messages. In this task, you can also set up the node so that it has direct IP access to a far-end non-ONS node over the DCC network.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note When MS-DCC is provisioned, an RS-DCC termination is allowed on the same port, but is not recommended. RS-DCC and MS-DCC are only needed on the same port during a software upgrade if the software version does not support MS-DCC. Changing configuration of a port having MS-DCC termination to RS-DCC termination is allowed. During this procedure both MS-DCC and RS-DCC terminations can be present on the same port. Once the RS-DCC termination is configured see "DLP-F253 Provision RS-DCC Terminations" task on page 17-46 delete the MS-DCC terminations as specified in"DLP-F322 Delete an MS-DCC Termination" task on page 18-20, and enable the OSPF on RS-DCC termination if not enabled see "DLP-F319 Change an RS-DCC Termination" task on page 18-19.

Step 1 In node view, click the **Provisioning > Comm Channels > MS-DCC** tabs.

Step 2 Click **Create.**

Step 3 In the Create MS-DCC Terminations dialog box, click the ports where you want to create the MS-DCC termination. To select more than one port, press the Shift key or the Ctrl key.

Note MS-DCC refers to the multiplex section DCC, which is used for ONS 15600 SDH DCC terminations. The SDH MS-DCCs and the RS-DCC (when not used as a DCC termination by the ONS 15600 SDH) can be provisioned as DCC tunnels. See the "DLP-F244 Create a DCC Tunnel" task on page 17-36.

Step 4 In the Port Admin State area, click **Set to unlocked** to put the port in service.

Step 5 Verify that the Disable OSPF on DCC Link check box is unchecked.

Step 6 If the RS-DCC termination is to include a non-ONS node, check the **Far End is Foreign** check box. This automatically sets the far-end node IP address to 0.0.0.0, which means that any address can be specified by the far end. To change the default to a specific the IP address, see the "DLP-F320 Change an MS-DCC Termination" task on page 18-19.

Step 7 In the Layer 3 area, perform one of the following:

- Check the IP box only—If the MS-DCC is between the ONS 15600 SDH and another ONS node and only ONS nodes reside on the network. The MS-DCC will use point-to-point protocol (PPP).
- Check the IP and OSI boxes—If the MS-DCC is between the ONS 15600 SDH and another ONS node and third party NEs that use the OSI protocol stack are on the same network. The MS-DCC will use PPP.

Note Checking only the OSI box (LAP-D) is not available for MS-DCCs.

Step 8 If you checked OSI, complete the following steps. If you checked IP only, continue with Step 9.

a. Click **Next**.

b. Provision the following fields:

   – Router—Sets the OSI router.

   – ESH—Sets the End System Hello propagation frequency. End system NEs transmit ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.

- ISH—Sets the Intermediate System Hello PDU propagation frequency. Intermediate system NEs send ISHs to other ESs and ISs to inform them about the IS NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- IIH—Sets the Intermediate System to Intermediate System Hello PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
- IS-IS Cost—Sets the cost for sending packets on the LAN subnet. The IS-IS protocol uses the cost to calculate the shortest routing path. The default metric cost for LAN subnets is 20. It normally should not be changed.

Step 9 Click **Finish**.

Note MS-DCC Termination Failure (EOC-L) and Loss of Signal (LOS) alarms appear until you create all network DCC terminations and put the DCC termination STM-N ports in service.

Step 10 Return to your originating procedure (NTP).

DLP-F315 Provision a Proxy Tunnel

Purpose	This task sets up a proxy tunnel to communicate with a non-ONS far-end node. Proxy tunnels are only necessary when the proxy server is enabled and a foreign DCC termination exists, or if static routes exist so that the DCC network is used to access remote networks or devices. You can provision a maximum of 12 proxy server tunnels.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 DLP-F253 Provision RS-DCC Terminations, page 17-46
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note If the proxy server is disabled, you cannot set up a proxy tunnel.

Step 1 Click the **Provisioning > Network > Proxy** subtabs.

Step 2 Click **Create**.

Step 3 In the Create Tunnel dialog box, complete the following:

- Source Address—Type the IP address of the source node (32 bit length) or source subnet (any other length).
- Length—Choose the length of the source subnet mask.
- Destination Address—Type the IP address of the destination node (32 bit length) or destination subnet (any other length).
- Length—Choose the length of the destination subnet mask.

Step 4 Click **OK**.

Step 5 Continue with your originating procedure (NTP).

DLP-F316 Provision a Firewall Tunnel

Purpose	This task provisions destinations that will not be blocked by the firewall. Firewall tunnels are only necessary when the proxy server is enabled and a foreign DCC termination exists, or if static routes exist so that the DCC network is used to access remote networks or devices. You can provision a maximum of 12 firewall tunnels.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
	DLP-F253 Provision RS-DCC Terminations, page 17-46
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note If the proxy server is configured as proxy-only or is disabled, you cannot set up a firewall tunnel.

Step 1 Click the **Provisioning > Network > Firewall** subtabs.

Step 2 Click **Create**.

Step 3 In the Create Tunnel dialog box, complete the following:

- Source Address—Type the IP address of the source node (32 bit length) or source subnet (any other length).
- Length—Choose the length of the source subnet mask.
- Destination Address—Type the IP address of the destination node (32 bit length) or destination subnet (any other length).
- Length—Choose the length of the destination subnet mask.

Step 4 Click **OK**.

Step 5 Continue with your originating procedure (NTP).

DLP-F317 Delete a Proxy Tunnel

Purpose	This task removes a proxy tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Click the **Provisioning > Network > Proxy** subtabs.

Step 2 Click the proxy tunnel that you want to delete.

Step 3 Click **Delete**.

Step 4 Return to your originating procedure (NTP).

DLP-F318 Delete a Firewall Tunnel

Purpose	This task removes a firewall tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Click the **Provisioning > Network > Firewall** subtabs.

Step 2 Click the firewall tunnel that you want to delete.

Step 3 Click **Delete**.

Step 4 Return to your originating procedure (NTP).

DLP-F319 Change an RS-DCC Termination

Purpose	This task modifies an RS-DCC termination. You can enable or disable Open Shortest Path First (OSPF) and enable or disable the foreign node setting.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **Provisioning > Comm Channels > RS-DCC** tabs.

Step 2 Click the RS-DCC that you want to change.

Step 3 Click **Edit**.

Step 4 In the RS-DCC Termination Editor dialog box, complete the following as necessary:

- Disable OSPF on RS-DCC Link—If checked, OSPF is disabled on the link. OSPF should be disabled only when the slot and port connect to third-party equipment that does not support OSPF.
- Far End is Foreign—Check this box to specify that the RS-DCC termination is a non-ONS node.
- Far End IP—If you checked the Far End is Foreign check box, type the IP address of the far-end node or leave the 0.0.0.0 default. An IP address of 0.0.0.0 means that any address can be used by the far end.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-F320 Change an MS-DCC Termination

Purpose	This task modifies an SDH MS-DCC termination. You can enable or disable OSPF and enable or disable the foreign node setting.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **Provisioning > Comm Channels > MS-DCC** tabs.

Step 2 Click the MS-DCC that you want to change.

Step 3 Click **Edit**.

Step 4 In the MS-DCC Termination Editor dialog box, complete the following as necessary:

- Disable OSPF on MS-DCC Link—If checked, OSPF is disabled on the link. OSPF should be disabled only when the slot and port connect to third-party equipment that does not support OSPF.

- Far End is Foreign—Check this box to specify that the MS-DCC termination is a non-ONS node.
- Far end IP—If you checked the Far End is Foreign check box, type the IP address of the far-end node or leave the 0.0.0.0 default. An IP address of 0.0.0.0 means that any address can be used by the far end.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-F321 Delete an RS-DCC Termination

Purpose	This task deletes an RS-DCC termination.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Deleting an RS-DCC termination might cause you to lose visibility of nodes that do not have other data communications channels (DCCs) or network connections to the CTC computer.

Note If you have circuits traversing the fiber on which you delete a DCC termination, the circuits will go to an Incomplete state.

Step 1 In node view, click the **Provisioning > Comm Channel > RS-DCC** tabs.

Step 2 Click the RS-DCC termination to be deleted and click **Delete**. The Delete RS-DCC Termination dialog box appears.

Step 3 Click **Yes** in the confirmation dialog box. Confirm that the changes appear; if not, repeat the task.

Step 4 Return to your originating procedure (NTP).

DLP-F322 Delete an MS-DCC Termination

Purpose	This task deletes an SDH MS-DCC termination.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Deleting a DCC termination can cause you to lose visibility of nodes that do not have other DCCs or network connections to the CTC computer.

Step 1 Click the **Provisioning > Comm Channel > MS-DCC** tabs.

Step 2 Click the MS-DCC termination to be deleted and click **Delete**. The Delete MS-DCC Termination dialog box appears.

Step 3 Click **Yes** in the confirmation dialog box. Confirm that the changes appear; if not, repeat the task.

Step 4 Return to your originating procedure (NTP).

DLP-F323 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)

Purpose	This task reinitializes the ONS 15600 SDH using the CTC reinitialization (reinit) tool on a UNIX computer. Reinitialization uploads a new software package to the TSC cards, clears the node database, and restores the factory default parameters.
Tools/Equipment	Cisco ONS 15600 SDH System Software CD, Version 8.0 JRE 5.0 must be installed on the computer to log into the node at the completion of the reinitialization. The reinitialization tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 5.0.
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note Restoring a node to the factory configuration deletes all cross-connects on the node.

Step 1 Insert the Cisco ONS 15600 SDH System Software CD, Version 8.0, into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.

Step 2 To find the recovery tool file, go to the CISCO15600 SDH directory on the CD (usually /cdrom/cdrom0/CISCO15600SDH).

Step 3 If you are using a file explorer, double-click the RE-INIT.jar file. If you are working with a command line interface, run **java -jar RE-INIT.jar**. The NE Reinitialization window appears.

Step 4 Complete the following fields:

- GNE IP—If the node you are reinitializing is accessed through another node configured as a gateway network element (GNE), enter the GNE IP address. If you have a direct connection to the node, leave this field blank.
- Node IP—Enter the node name or IP address of the node that you are reinitializing.
- User ID—Enter the user ID needed to access the node.

- Password—Enter the password for the user ID.
- Upload Package—Check this box to send the software package file to the node. If unchecked, the software stored on the node is not modified.
- Force Upload—Check this box to send the software package file to the node even if the node is running the same software version. If unchecked, reinitialization will not send the software package if the node is already running the same version.
- Activate/Revert—Check this box to activate the uploaded software (if the software is a later than the installed version) or revert to the uploaded software (if the software is earlier than the installed version) as soon as the software file is uploaded. If unchecked, the software is not activated or reverted after the upload, allowing you to initiate the functions later from the node view Maintenance > Software tabs.
- Re-init Database—Check this box to send a new database to the node. (This is equivalent to the CTC database restore operation.) If unchecked, the node database is not modified.
- Confirm—Check this box if you want a warning message displayed before any operation is performed. If unchecked, reinitialization does not display a warning message.
- Search Path—Enter the path to the CISCO15600SDH folder on the CD drive.

Step 5 Click **Go**.

Caution Before continuing with the next step, verify that the database to upload is correct. You cannot reverse the upload process after you click Yes.

Step 6 Review the information on the Confirm NE Re-Initialization dialog box, then click **Yes** to start the reinitialization.

The reinitialization begins. After the software is downloaded and activated, and the database is uploaded to the TSC cards, “Complete” appears in the status bar and the TSC cards will reboot. Wait a few minutes for the reboot to complete.

Step 7 After the reboot is complete, log into the node using the “DLP-F181 Log into CTC” task on page 16-34.

Step 8 Complete the “NTP-F133 Set Up Date, Time, and Contact Information” procedure on page 4-4.

Step 9 Return to your originating procedure (NTP).

DLP-F324 Provision ASAP Ethernet Ports

Purpose	This task provisions ASAP Ethernet ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, double-click the ASAP card graphic to open the card.

Step 2 Click the **Provisioning** > **Ethernet > Ports** tabs.

Step 3 For each port, provision the following parameters:

- Port Name—If you want to label the port, type the port name.
- Admin State—Choose **Unlocked** to put the port in service.
- Enable Flow Control—Check this check box to enable flow control on the port (default). If you do not want to enable flow control, uncheck the box. The ASAP attempts to negotiate symmetrical flow control with the attached device.

Step 4 Click **Apply**.

Step 5 Refresh the Ethernet statistics:

a. Click the **Performance > Ethernet > Ether Ports > Statistics** tabs.

b. Click **Refresh**.

Note Reprovisioning an Ethernet port on the ASAP card does not reset the Ethernet statistics for that port.

Step 6 Return to your originating procedure (NTP).

DLP-F325 Provision ASAP POS Ports

Purpose	This task provisions ASAP packet-over-SDH (POS) ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, double-click the ASAP card graphic to open the card.

Step 2 Click the **Provisioning > Ethernet > POS Ports** tabs.

Step 3 For each POS port, provision the following parameters:

- Port Name—If you want to label the port, type the port name.
- Admin State—Choose **Unlocked** to put the port in service.
- Framing Type—Choose **GPF-F** POS framing (the default), **HDLC** POS, or **X.86** framing. The framing type needs to match the framing type of the POS device at the end of the SDH circuit.
- Encap CRC—With frame-mapped generic framing procedure (GFP-F) framing, the user can configure a **32-bit** cyclic redundancy check (CRC), **16-bit** CRC, or **none** (no CRC). High-level data link control (HDLC) framing provides a set 32-bit CRC. The CRC should be set to match the CRC of the POS device on the end of the SDH circuit.

Note The ASAP uses LEX encapsulation, which is the primary POS encapsulation used in ONS Ethernet cards.

Note An Encapsulation Mismatch Path (ENCAP-MISMATCH-P) alarm appears when a point-to-point circuit is created between two Ethernet card ports with incompatible encapsulation payload types.

Step 4 Click **Apply**.

Step 5 Refresh the POS statistics:

a. Click the **Performance > Ethernet > POS Ports > Statistics** tabs.

b. Click **Refresh**.

Step 6 Return to your originating procedure (NTP).

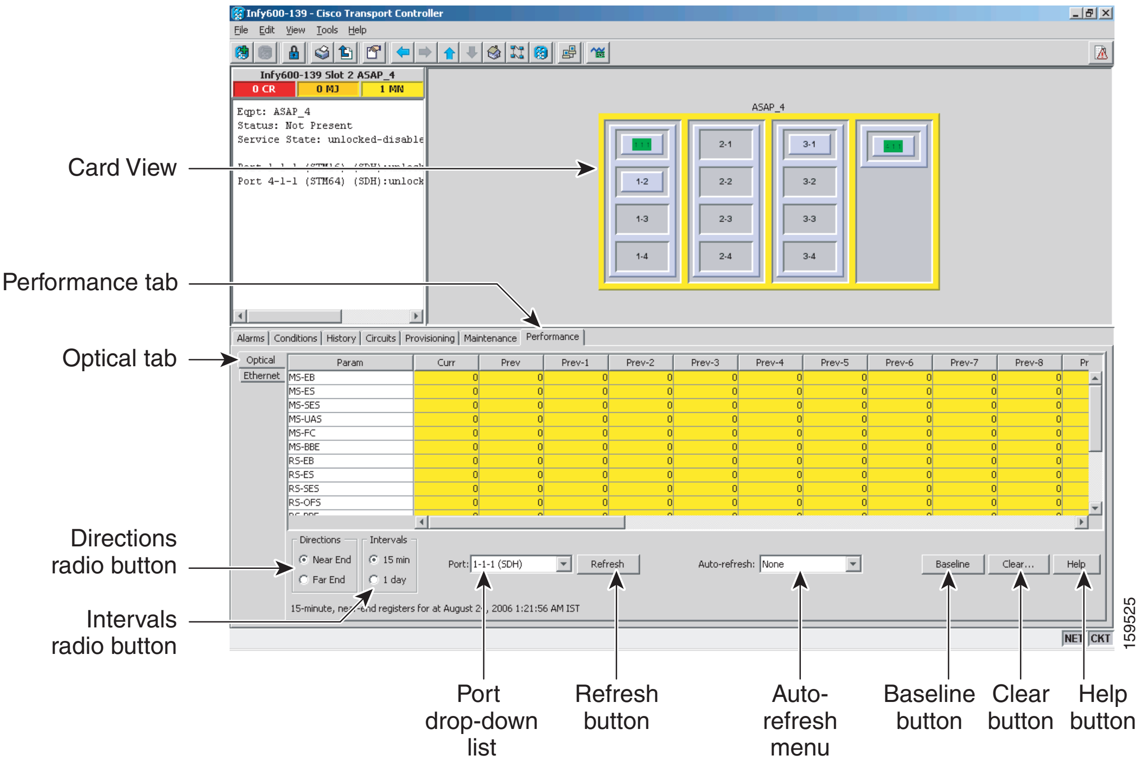
DLP-F326 View ASAP STM-N PM Parameters

Purpose	This task enables you to view performance monitoring (PM) counts on an ASAP card to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the ASAP card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance > Optical** tabs (Figure 18-3).

Figure 18-3 Viewing ASAP Card Performance Monitoring Information



```
Eqpt: ASAP_4
Status: Not Present
Service State: unlocked-disable

Port 1-1-1 (STM16) (SDH):unlock
Port 4-1-1 (STM64) (SDH):unlock
```

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Pr
MS-EB	0	0	0	0	0	0	0	0	0	0	
MS-ES	0	0	0	0	0	0	0	0	0	0	
MS-SES	0	0	0	0	0	0	0	0	0	0	
MS-UAS	0	0	0	0	0	0	0	0	0	0	
MS-FC	0	0	0	0	0	0	0	0	0	0	
MS-BBE	0	0	0	0	0	0	0	0	0	0	
RS-EB	0	0	0	0	0	0	0	0	0	0	
RS-ES	0	0	0	0	0	0	0	0	0	0	
RS-SES	0	0	0	0	0	0	0	0	0	0	
RS-OFS	0	0	0	0	0	0	0	0	0	0	

Directions: ● Near End ○ Far End

Intervals: ● 15 min ○ 1 day

Port: 1-1-1 (SDH)

Auto-refresh: None

15-minute, near-end registers for at August 24, 2006 1:21:56 AM IST

Step 3 In the Port drop-down list, choose the port that you want to monitor.

Step 4 Click **Refresh**.

Step 5 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the “Performance Monitoring” chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Step 6 To monitor another port on a multiport card, choose another port from the Port drop-down list and click **Refresh**.

Step 7 Return to your originating procedure (NTP).

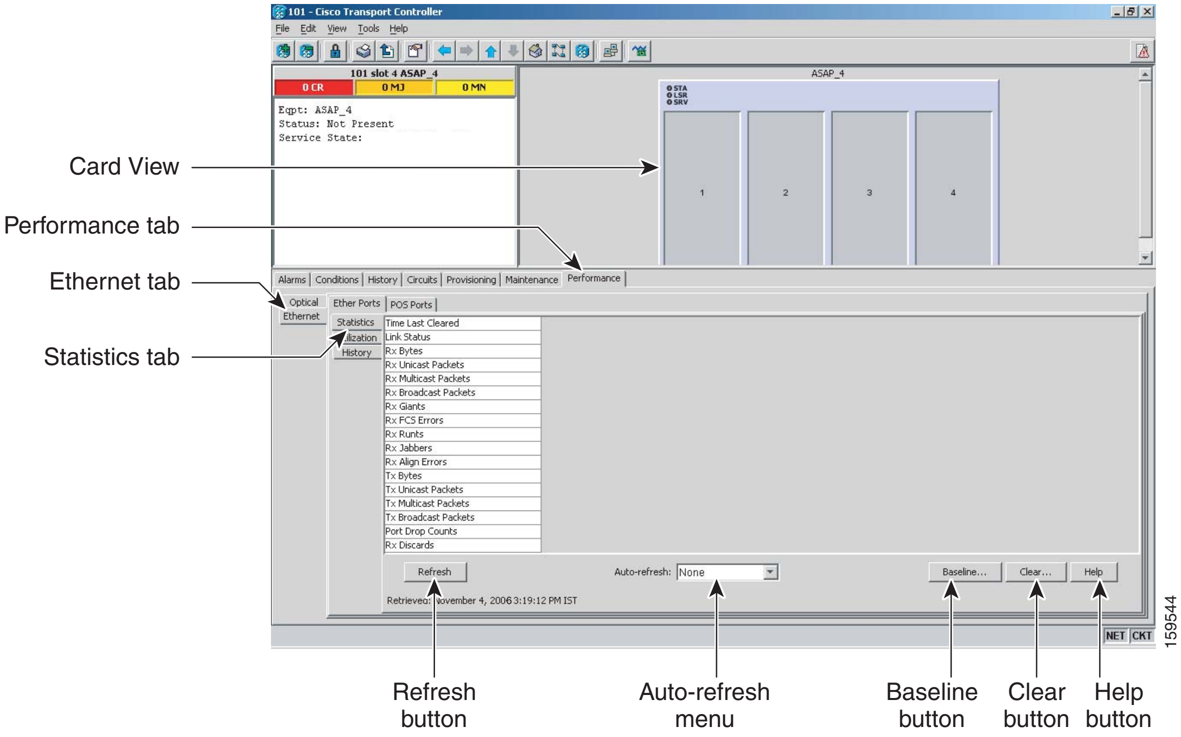
DLP-F327 View ASAP Ether Ports Statistics PM Parameters

Purpose	This task enables you to view current statistical PM counts on an ASAP card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Ethernet** > **Ether Ports** > **Statistics** tabs (Figure 18-4).

Figure 18-4 Ether Ports Statistics in the Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring statistics appear for each port on the card.

Step 4 View the PM parameter names appear in the Param column. The current PM parameter values appear in the Port # columns. For PM parameter definitions, refer to the “Performance Monitoring” chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Note To refresh, reset, or clear PM counts, see the “NTP-F184 Change the PM Display” procedure on page 8-2.

Step 5 Return to your originating procedure (NTP).

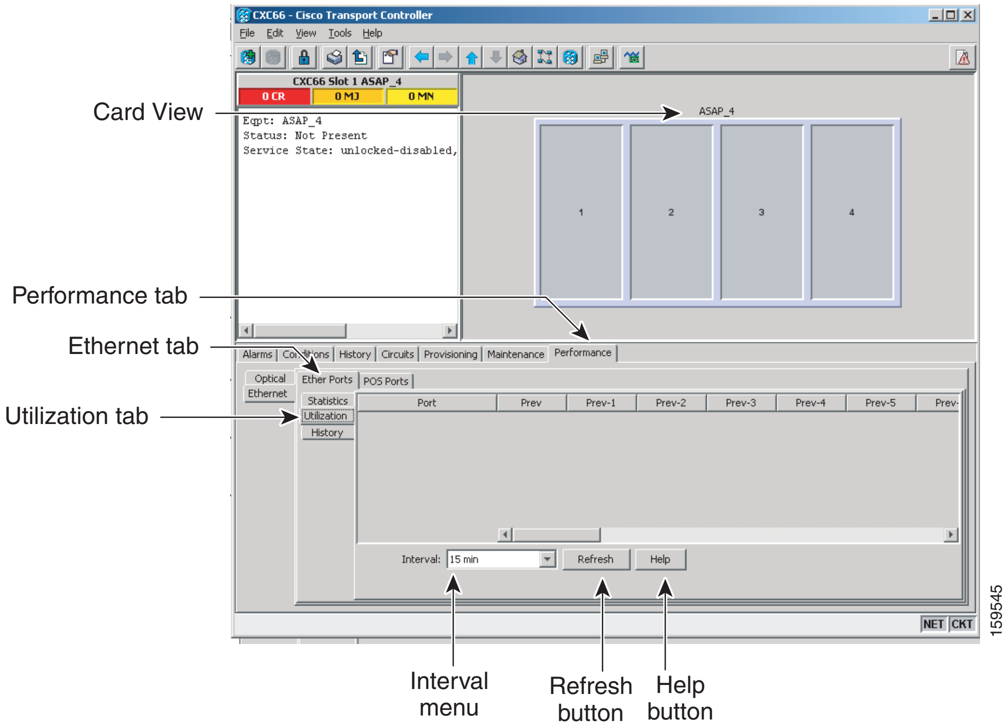
DLP-F328 View ASAP Ether Ports Utilization PM Parameters

Purpose	This task enables you to view line utilization PM counts on an ASAP card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the ASAP card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Ethernet** > **Ether Ports** > **Utilization** tabs (Figure 18-5).

Figure 18-5 Ether Ports Utilization in the Card View Performance Window



```
Eqpt: ASAP_4
Status: Not Present
Service State: unlocked-disabled,
```

Step 3 Click **Refresh**. Performance monitoring utilization values appear for each port on the card.

Step 4 View the Port # column for the port that you want to monitor.

Step 5 The transmit (Tx) and receive (Rx) bandwidth utilization values for the previous time intervals appear in the Prev-*n* columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-F184 Change the PM Display" procedure on page 8-2.

Step 6 Return to your originating procedure (NTP).

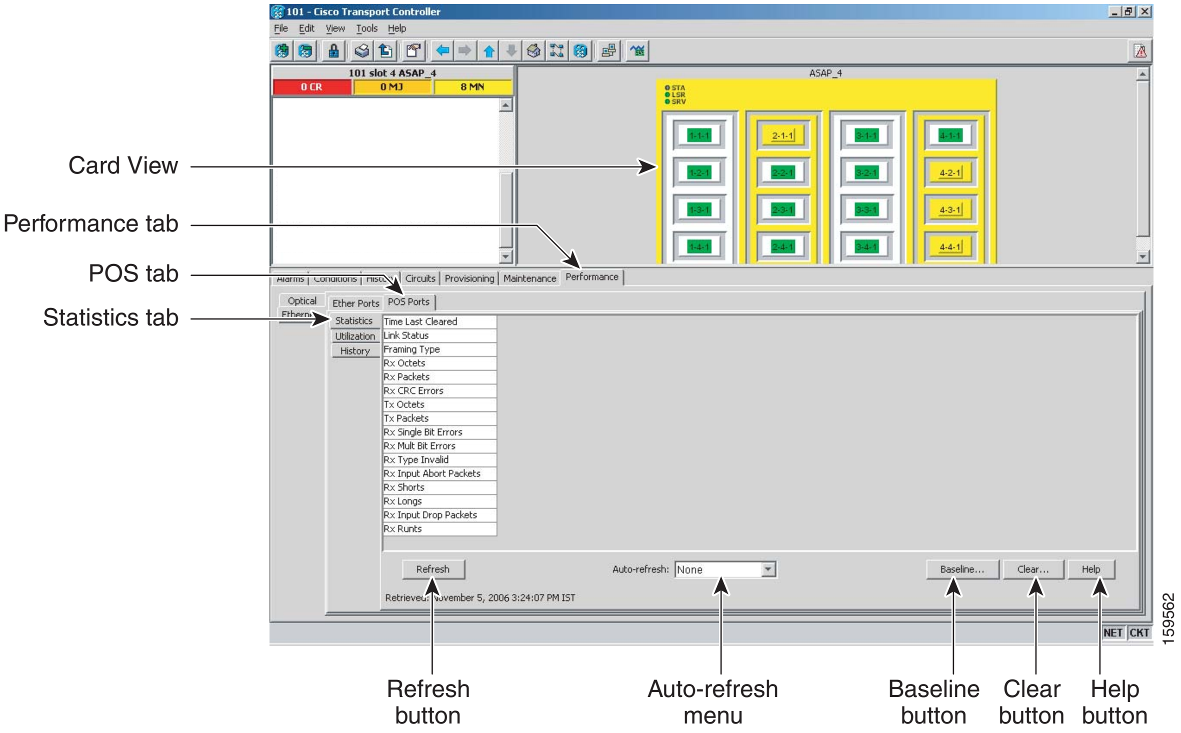
DLP-F329 View ASAP POS Ports Statistics PM Parameters

Purpose	This task enables you to view POS port PM counts at selected time intervals on an ASAP card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the ASAP card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Ethernet** > **POS Ports** > **Statistics** tabs (Figure 18-6).

Figure 18-6 POS Ports Statistics in the Card View Performance Window



101 - Cisco Transport Controller

101 slot 4 ASAP_4

Time Last Cleared
Link Status
Framing Type
Rx Octets
Rx Packets
Rx CRC Errors
Tx Octets
Tx Packets
Rx Single Bit Errors
Rx Mult Bit Errors
Rx Type Invalid
Rx Input Abort Packets
Rx Shorts
Rx Longs
Rx Input Drop Packets
Rx Runts

Auto-refresh: None

Retrieved: November 5, 2006 3:24:07 PM IST

Step 3 Click **Refresh**. Performance monitoring statistics appear for each port on the card.

Step 4 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Port # columns. For PM parameter definitions refer to the “Performance Monitoring” chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-F184 Change the PM Display" procedure on page 8-2.

Step 5 Return to your originating procedure (NTP).

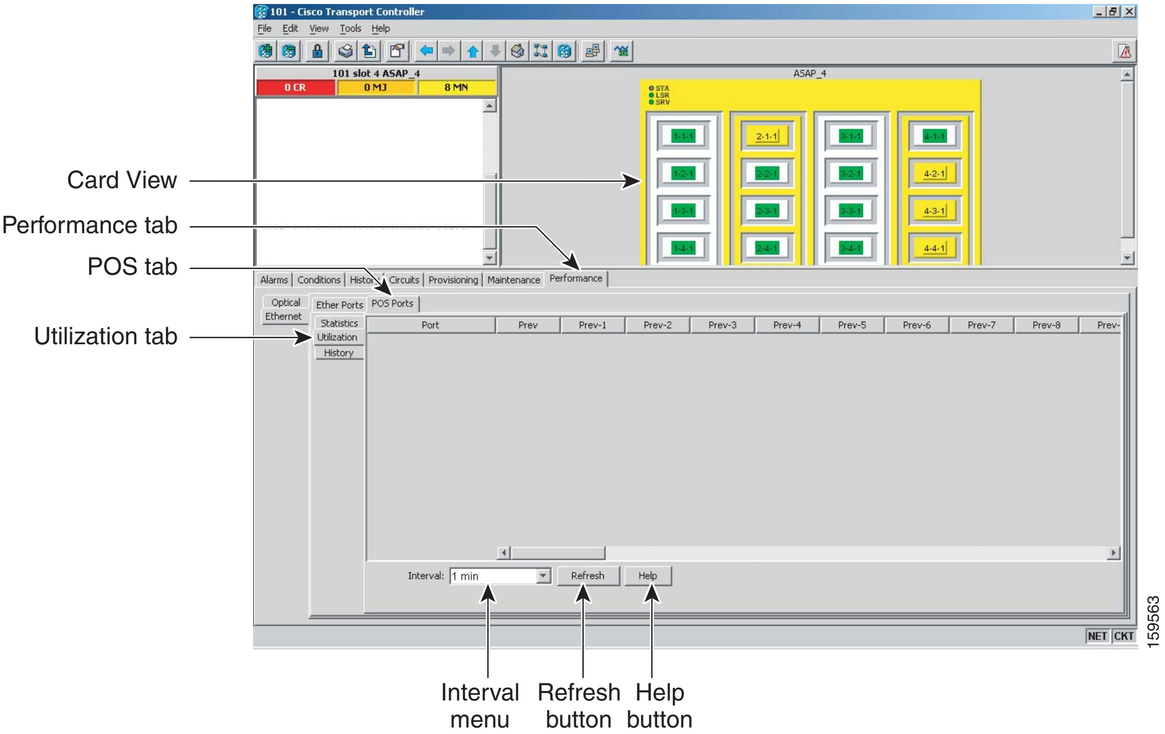
DLP-F330 View ASAP POS Ports Utilization PM Parameters

Purpose	This task enables you to view POS port utilization PM counts on an ASAP card and ports to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the ASAP card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Ethernet** > **POS Ports** > **Utilization** tabs (Figure 18-7).

Figure 18-7 POS Ports Utilization in the Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring utilization values for each port on the card appear.

Step 4 View the Port # column for the port that you want to monitor.

Step 5 The Tx and Rx bandwidth utilization values for the previous time intervals appear in the Prev-*n* columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-F184 Change the PM Display" procedure on page 8-2.

Step 6 Return to your originating procedure (NTP).

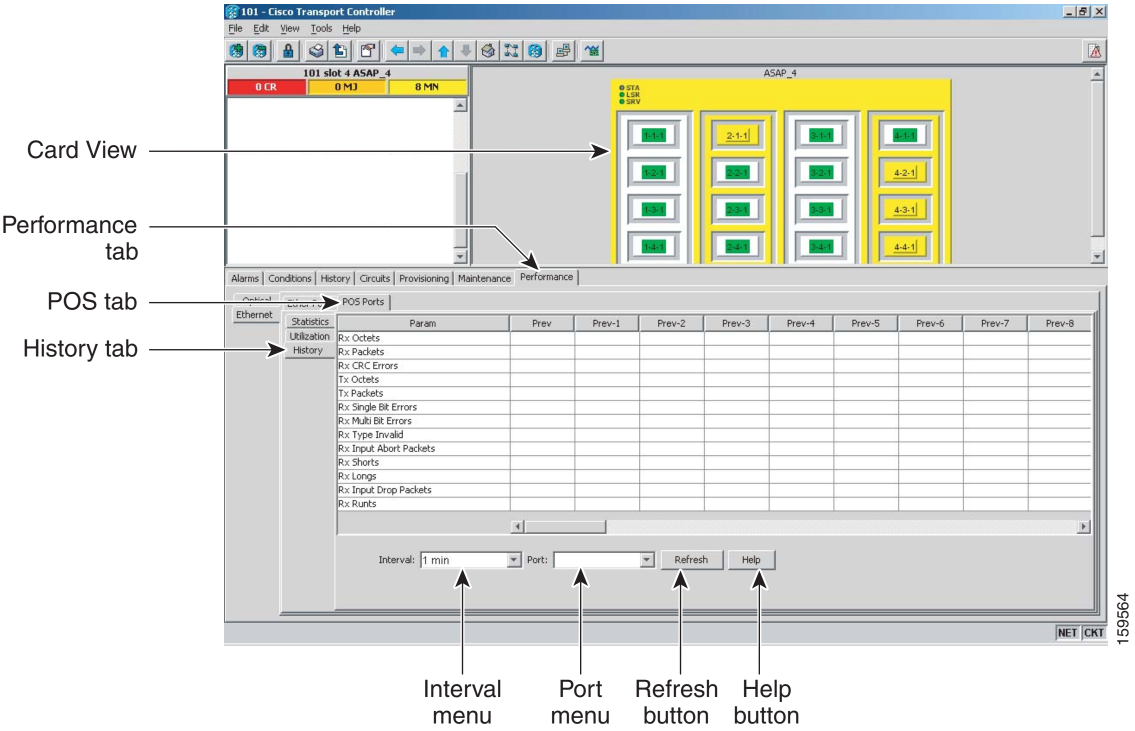
DLP-F331 View ASAP POS Ports History PM Parameters

Purpose	This task enables you to view historical PM counts at selected time intervals on an ASAP card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the ASAP card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Ethernet** > **POS Ports** > **History** tabs (Figure 18-8).

Figure 18-8 Ethernet POS Ports History in the Card View Performance Window



Param	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8
Rx Octets									
Rx Packets									
Rx CRC Errors									
Tx Octets									
Tx Packets									
Rx Single Bit Errors									
Rx Multi Bit Errors									
Rx Type Invalid									
Rx Input Abort Packets									
Rx Shorts									
Rx Longs									
Rx Input Drop Packets									
Rx Runts									

Interval: 1 min
Port:

Step 3 Click **Refresh**. Performance monitoring statistics appear for each port on the card.

Step 4 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Prev-*n* columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-F184 Change the PM Display" procedure on page 8-2.

Step 5 Return to your originating procedure (NTP).

DLP-F332 Change Node Access and PM Clearing Privilege

Purpose	This task provisions the physical access points and shell programs used to connect to the ONS 15600 SDH and sets the user security level that can clear node performance monitoring data.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Step 2 In the Access area, provision the following:

- LAN access—Choose one of the following options to set the access paths to the node:
  - **No LAN Access**—Allows access to the node only through data communications channel (DCC) connections. Access through the TSC RJ-45 port and backplane is not permitted.
  - **Front only**—Allows access through the TSC RJ-45 port. Access through the DCC and the backplane is not permitted.
  - **Backplane only**—Allows access through DCC connections and the backplane. Access through the TSC RJ-45 port is not allowed.
  - **Front and Backplane**—Allows access through DCC, TSC RJ-45, and backplane connections.
- Restore Timeout—Sets a time delay for enabling of front and backplane access when DCC connections are lost and “DCC only” is chosen in LAN Access. Front and backplane access is enabled after the restore timeout period has passed. Front and backplane access is disabled as soon as DCC connections are restored.
- Disable IPv4 access for IPv6 enabled ports— Select this option to disable IPv4 on ports which are IPv6 enabled. Before you select this option, ensure that IPv6 is enabled and the node is not in multishelf mode.

Step 3 In the Shell Access area, set the shell program used to access the node:

- Access State: Allows you to set the shell program access mode to Disable (disables shell access), Non-Secure, or Secure. Secure mode allows access to the node using the Secure Shell (SSH) program. SSH is a terminal-remote host Internet protocol that uses encrypted links.
- Telnet Port: Allows access to the node using the Telnet port. Telnet is the terminal-remote host Internet protocol developed for the Advanced Agency Research Project Network (ARPANET). Port 23 is the default.
- Enable Shell Password: If checked, enables the SSH password. To disable the password, you must uncheck the check box and click Apply. You must type the password in the confirmation dialog box and click OK to disable it.

Step 4 In the TL1 Access area, select the desired level of TL1 access. Disabled completely disables all TL1 access; Non-Secure, and Secure allows access using SSH.

Step 5 In the PM Clearing Privilege field, choose the minimum security level that can clear node PM data: PROVISIONING or SUPERUSER.

Step 6 Select the Enable Craft Port check box to turn on the shelf controller serial ports.

Step 7 Select the EMS access state from the list. Available states are Non-Secure and Secure (allows access using SSH).

In the TCC CORBA (IIOP/SSLIOP) Listener Port area, choose a listener port option:

- **Default - TCC Fixed**—Uses Port 57790 to connect to ONS 15454s on the same side of the firewall or if no firewall is used (default). This option can be used for access through a firewall if Port 57790 is open.
- **Standard Constant**—Uses Port 683 (IIOP) or Port 684 (SSLIOP), the Common Object Request Broker Architecture (CORBA) default port number.
- **Other Constant**—If the default port is not used, type the Internet Inter-ORB Protocol (IIOP) or SSLIOP port specified by your firewall administrator.

Step 8 In the SNMP Access area, set the Simple Network Management Protocol (SNMP) access state to Non-Secure or Disabled (disables SNMP access).

Step 9 Click **Apply**.

Step 10 Return to your originating procedure (NTP).

DLP-F333 Install the ASAP Carrier Modules

Purpose	This procedure explains how to install the carrier modules in the ONS 15600 SDH shelf.
Tools/Equipment	ASAP carrier modules
Prerequisite Procedures	NTP-F118 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the midplane with your hand or any metal tool, or you could shock yourself.** Statement 181

Caution Always use the supplied ESD wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-left outside edge of the shelf.

Warning **Class 1 laser product.** Statement 1008

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

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

Note For information about the ASAP card, refer to the *Cisco ONS 15600 SDH Reference Manual.*

Step 1 Remove the carrier module from the box and antistatic sleeve.

Caution Setting an ASAP carrier module on its connectors can cause damage to the connectors.

Step 2 Slide the module along the top and bottom guide rails into the correct slot: Slots 1 to 4 and 11 to 14 are available for traffic cards. Insert the card until it contacts the backplane.

Step 3 Close the ejectors.

Step 4 Verify the LED activity on the card faceplate:

1. The STAT, SRV, and LASER ON LEDs turn on for 20 seconds.
2. The STAT LED blinks and the other LEDs turn on for 30 to 50 seconds.
3. All LEDs blink once and the SRV and LASER ON LEDs illuminate.

Note If the LEDs do not turn on, check that the power breakers on the power distribution unit (PDU) are on. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Note If you insert a card into a slot provisioned for a different card, all red LEDs turn on and you will see a mismatched equipment (MEA) alarm for that slot when you open Cisco Transport Controller (CTC).

Step 5 After you have logged into CTC, verify that the card appears in the correct slot on the CTC node view. See Chapter 3, "Connect the PC and Log into the GUI" for CTC information and setup instructions.

Step 6 Return to your originating procedure (NTP).

DLP-F334 Verify Pass-Through Circuits

Purpose	This task verifies that circuits passing through a node that will be removed enter and exit the node on the same virtual container (VC).
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the Circuits window, choose a circuit that passes through the node that will be removed and click **Edit**.

Step 2 In the Edit Circuits window, check **Show Detailed Map**.

Step 3 Verify that the VC mapping on the node's east and west ports is the same. For example, if a circuit is mapping on the west port s2/p1/VC4-1 (Slot 2, Port 1, VC4-1), verify that the mapping is VC4-1 on the east port. If the circuit displays different VCs on the east and west ports, write down the name of the circuit.

Step 4 Repeat Steps 1 to 3 for each circuit in the Circuits tab.

Step 5 Delete and recreate each circuit recorded in Step 3 that entered/exited the node on different VCs. To delete the circuit, see the "DLP-F293 Delete Circuits" task on page 17-83. To create the circuit, see Chapter 6, "Create Circuits."

Step 6 Return to your originating procedure (NTP).

DLP-F335 Preprovision an SFP

Purpose	This procedure preprovisions Small Form-factor Pluggables (SFPs), which are referred to as pluggable port modules (PPMs) in CTC. Cisco-approved STM-1, STM-4, STM-16, Ethernet, and multirate PPMs are compatible with the ONS 15600 SDH. See the *Cisco ONS 15600 SDH Reference Manual* for a list of acceptable SFPs.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If you preprovision a multirate SFP, you must next select the line rate using the "DLP-F391 Provision an Optical Line Rate and Wavelength" task on page 18-107.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 to log into an ONS 15600 SDH on the network.

Step 2 Click the **Alarms** tab:

a. Verify that the alarm filter is not turned on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 as necessary.

b. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for procedures to clear alarms.

c. Complete the "DLP-F379 Export CTC Data" task on page 18-88 to export alarm and condition information.

Step 3 In node view, double-click the ASAP card where you want to provision PPM settings.

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

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

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

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

Step 7 Click **OK**. The newly created port appears on the Pluggable Port Modules pane. The row on the Pluggable Port Modules pane turns light blue and the Actual Equipment Type column lists the preprovisioned PPM as unknown until the actual SFP is installed. After the SFP is installed, the row on the pane turns white and the column lists the equipment name.

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

Step 9 On the Provisioning tab, click the **Line** subtab. If applicable for the PPM you are preprovisioning, use the **Reach** and **Wavelength** columns to configure these parameters as needed.

Note Only the parameters that are editable for the PPMs on a particular platform type are provisionable. For example, some platforms may not have PPMs with configurable wavelengths or reaches. In this case, wavelength and reach are not provisionable.

Step 10 Repeat Steps 1 to 10 create a second PPM.

Step 11 Click **OK**.

Step 12 When you are ready to install the SFP, complete the "DLP-F388 Install an SFP/XFP" task on page 18-104.

Step 13 Return to your originating procedure (NTP).

DLP-F336 Print CTC Data

Purpose	This task prints CTC windows and CTC table data such as alarms and inventory.
Equipment/Tools	A printer must be connected to the CTC computer
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From the CTC File menu, click **Print**.

Step 2 In the Print dialog box (Figure 18-9), choose an option:

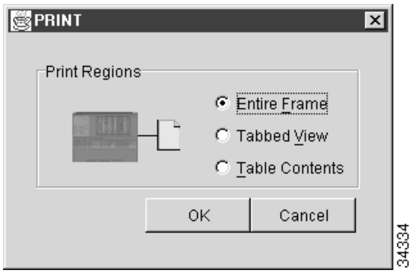
- Entire Frame—Prints the entire CTC window including the graphical view of the card, node, or network.
- Tabbed View—Prints the lower half of the CTC window.
- Table Contents—Prints CTC data in table format; this option is only available for CTC table data (see Table A-6 on page A-10). It does not apply to:
  - Provisioning > General window
  - Provisioning > SNMP window
  - Provisioning > Timing window
  - Provisioning > Network > Internal Subnet window
  - Provisioning > Network > General window
  - Provisioning > Security > Policy window
  - Provisioning > Security > Access window
  - Provisioning > Security > Legal Disclaimer window
  - Provisioning > OSI > Main Setup window
  - Provisioning > OSI > TARP > Config window
  - Maintenance > Database window

- Maintenance > Protection window
- Maintenance > Diagnostic window
- Maintenance > Preferred Copy window
- Maintenance > Timing > Source window

The Table Contents option prints all the data contained in a table and the table column headings. For example, if you print the History window Table Contents view, you print all data included in the table whether or not items appear in the window.

Tip When you print using the Tabbed View option, it can be difficult to distinguish whether the printout applies to the network, node, or card view. To determine the view, compare the tabs on the printout. The network, node, and card views are identical except that network view does not contain an Inventory or Performance tab.

Figure 18-9 Selecting CTC Data for Print



Step 3 Click **OK**.

Step 4 In the Windows Print dialog box, choose a printer and click **OK**.

Step 5 Return to your originating procedure (NTP).

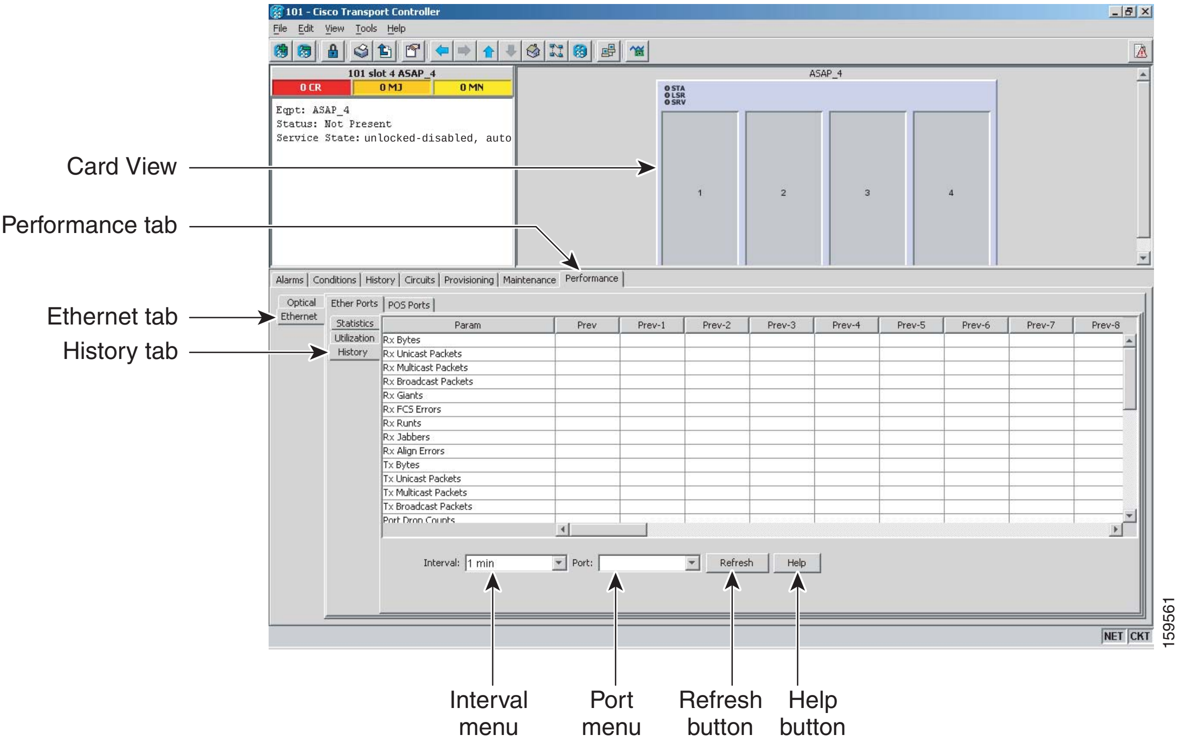
DLP-F337 View ASAP Ether Ports History PM Parameters

Purpose	This task enables you to view historical PM counts at selected time intervals on an ASAP card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the ASAP card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Ethernet** > **Ether Ports** > **History** tabs (Figure 18-10).

Figure 18-10 Ethernet Ether Ports History on the Card View Performance Window



Eqpt: ASAP_4
Status: Not Present
Service State: unlocked-disabled, auto

Param	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8
Rx Bytes									
Rx Unicast Packets									
Rx Multicast Packets									
Rx Broadcast Packets									
Rx Giants									
Rx FCS Errors									
Rx Runts									
Rx Jabbers									
Rx Align Errors									
Tx Bytes									
Tx Unicast Packets									
Tx Multicast Packets									
Tx Broadcast Packets									
Port Drop Counts									

Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Prev-*n* columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Note To refresh, reset, or clear PM counts, see the NTP-F184 Change the PM Display, page 8-2.

Step 5 Return to your originating procedure (NTP).

DLP-F338 Create a Two-Fiber MS-SPRing Using the MS-SPRing Wizard

Purpose	This task creates a two-fiber multiplex section-shared protection ring (MS-SPRing) at each MS-SPRing-provisioned node using the CTC MS-SPRing wizard. The MS-SPRing wizard checks to see that each node is ready for MS-SPRing provisioning, then provisions all the nodes at one time.
Tools/Equipment	None
Prerequisite Procedures	DLP-F293 Delete Circuits, page 17-83 DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > MS-SPRing** tabs.

Step 3 Click **Create MS-SPRing**.

Step 4 In the MS-SPRing Creation dialog box, set the MS-SPRing properties:

- Ring Type—Choose **two-fiber**.
- Speed—Choose the MS-SPRing ring speed: **STM-4**, **STM-16**, or **STM-64**. The speed must match the STM-N speed of the MS-SPRing trunk (span) ports.
- Ring Name—Assign a ring name. The name can be from 1 to 6 characters in length. Any alphanumeric string is permissible, and uppercase and lowercase letters can be combined. Do not use the character string All in either uppercase or lowercase letters; this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another MS-SPRing.
- Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path following a ring switch. The default is 5 minutes. Ring reversion can be set to Never.

Step 5 Click **Next**. If the network graphic appears, go to Step 6.

If CTC determines that an MS-SPRing cannot be created, for example, not enough optical cards are installed or it finds circuits with SNCP selectors, a “Cannot Create MS-SPRing” message appears. If this occurs, complete the following steps:

a. Click **OK**.

b. In the Create MS-SPRing window, click **Excluded Nodes**. Review the information explaining why the MS-SPRing could not be created, then click **OK**.

c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.

d. Complete the NTP-F147 Provision MS-SPRing Nodes, page 5-6, making sure all steps are completed accurately, then start this procedure again.

Step 6 In the network graphic, double-click an MS-SPRing span line. If the span line is DCC-connected to other MS-SPRing ports that constitute a complete ring, the lines turn blue. If the lines do not form a complete ring, double-click the span lines until a complete ring is formed. When the ring is DCC-connected, go to Step 7.

Step 7 Click **Finish**. If the MS-SPRing window appears with the MS-SPRing you created, go to Step 8. If a “Cannot Create MS-SPRing” or “Error While Creating MS-SPRing” message appears:

a. Click **OK**.

b. In the Create MS-SPRing window, click **Excluded Nodes.** Review the information explaining why the MS-SPRing could not be created, then click **OK**.

c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.

d. Complete the NTP-F147 Provision MS-SPRing Nodes, page 5-6, making sure all steps are completed accurately, then start this procedure again.

Note Some or all of the following alarms might briefly appear during MS-SPRing setup: E-W-MISMATCH, RING-MISMATCH, APSCIMP, APSCDFLTK, and MSSP-OOSYNC.

Step 8 Verify the following:

- On the network view graphic, a green span line appears between all MS-SPRing nodes.
- All E-W-MISMATCH, RING-MISMATCH, APSCIMP, APSCDFLTK, and MSSP-OOSYNC alarms are cleared. See the *Cisco ONS 15600 SDH Troubleshooting Guide* for alarm troubleshooting procedures.

Note The numbers in parentheses after the node name are the MS-SPRing node IDs assigned by CTC. Every ONS 15600 SDH in an MS-SPRing is given a unique node ID, 0 through 31. To change it, complete the "DLP-F340 Change an MS-SPRing Node ID" task on page 18-41.

Step 9 Return to your originating procedure (NTP).

DLP-F339 Create a Two-Fiber MS-SPRing Manually

Purpose	This tasks creates a two-fiber MS-SPRing at each MS-SPRing-provisioned node without using the MS-SPRing wizard.
Tools/Equipment	None
Prerequisite Procedures	NTP-F147 Provision MS-SPRing Nodes, page 5-6 DLP-F181 Log into CTC, page 16-34
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > MS-SPRing** tabs.

Step 2 Click **Create**.

Step 3 In the Suggestion dialog box, click **OK**.

Step 4 In the Create MS-SPRing dialog box, set the MS-SPRing properties:

- Ring Type—Choose **two-fiber**.
- Ring Name—Assign a ring name. You must use the same ring name for each node in the MS-SPRing. Any alphanumeric character string is permissible, and uppercase and lowercase letters can be combined. Do not use the character string All in either uppercase or lowercase letters; this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another MS-SPRing.
- Node ID—Choose a Node ID from the drop-down list (0 through 31). The Node ID identifies the node to the MS-SPRing. Nodes in the same MS-SPRing must have unique Node IDs.
- Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path. The default is 5 minutes. All nodes in a MS-SPRing must have the same reversion time setting.
- West Line—Assign the west MS-SPRing port for the node from the drop-down list.

Note The east and west ports must match the fiber connections and DCC terminations set up in the NTP-F147 Provision MS-SPRing Nodes, page 5-6.

- East Line—Assign the east MS-SPRing port for the node from the drop-down list.

Step 5 Click **OK**.

Note Some or all of the following alarms will appear until all the MS-SPRing nodes are provisioned: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, and MSSP-OOSYNC. The alarms will clear after you configure all the nodes in the MS-SPRing.

Step 6 From the View menu, choose **Go to Other Node**.

Step 7 In the Select Node dialog box, choose the next node that you want to add to the MS-SPRing.

Step 8 Repeat Steps 1 through 7 at each node that you want to add to the MS-SPRing. When all nodes have been added, continue with Step 9.

Step 9 From the View menu, choose **Go to Network View**. After 10 to 15 seconds, verify the following:

- A green span line appears between all BLSR nodes.
- All E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, and MSSP-OOSYNC alarms are cleared.

Step 10 Return to your originating procedure (NTP).

DLP-F340 Change an MS-SPRing Node ID

Purpose	This task changes an MS-SPRing node ID.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 On the network map, double-click the node with the node ID you want to change.

Step 3 From node view, click the **Provisioning > MS-SPRing** tabs.

Step 4 Choose a Node ID number. Do not choose a number already assigned to another node in the same MS-SPRing.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

DLP-F341 MS-SPRing Exercise Ring Test

Purpose	This task tests the MS-SPRing ring functionality without switching traffic. Ring exercise conditions (including the K-byte pass-through) are reported and cleared within 10 to 15 seconds.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Provisioning > MS-SPRing** tabs.

Step 3 Click the row of the MS-SPRing you will exercise, then click **Edit**.

Step 4 Exercise the west port:

a. Right-click the west port of any MS-SPRing node and choose **Set West Protection Operation**. (To move a graphic icon, press **Ctrl** while you drag and drop it to a new location.)

Note For two-fiber MS-SPRings, the squares on the node icons represent the MS-SPRing working and protect channels. You can right-click either channel.

b. In the Set West Protection Operation dialog box, choose **EXERCISE RING** from the drop-down list.

c. Click **OK**.

d. In the Confirm MS-SPRing Operation dialog box, click **Yes**.

On the network view graphic, an E appears on the working MS-SPRing channel where you invoked the protection switch. The E will appear for 10 to 15 seconds, then disappear.

Step 5 Exercise the east port:

a. Right-click the east port of any MS-SPRing node and choose **Set East Protection Operation**.

Note For two-fiber MS-SPRings, the squares on the node icons represent the MS-SPRing working and protect channels. You can right-click either channel.

b. In the Set East Protection Operation dialog box, choose **EXERCISE RING** from the drop-down list.

c. Click **OK**.

d. In the Confirm MS-SPRing Operation dialog box, click **Yes**.

On the network view graphic, an E appears on the MS-SPRing channel where you invoked the exercise. The E will appear for 10 to 15 seconds, then disappear.

Step 6 In the Cisco Transport Controller window, click the **History** tab. Verify that an Exercising Ring Successfully (EXERCISING-RING) condition appears for the node where you exercised the ring. Other conditions that appear include KB-PASSTHR and FE-EXERCISING-RING.

If you do not see any MS-SPRing exercise conditions, click the **Filter** button and verify that filtering is not turned on. Also, check that alarms and conditions are not suppressed for a node or MS-SPRing drop cards. See the "NTP-F195 Suppress and Restore Alarm Reporting" procedure on page 9-7 for more information.

Step 7 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 for instructions.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for alarm clearing procedures.

Step 8 From the File menu, choose **Close** to close the MS-SPRing window.

Step 9 Return to your originating procedure (NTP).

DLP-F342 MS-SPRing Switch Test

Purpose	This task verifies that protection switching is working correctly in an MS-SPRing.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > MS-SPRing** tabs.

Step 3 Click the row of the MS-SPRing you will switch, then click **Edit**.

Step 4 Initiate a Force Ring switch on the west port:

a. Right-click any MS-SPRing node west port and choose **Set West Protection Operation**. (To move a graphic icon, click it, then press **Ctrl** while you drag and drop it to a new location.)

Note For two-fiber MS-SPRings, the squares on the node icons represent the MS-SPRing working and protect channels. You can right-click either channel.

b. In the Set West Protection Operation dialog box, choose **FORCE RING** from the drop-down list.

c. Click **OK**.

d. Click **Yes** in the two Confirm MS-SPRing Operation dialog boxes that appear.

On the network view graphic, an F appears on the MS-SPRing channel where you invoked the Force Ring switch. The MS-SPRing span lines turn purple where the switch was invoked, and all span lines between other MS-SPRing nodes turn green.

Step 5 Verify the conditions:

a. Click the **Conditions** tab.

b. Click **Retrieve**.

c. Verify that the following conditions are reported on the node where you invoked the Force Ring switch on the west port:

- FORCE-REQ-RING—A Force Switch Request On Ring condition is reported against the span's working slot on the west side of the node.
- RING-SW-EAST—A Ring Switch Active on the east side condition is reported against the working span on the east side of the node.

Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

d. Verify that the following conditions are reported on the node that is connected to the West line of the node where you performed the switch:

- FE-FRCDWKSWPR-RING—A Far-End Working Facility Forced to Switch to Protection condition is reported against the working span on the east side of the node.
- RING-SW-WEST—A Ring Switch Active on the west side condition is reported against the working span on the west side of the node.

Step 6 (Optional) If you remapped the K3 byte to run an ONS 15600 SDH MS-SPRing through third-party equipment, check the following condition. Verify a FULLPASSTHR-BI condition reported on other nodes that are not connected to the west side of the node where you invoked the Force Ring switch.

Step 7 Verify the MS-SPRing line status on each node:

a. From the View menu, choose **Go to Node View**.

b. Click the **Maintenance > MS-SPRing** tabs.

c. Verify the following:

- The line states are shown as Stby/Stby on the west side of the node and Act/Act on the east side of the node where you invoked the Force Ring switch.
- The line states are shown as Stby/Stby on the east side of the node and Act/Act on the west side of the node that is connected to the west line of the node where you invoked the Force Ring switch.
- The line states are shown as Act/Act on both the east and west sides of the remaining nodes in the ring.

Step 8 From the View menu, choose **Go to Network View**.

Step 9 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 for instructions.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for procedures.

Step 10 Display the MS-SPRing window where you invoked the Force Ring switch (the window might be hidden by the CTC window).

Step 11 Clear the switch on the west port:

a. Right-click the west port of the MS-SPRing node where you invoked the Force Ring switch and choose **Set West Protection Operation**.

b. In the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down list.

c. Click **OK**.

d. Click **Yes** in the Confirm MS-SPRing Operation dialog box.

On the network view graphic, the Force Ring switch is removed, the F indicating the switch is removed, and the span lines between MS-SPRing nodes will be purple and green. The span lines might take a few moments to change color.

Step 12 In network view, click the **Conditions** tab. Verify that all conditions raised in this procedure are cleared from the network. If unexplained conditions appear, resolve them before continuing.

Step 13 Verify the MS-SPRing line status on each node:

a. From the View menu, choose **Go to Node View**.

a. Click the **Maintenance > MS-SPRing** tabs.

b. Verify that the line states are shown as Act/Stby on both the east and west sides of each node in the ring.

Step 14 Initiate a Force Ring switch on the east port:

a. Right-click the east port of MS-SPRing node and choose **Set East Protection Operation**.

b. In the Set East Protection Operation dialog box, choose **FORCE RING** from the drop-down list.

c. Click **OK**.

d. Click **Yes** in the two Confirm MS-SPRing Operation dialog boxes that appear.

On the network view graphic, an F appears on the working MS-SPRing channel where you invoked the Force Ring switch. The MS-SPRing span lines are purple where the Force Ring switch was invoked, and all span lines between other MS-SPRing nodes are green. The span lines might take a few moments to change color.

Step 15 Verify the conditions:

a. Click the **Conditions** tab.

b. Click **Retrieve**.

c. Verify that the following conditions are reported on the node where you invoked the Force Ring switch on the east port:

- FORCE-REQ-RING—A Force Switch Request On Ring condition is reported against the span's working slot on the east side of the node.
- RING-SW-WEST—A Ring Switch Active on the west side condition is reported against the working span on the east side of the node.

Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

d. Verify that the following conditions are reported on the node that is connected to the East line of the node where you performed the switch:

- FE-FRCDWKSWPR-RING—A Far-End Working Facility Forced to Switch to Protection condition is reported against the working span on the west side of the node.

- RING-SW-EAST—A Ring Switch Active on the east side condition is reported against the working span on the west side of the node.

Step 16 (Optional) If you remapped the K3 byte to run an ONS 15600 SDH MS-SPRing through third-party equipment, verify a FULLPASSTHR-BI condition reported on other nodes that are not connected to the west side of the node where you invoked the Force Ring switch.

Step 17 Verify the MS-SPRing line status on each node:

a. From the View menu, choose **Go to Node View**.

b. Click the **Maintenance > MS-SPRing** tabs. Verify the following:

- The line states are shown as Stby/Stby on the east side of the node and Act/Act on the west side of the node where you invoked the Force Ring switch.
- The line states are shown as Stby/Stby on the west side of the node and Act/Act on the east side of the node that is connected to the east line of the node where you invoked the Force Ring switch.
- The line states are shown as Act/Act on both east and west sides of the remaining nodes in the ring.

Step 18 From the View menu, choose **Go To Network View**.

Step 19 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-F288 Disable Alarm Filtering" task on page 17-80 for instructions.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for procedures.

Step 20 Display the MS-SPRing window where you invoked the Force Ring switch (the window might be hidden by the CTC window).

Step 21 Clear the switch on the east port:

a. Right-click the east port of the MS-SPRing node where you invoked the Force Ring switch and choose **Set East Protection Operation**.

b. In the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down list.

c. Click **OK**.

d. Click **Yes** in the Confirm MS-SPRing Operation dialog box.

On the network view graphic, the Force Ring switch is removed, the F indicating the switch is removed, and the span lines between MS-SPRing nodes will be purple and green. The span lines might take a few moments to change color.

Step 22 From network view, click the **Conditions** tab. Verify that all conditions raised in this procedure are cleared from the network. If unexplained conditions appear, resolve them before continuing.

Step 23 Verify the MS-SPRing line status on each node:

a. From the View menu, choose **Go to Node View**.

b. Click the **Maintenance > MS-SPRing** tabs.

c. Verify that the line states are shown as Act/Stby on both the east and west sides of each node in the ring.

Step 24 From the File menu, choose **Close** to close the MS-SPRing window.

Step 25 Return to your originating procedure (NTP).

DLP-F343 Provision an STM-N Circuit Route

Purpose	This task provisions the circuit route for manually routed STM-N circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 The Circuit Creation Wizard must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the Circuit Creation wizard in the Route Review/Edit area, click the source node icon if it is not already selected.

Step 2 Starting with a span on the source node, click the arrow of the span you want the circuit to travel. To reverse the direction of the arrow, click the arrow twice.

The arrow turns white. In the Selected Span area, the From and To fields provide span information. The source VC appears.

Step 3 If you want to change the source VC, adjust the Source VC field; otherwise, continue with Step 4.

Step 4 Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

Step 5 Repeat Steps 2 through 4 until the circuit is provisioned from the source to the destination node through all intermediary nodes. If Fully Protected Path is checked in the Circuit Routing Preferences area, you must:

- Add two spans for all SNCP or unprotected portions of the circuit route from the source to the destination.
- Add one span for all MS-SPRing or 1+1 portions of route from the source to the destination.
- Add primary spans for MS-SPRing-DRI from the source to the destination through the primary nodes, and then add spans through the secondary nodes as an alternative route. The circuit map shows all span types: unprotected, MS-SPRing, and PCA. PCA spans can only be chosen as part of the secondary path.

Step 6 Return to your originating procedure (NTP).

DLP-F344 Initiate an MS-SPRing Manual Ring Switch

Purpose	This task performs an MS-SPRing Manual ring switch. A Manual ring switch will switch traffic off a span if there is no higher priority switch (Force or lock out) and no signal degrade (SD) or signal failure (SF) conditions.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed

Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Traffic is not protected during a manual ring protection switch.

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Provisioning > MS-SPRing** tabs.

Step 3 Choose the MS-SPRing and click **Edit**.

Tip To move an icon to a new location, for example, to see MS-SPRing channel (port) information more clearly, click an icon, and drag and drop it in a new location.

Step 4 Right-click any MS-SPRing node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).

Note The squares on the node icons represent the MS-SPRing working and protect channels. You can right-click either channel. For four-fiber MS-SPRings, the squares represent ports. Right-click either working port.

Step 5 In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **MANUAL RING** from the drop-down list. Click **OK**.

Step 6 Click **Yes** in the two Confirm MS-SPRing Operation dialog boxes.

Step 7 Verify that the channel (port) displays the letter "M" for Manual ring. Also verify that the span lines between the nodes where the Manual switch was invoked turn purple, and that the span lines between all other nodes turn green on the network view map. This confirms the Manual switch.

Step 8 From the File menu, choose **Close**.

Step 9 Return to your originating procedure (NTP).

DLP-F345 Clear an MS-SPRing Manual Ring Switch

Purpose	This task clears a manual ring switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Provisioning > MS-SPRing** tabs.

Step 3 Choose the MS-SPRing and click **Edit**.

Tip To move an icon to a new location, for example, to see MS-SPRing channel (port) information more clearly, click an icon on the Edit MS-SPRing network graphic and while pressing **Ctrl**, drag the icon to a new location.

Step 4 Right-click the MS-SPRing node channel (port) where the manual ring switch was applied and choose **Set West Protection Operation** or **Set East Protection Operation**, as applicable.

Step 5 In the dialog box, choose **CLEAR** from the drop-down list. Click **OK**.

Step 6 Click **Yes** in the Confirm MS-SPRing Operation dialog box. The letter "M" is removed from the channel (port) and the span turns green on the network view map.

Step 7 From the File menu, choose **Close**.

Step 8 Return to your originating procedure (NTP).

DLP-F346 Create an MS-SPRing on a Single Node

Purpose	This task creates an MS-SPRing on a single node. Use this task to add a node to an existing MS-SPRing or to delete and then recreate an MS-SPRing temporarily on one node.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > MS-SPRing** tabs.

Step 2 In the Suggestion dialog box, click **OK**.

Step 3 In the Create MS-SPRing dialog box, enter the MS-SPRing information:

- Ring Type—Enter the ring type (2 Fiber) of the MS-SPRing.
- Ring Name—Enter the MS-SPRing name. If the node is being added to an MS-SPRing, use the MS-SPRing ring name.
- Node ID—Enter the node ID. If the node is being added to an MS-SPRing, use an ID that is not used by other MS-SPRing nodes in that ring.
- Ring Reversion—Enter the ring reversion time of the existing MS-SPRing.
- West Line—Enter the slot on the node that will connect to the existing MS-SPRing through the node's west line (port).
- East Line—Enter the slot on the node that will connect to the existing MS-SPRing through the node's east line (port).

Step 4 Click **OK**.

Note The MS-SPRing is incomplete and alarms are present until the node is connected to other MS-SPRing nodes.

Step 5 Return to your originating procedure (NTP).

DLP-F347 Initiate an MS-SPRing Force Ring Switch

Purpose	Use this task to perform an MS-SPRing Force switch on an MS-SPRing port. A Force ring switch will switch traffic off a span if there is no signal degrade (SD), signal failure (SF), or lockout switch present on the span.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution The Force Switch Away command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution Traffic is not protected during a Force protection switch.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > MS-SPRing** tabs. Select the MS-SPRing.

Step 3 Click **Edit**.

Step 4 To apply a Force switch to the west line:

a. Right-click the west MS-SPRing port where you want to switch the MS-SPRing traffic and choose **Set West Protection Operation**.

Note If node icons overlap, drag and drop the icons to a new location. You can also return to network view and change the positions of the network node icons, because MS-SPRing node icons are based on the network view node icon positions.

Note For two-fiber MS-SPRings, the squares on the node icons represent the MS-SPRing working and protect channels. You can right-click either channel.

b. In the Set West Protection Operation dialog box, choose **FORCE RING** from the drop-down list. Click **OK**.

c. Click **Yes** in the two Confirm MS-SPRing Operation dialog boxes that appear.

On the network graphic, an F appears on the working MS-SPRing channel where you invoked the protection switch. The span lines change color to reflect the forced traffic. Green span lines indicate the new MS-SPRing path, and the lines between the protection switch are purple.

Performing a Force switch generates several conditions including FORCED-REQ-RING and WKSWPR.

Step 5 To apply a Force switch to the east line:

a. Right-click the east MS-SPRing port and choose **Set East Protection Operation**.

Note If node icons overlap, drag and drop the icons to a new location or return to network view and change the positions of the network node icons. MS-SPRing node icons are based on the network view node icon positions.

Note For two-fiber MS-SPRings, the squares on the node icons represent the MS-SPRing working and protect channels. You can right-click either channel.

b. In the Set East Protection Operation dialog box, choose **FORCE RING** from the drop-down list. Click **OK**.

c. Click **Yes** in the two Confirm MS-SPRing Operation dialog boxes that appear.

On the network graphic, an F appears on the working MS-SPRing channel where you invoked the protection switch. The span lines change color to reflect the forced traffic. Green span lines indicate the new MS-SPRing path, and the lines between the protection switch are purple.

Performing a Force switch generates several conditions including FORCED-REQ-RING and WKSWPR.

Step 6 From the File menu, choose **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-F348 View Circuit Information

Purpose	This task enables you to view information about circuits, such as name, type, size, and direction.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate CTC view:

- To view circuits for an entire network, from the View menu, choose **Go To Network View**.
- To view circuits that originate, terminate, or pass through a specific node, from the View menu, choose **Go To Other Node**, then choose the node you want to search and click **OK**.
- To view circuits that originate, terminate, or pass through a specific card, in node view, double-click the card containing the circuits you want to view.

Note In node or card view, you can change the scope of the circuits that are displayed by choosing Card (in card view), Node, or Network from the Scope drop-down list in the bottom right corner of the Circuits window.

Step 2 Click the **Circuits** tab. The Circuits tab has the following information:

- Name—Name of the circuit. The circuit name can be manually assigned or automatically generated.
- Type—For the ONS 15600 SDH, the circuit type is STS (STS circuit).
- Size—VT circuit size is 1.5. STS circuit sizes can be 1, 3c, 6c, 9c, 12c, 24c, 48c, or 192c.
- OCHNC Wlen—(ONS 15454 dense wavelength division multiplexing [DWDM] only) For OCHNCs, the wavelength provisioned for the optical channel network connection. Refer to the *Cisco ONS 15454 DWDM Procedure Guide*.
- Direction—The circuit direction, either two-way or one-way.
- OCHNC Dir—(ONS 15454 DWDM only) For OCHNCs, the direction of the optical channel network connection, either East to West or West to East. Refer to the *Cisco ONS 15454 DWDM Procedure Guide*.
- Protection—The protection type; see Table 18-2.

Table 18-2 Circuit Protection Types

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

- Status—The circuit status. Table 18-3 lists the circuit statuses that can appear.

Table 18-3 ONS 15600 SDH Circuit Status

Status	Definition/Activity
CREATING	CTC is creating a circuit.
DISCOVERED	CTC created a circuit. All components are in place and a complete path exists from circuit source to destination.
DELETING	CTC is deleting a circuit.
PARTIAL	A CTC-created circuit is missing a connection or circuit span (network link), a complete path from source to destination(s) does not exist, or a MAC address change occurred on one of the circuit nodes and the circuit is in need of repair (in the ONS 15454, the MAC address resides on the alarm interface panel (AIP); in the ONS 15600 SDH, the MAC address resides on the backplane EEPROM). 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 destination(s) exists.
PARTIAL_TL1	A TL1-created circuit or a TL1-like, CTC-created circuit is missing a cross-connect or circuit span (network link), and a complete path from source to destination(s) does not exist.
CONVERSION_PENDING	An existing circuit in a topology upgrade is set to this status. The circuit returns to the DISCOVERED status when the topology upgrade is complete. For more information about topology upgrades, refer to the *Cisco ONS 15600 SDH Reference Manual*.

Table 18-3 ONS 15600 SDH Circuit Status (continued)

Status	Definition/Activity
PENDING_MERGE	Any new circuits created to represent an alternate path in a topology upgrade are set to this status to indicate that it is a temporary circuit. These circuits can be deleted if a topology upgrade fails. For more information about topology upgrades, refer to the *Cisco ONS 15600 SDH Reference Manual*.
DROP_PENDING	A circuit is set to this status when a new circuit drop is being added.

- Source—The circuit source in the format: *node/slot/port/STS*. If an ASAP PPM port is the circuit source, the port format is *PIM-PPM-port*, where PIM and PPM values are 1 through 4 (for example, p1-1-1). PPMs have only one port.
- Destination—The circuit destination in the format: *node/slot/port/STS*. If an ASAP PPM port is the circuit destination, the port format is *PIM-PPM-port*, where PIM and PPM values are 1 through 4 (for example, p1-1-1). PPMs have only one port.
- # of VLANS—(Future use) The number of VLANs used by an Ethernet circuit.
- # of Spans—The number of internode links that constitute the circuit. Right-clicking the column shows a shortcut menu from which you can choose Span Details to show or hide circuit span detail.
- State—The circuit service state, which is an aggregate of its cross-connects. The service states are Unlocked, Locked, or Locked-partial. For more information about circuit service states, refer to the “Administrative and Service States” appendix of the *Cisco ONS 15600 SDH Reference Manual*.
  - Unlocked—All cross-connects are in service and operational.
  - Locked—All cross-connects are Locked-enabled,maintenance or Locked-enabled,disabled.
  - Locked-partial—At least one cross-connect is Unlocked-enabled and others are in the Locked-enabled,maintenance and/or Locked-enabled,disabled service states.

Step 3 Return to your originating procedure (NTP).

DLP-F349 Install Fiber-Optic Cables for MS-SPRing Configurations

Purpose	This task installs the fiber-optics to the east and west MS-SPRing ports at each node. See Chapter 5, “Turn Up a Network” to provision and test MS-SPRing configurations.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-F119 Install the STM-N Cards, page 2-4 NTP-F231 Clean Fiber Connectors and Adapters, page 14-16
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution Do not provision the MS-SPRing east and west ports on the same STM-N card.

Note To avoid error, connect fiber-optic cable so that the farthest slot to the right represents the east port, and the farthest slot to the left represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.

Note See Table 16-1 on page 16-19 and Table 16-2 on page 16-19 for OGI connector pinouts of STM-N cards.

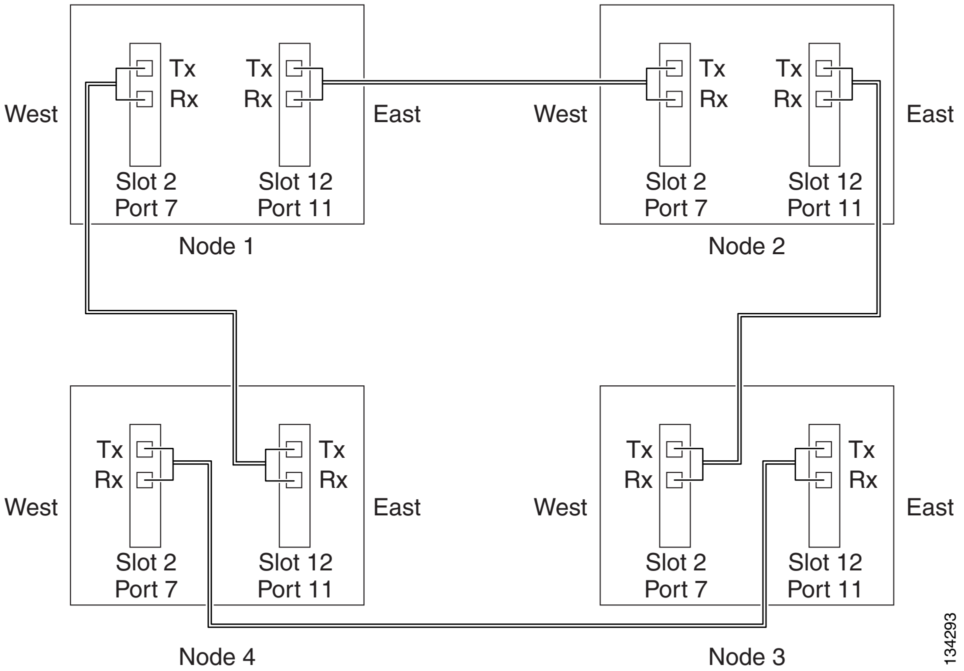
Step 1 Plan your fiber connections. Use the same plan for all MS-SPRing nodes. MS-SPRing configuration is achieved by correctly cabling the transmit and receive fibers of each node to the others.

Step 2 Plug the fiber into the Tx connector of an STM-N port at one node and plug the other end into the Rx connector of an STM-N port at the adjacent node. The card displays an SF LED if the transmit and receive fibers are mismatched.

Step 3 Repeat Step 2 until you have configured the ring.

Figure 18-11 shows fiber connections for a two-fiber MS-SPRing with trunk ports in Slot 2, Port 7 (west) and Slot 12, Port 11 (east).

Figure 18-11 Connecting Fiber to a Four-Node, Two-Fiber MS-SPRing



Note To provision an MS-SPRing, see Chapter 5, "Turn Up a Network"

Step 4 Return to your originating procedure (NTP).

DLP-F350 Delete an MS-SPRing from a Single Node

Purpose	This task deletes an MS-SPRing from a node after you remove the node from the MS-SPRing.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, display the node that was removed from the MS-SPRing:

- If the node that was removed is connected to the same LAN as your computer, from the File menu, choose **Add Node**, then enter the node name or IP address.
- If the node that was removed is not connected to the same LAN as your computer, you must connect to the node using a direct connection. See Chapter 3, "Connect the PC and Log into the GUI" for procedures.

Step 2 Click the **Provisioning > MS-SPRing** tabs.

Step 3 Highlight the ring and click **Delete**.

Step 4 In the Suggestion dialog box, click **OK**.

Step 5 In the confirmation message, confirm that this is the ring you want to delete. If so, click **Yes**.

Step 6 Return to your originating procedure (NTP).

DLP-F351 Roll the Source or Destination of One Optical Circuit

Purpose	This task reroutes traffic from one source or destination to another on the same circuit, thus changing the original source or destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Circuits** tab.

Step 3 Click the circuit that you want to roll. The circuit must have a DISCOVERED status for you to start a roll.

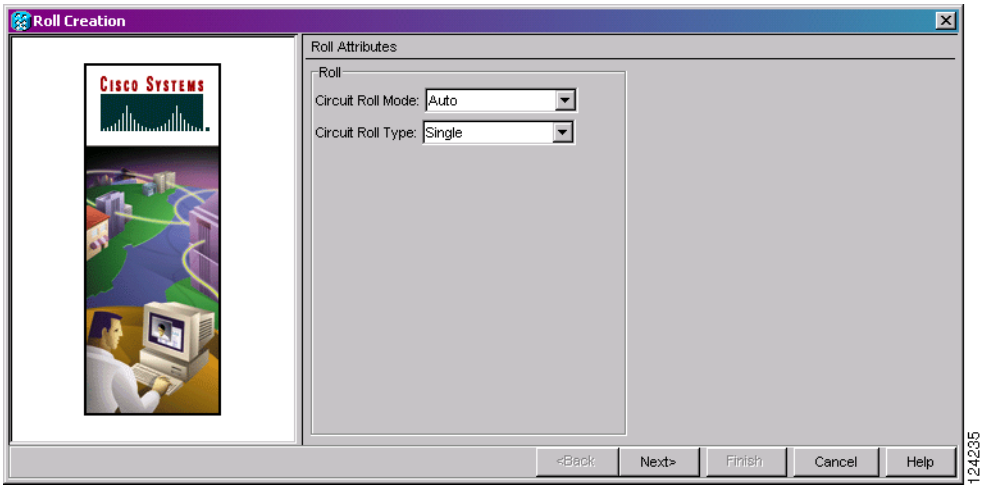
Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

Step 5 In the Roll Attributes area, complete the following (Figure 18-12):

a. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll (required for a 1-way source roll) or **Manual** to create a manual roll (required for a 1-way destination roll).

b. From the Circuit Roll Type drop-down list, choose **Single** to indicate that you want to roll one cross-connect on the chosen circuit.

Figure 18-12 Selecting Single Roll Attributes



Circuit Roll Mode: Auto

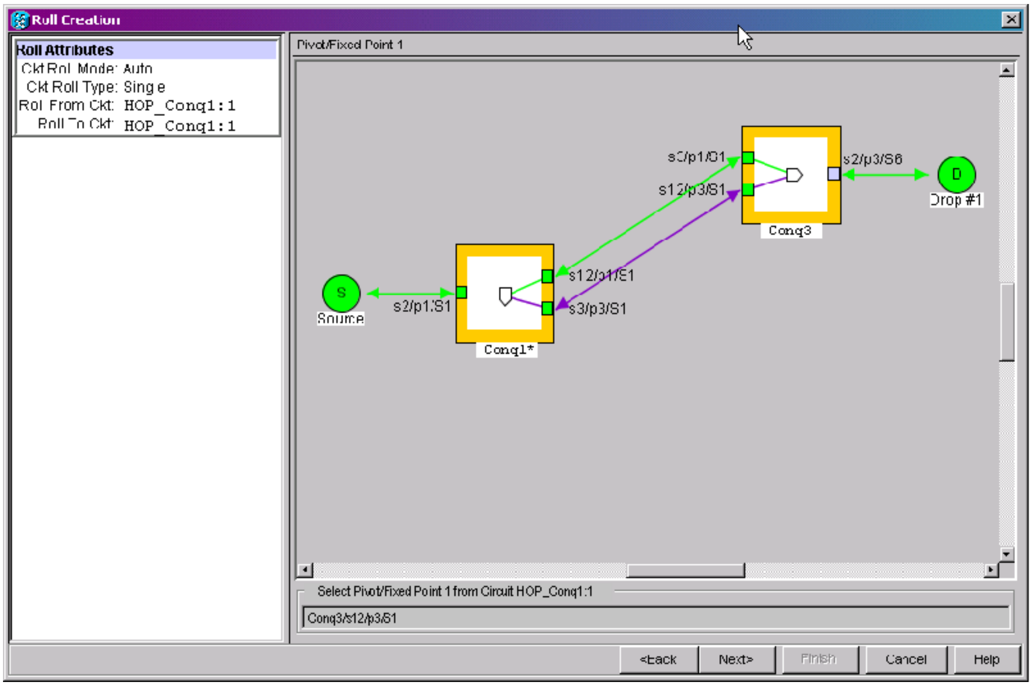
Circuit Roll Type: Single

Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square in the graphic image that represents the facility that you want to keep (Figure 18-13).

This facility is the fixed location in the cross-connect involved in the roll process. The identifier appears in the text box below the graphic image. The facility that is not selected is the Roll From path. The Roll From path is deleted after the roll is completed.

Figure 18-13 Selecting a Path



Roll Creation

Roll Attributes
Ckt Roll Mode: Auto
Ckt Roll Type: Single
Roll From Ckt: HOP_Conq1:1
Roll To Ckt: HOP_Conq1:1

Pivot/Fixed Point 1

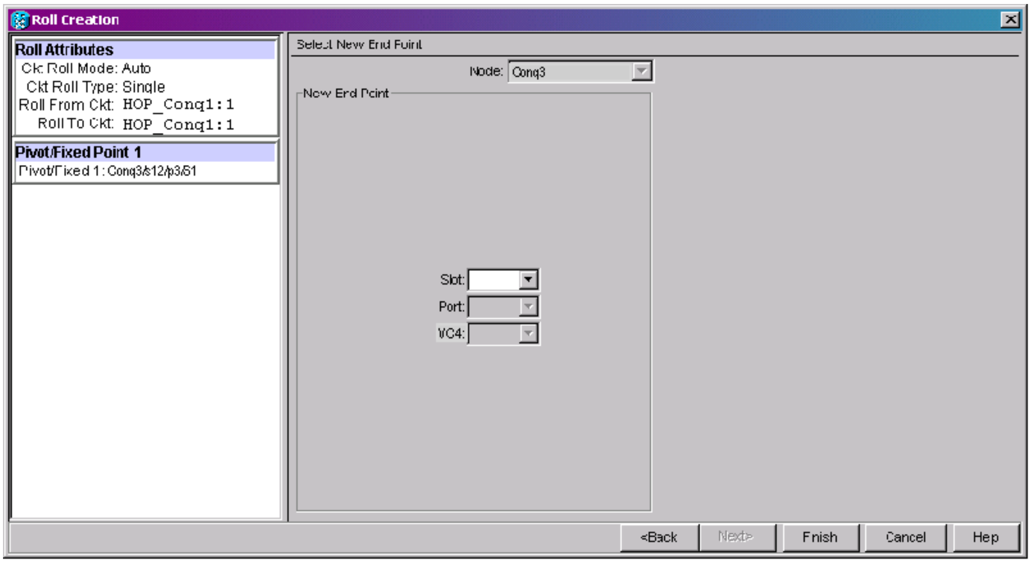
Select Pivot/Fixed Point 1 from Circuit HOP_Conq1:1

Conq3/s12/p3/S1

Step 8 Click **Next**.

Step 9 In the Select New End Point area, choose the **Slot**, **Port**, and **VC3 or VC4** from the drop-down lists to select the Roll To facility (Figure 18-14).

Figure 18-14 Selecting a New Endpoint



Roll Creation

Roll Attributes
Ckt Roll Mode: Auto
Ckt Roll Type: Single
Roll From Ckt: HOP_Conq1:1
Roll To Ckt: HOP_Conq1:1

Pivot/Fixed Point 1
Pivot/Fixed 1: Conq3/s12/p3/S1

Select New End Point

Node: Conq3

New End Point

Slot:
Port:
VC4:

Step 10 Click **Finish**. On the Circuits tab, the circuit status for the Roll From port changes from DISCOVERED to ROLL_PENDING.

Step 11 Click the **Rolls** tab (Figure 18-15). For the pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with Step 12.

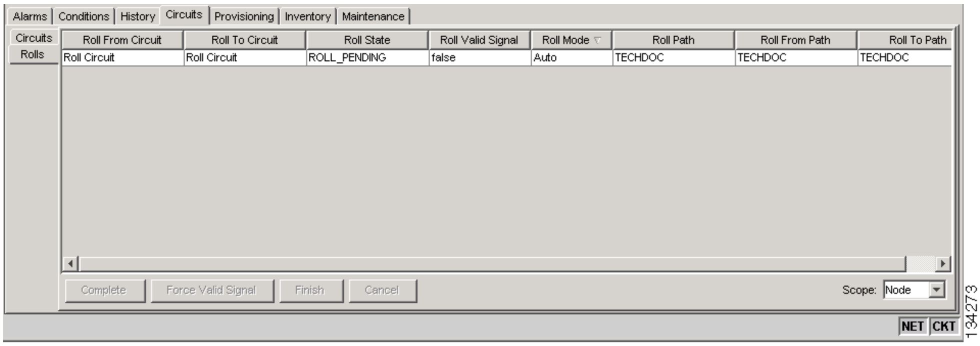
- If the Roll Valid Signal status is true, a valid signal was found on the new port.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If the signal is not found, refer to the “General Troubleshooting” chapter in the *Cisco ONS 15600 SDH Troubleshooting Guide*. To cancel the roll, see the “DLP-F357 Cancel a Roll” task on page 18-70.
- The roll is a one-way destination roll and the Roll Valid Signal is false. It is not possible to get a Roll Valid Signal status of true for a one-way destination roll.

Note You cannot cancel an automatic roll after a valid signal is found.

- You can force a signal onto the Roll To circuit by using the Force Valid Signal button. If you choose Force Valid Signal, traffic on the circuit that is involved in the roll might drop depending on conditions at the other end of the circuit when the roll is completed. You must force a signal if the circuits do not have a signal or have a bad signal and you want to complete the roll.

Note For a one-way destination roll in manual mode, you do not need to force the valid signal.

Figure 18-15 Viewing the Rolls Tab



Roll From Circuit	Roll To Circuit	Roll State	Roll Valid Signal	Roll Mode	Roll Path	Roll From Path	Roll To Path
Roll Circuit	Roll Circuit	ROLL_PENDING	false	Auto	TECHDOC	TECHDOC	TECHDOC

Scope: Node

Step 12 If you selected Manual in Step 5, click the rolled facility on the Rolls tab and then click **Complete**. If you selected Auto, continue with Step 13.

Step 13 For both Manual and Auto rolls, click **Finish** to complete the circuit roll process. The roll clears from the Rolls tab and the rolled circuit now appears on the Circuits tab in the DISCOVERED status.

Step 14 Return to your originating procedure (NTP).

DLP-F352 Roll One Cross-Connect from an Optical Circuit to a Second Optical Circuit

Purpose	This task reroutes a cross-connect on one circuit onto another circuit resulting in a new destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 "DLP-F253 Provision RS-DCC Terminations" task on page 17-46 for the ports involved in the roll
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Circuits** tab.

Step 3 Press **Ctrl** and click the two circuits that you want to use in the roll process.

The circuits must have a DISCOVERED status; in addition, they must be the same size and direction for you to start a roll. The planned Roll To circuit must not carry traffic.The Roll To facility should be DCC connected to the source node of the Roll To circuit.

Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

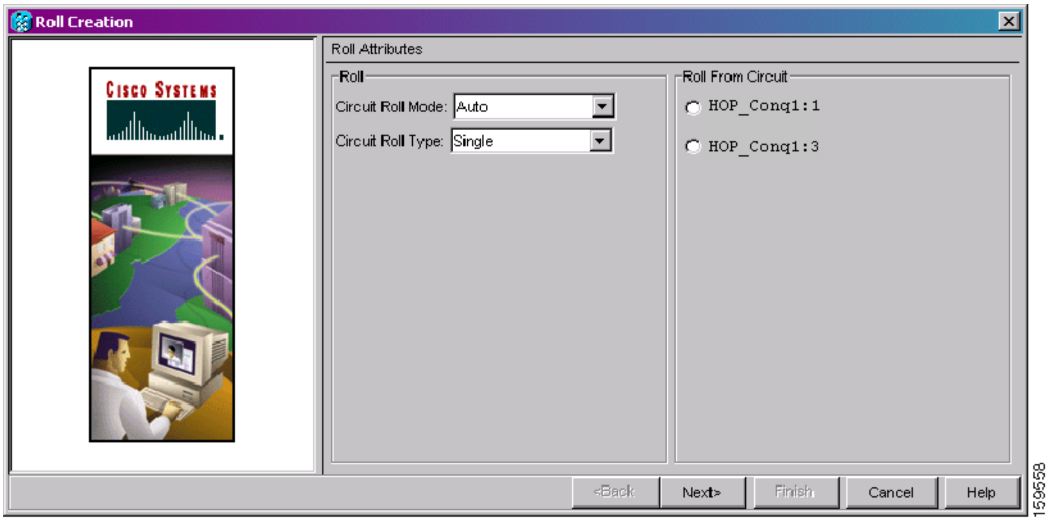
Step 5 In the Roll Attributes area, complete the following (Figure 18-16):

a. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll (required for a 1-way source roll) or **Manual** to create a manual roll (required for 1-way destination roll).

b. From the Circuit Roll Type drop-down list, choose **Single** to indicate that you want to roll a single connection from the Roll From circuit to the Roll To circuit.

c. In the Roll From Circuit area, click the circuit that contains the Roll From connection.

Figure 18-16 Selecting Roll Attributes for a Single Roll onto a Second Circuit



Roll Creation

Roll Attributes

Roll

Circuit Roll Mode: Auto

Circuit Roll Type: Single

Roll From Circuit

○ HOP_Conq1:1

○ HOP_Conq1:3

Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square representing the facility that you want to keep (Figure 18-13 on page 18-58).

This facility is the fixed location in the cross-connect involved in the roll process. The identifier appears in the text box below the graphic image. The facility that is not selected is the Roll From path. The Roll From path is deleted after the roll is completed.

Step 8 Click **Next**.

Step 9 In the Select New End Point area, choose the **Slot**, **Port**, and **VC3 or VC4** from the drop-down lists to identify the Roll To facility on the connection being rolled.

Step 10 Click **Finish**.

The statuses of the Roll From and Roll To circuits change from DISCOVERED to ROLL_PENDING in the Circuits tab.

Step 11 Click the **Rolls** tab. For the pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with Step 12.

- If the Roll Valid Signal status is true, a valid signal was found on the new port.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If the signal is not found, refer to the "General Troubleshooting" chapter in the *Cisco ONS 15600 SDH Troubleshooting Guide*. To cancel the roll, see the "DLP-F357 Cancel a Roll" task on page 18-70.
- The roll is a one-way destination roll and the Roll Valid Signal is false. It is not possible to get a "true" Roll Valid Signal status for a one-way destination roll.

Note You cannot cancel an automatic roll after a valid signal is found.

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

Step 12 If you selected Manual in Step 5, click the roll on the Rolls tab and click **Complete** to route the traffic to the new port. If you selected Auto, continue with Step 13.

Step 13 For both manual and automatic rolls, click **Finish** to complete the circuit roll process.

The roll is cleared from the Rolls tab and the new rolled circuit on Circuits tab returns to the DISCOVERED status.

Step 14 Return to your originating procedure (NTP).

DLP-F353 Roll Two Cross-Connects on One Optical Circuit Using Automatic Routing

Purpose	This task reroutes the network path while maintaining the same source and destination. This task allows CTC to automatically select a Roll To path.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This task optionally uses automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see Appendix C, “Network Element Defaults,” in the *Cisco ONS 15600 SDH Reference Manual.*

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Circuits tab**.

Step 3 Click the circuit that has the connections that you want to roll. The circuit must have a DISCOVERED status for you to start a roll.

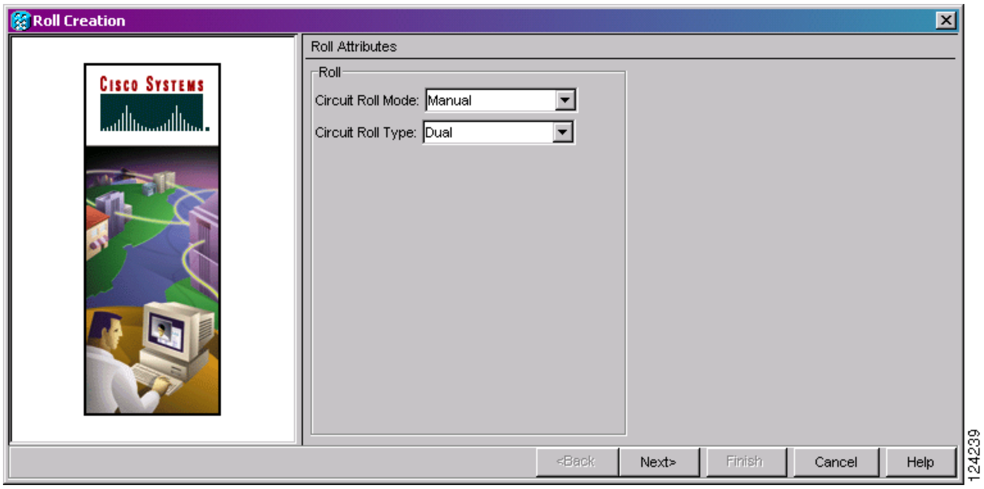
Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

Step 5 In the Roll Attributes area, complete the following (Figure 18-17):

a. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll or **Manual** to create a manual roll.

b. From the Circuit Type drop-down list, choose **Dual** to indicate that you want to roll two connections on the chosen circuit.

Figure 18-17 Selecting Dual Roll Attributes



Circuit Roll Mode: Manual

Circuit Roll Type: Dual

Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square representing the fixed path of the first connection to be rolled (Figure 18-13 on page 18-58).

This path is a fixed point in the cross connection involved in the roll process. The path identifier appears in the text box below the graphic image. The path that is not selected contains the Roll From path. The Roll From path is deleted after the roll is completed.

Step 8 Click **Next**.

Step 9 Complete one of the following:

- If multiple Roll From paths exist, the Select Roll From dialog box appears. Select the path from which you want to roll traffic and click **OK**.
- If multiple Roll From paths do not exist, continue with Step 10. The circuit status for the Roll To path changes states from DISCOVERED to ROLL_PENDING.

Step 10 In the Pivot/Fixed Point 2 window, click the square that represents the fixed path of the second connection to be rolled.

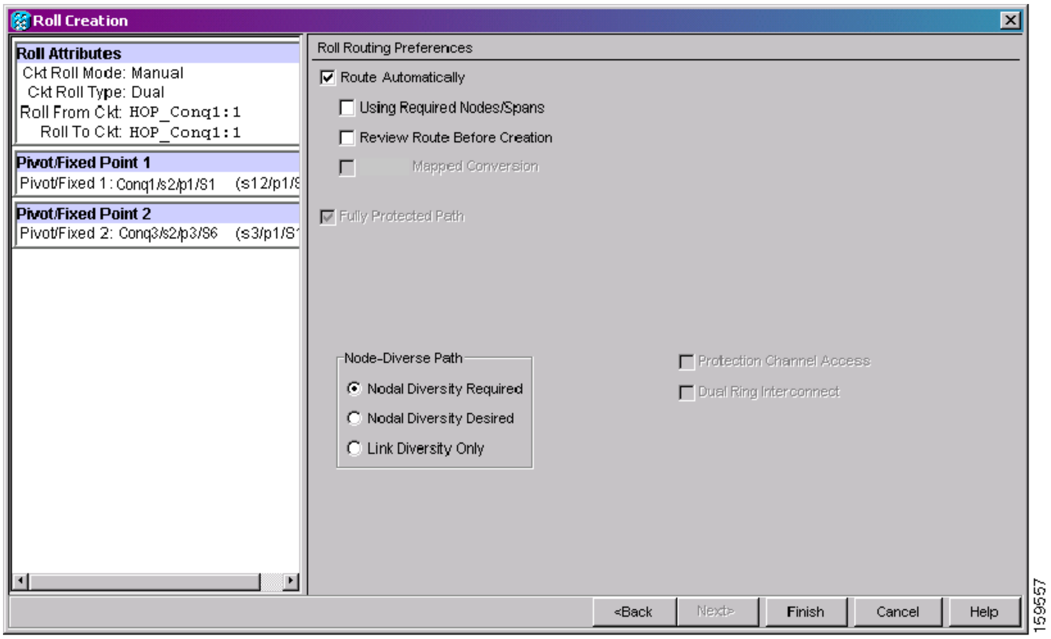
The path that is not selected is the Roll From path. The Roll From path is deleted after the roll is completed. The path identifier appears in the text box below the graphic image.

Step 11 Click **Next**.

Step 12 In the Circuit Routing Preferences area, check **Route Automatically** to allow CTC to find the route (Figure 18-18). If you check Route Automatically, the following options are available:

- Using Required Nodes/Spans—If checked, you can specify nodes and spans to include or exclude in the CTC-generated circuit route in Step 15.
- Review Route Before Creation—If checked, you can review and edit the circuit route before the circuit is created.

Figure 18-18 Setting Roll Routing Preferences



Roll Creation

Roll Attributes
Ckt Roll Mode: Manual
Ckt Roll Type: Dual
Roll From Ckt: HOP_Conq1:1
Roll To Ckt: HOP_Conq1:1

Pivot/Fixed Point 1
Pivot/Fixed 1: Conq1/s2/p1/S1 (s12/p1/S

Pivot/Fixed Point 2
Pivot/Fixed 2: Conq3/s2/p3/S6 (s3/p1/S

Roll Routing Preferences

☑ Route Automatically
□ Using Required Nodes/Spans
□ Review Route Before Creation
□ Mapped Conversion
☑ Fully Protected Path

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

□ Protection Channel Access
□ Dual Ring Interconnect

Step 13 To route the circuit over a protected path, check **Fully Protected Path**. (If you do not want to route the circuit on a protected path, continue with Step 14.) CTC creates a primary and alternate circuit route (virtual SNCP) based on the following nodal diversity options. Select one of the following choices and follow subsequent window prompts to complete the routing:

- **Nodal Diversity Required**—Ensures that the primary and alternate paths within path-protected mesh network (PPMN) portions of the complete circuit path are nodally diverse.
- **Nodal Diversity Desired**—Specifies that node diversity should be attempted, but if node diversity is not possible, CTC creates link diverse paths for the PPMN portion of the complete circuit path.
- **Link Diversity Only**—Specifies that only link-diverse primary and alternate paths for PPMN portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you checked Route Automatically in Step 12:

- If you checked Using Required Nodes/Spans, continue with Step 15.
- If you checked only Review Route Before Creation, continue with Step 16.
- If you did not check Using Required Nodes/Spans or Review Route Before Creation, continue with Step 17.

Step 15 If you checked Using Required Nodes/Spans in Step 12:

a. In the Roll Route Constraints area, click a node or span on the circuit map.

b. Click **Include** to include the node or span in the circuit. Click **Exclude** to exclude the node/span from the circuit. The order in which you select included nodes and spans sets the circuit sequence. Click spans twice to change the circuit direction.

c. Repeat Step b for each node or span you wish to include or exclude.

d. Review the circuit route. To change the circuit routing order, select a node in the Required Nodes/Lines or Excluded Nodes Links lists, then click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 16 If you checked Review Route Before Creation in Step 12:

a. In the Roll Route Review and Edit area, review the circuit route. To add or delete a circuit span, select a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

b. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information.

Step 17 Click **Finish**.

In the Circuits tab, verify that a new circuit appears. This circuit is the Roll To circuit. It is designated with the Roll From circuit name appended with ROLL**.

Step 18 Click the **Rolls** tab. Two new rolls now appear. For each pending roll, view the Roll Valid Signal status. When one of the following requirements is met, continue with Step 19.

- If the Roll Valid Signal status is true, a valid signal was found on the new port.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If a valid signal is not found, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*. To cancel the roll, see the "DLP-F357 Cancel a Roll" task on page 18-70.
- The roll is a one-way destination roll and the Roll Valid signal status is false. It is not possible to get a Roll Valid Signal status of true for a one-way destination roll.

Note If you have completed a roll, you cannot cancel the sibling roll. You must cancel the two rolls together.

Note You cannot cancel an automatic roll after a valid signal is found.

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

Step 19 If you selected Manual in Step 5, click both rolls on the Rolls tab and click **Complete** to route the traffic to the new port. If you selected Auto, continue with Step 20.

Note You cannot complete a roll if you cancelled the sibling roll. You must complete the two rolls together.

Step 20 For both manual and automatic rolls, click **Finish** to complete circuit roll process.

Step 21 Return to your originating procedure (NTP).

DLP-F354 Roll Two Cross-Connects on One Optical Circuit Using Manual Routing

Purpose	This task reroutes a network path of an optical circuit using manual routing.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Circuits tab.**

Step 3 Click the circuit that you want to roll to a new path. The circuit must have a DISCOVERED status for you to start a roll.

Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

Step 5 In the Roll Attributes area, complete the following (Figure 18-17 on page 18-63):

- **a.** From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll or **Manual** to create a manual roll.
- **b.** From the Circuit Type drop-down list, choose **Dual** to indicate that you want to roll two connections on the chosen circuit.

Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square representing the fixed path of the first cross-connect to be rolled (Figure 18-13 on page 18-58).

This path is a fixed point in the cross-connect involved in the roll process. The path identifier appears in the text box below the graphic image. The path that is not selected contains the Roll From path. The Roll From path is deleted after the roll is completed.

Step 8 Click **Next**.

Step 9 Complete one of the following:

- If multiple Roll From paths exist, the Select Roll From dialog box appears. Select the path from which you want to roll traffic and click **OK**, then click **Next** (Figure 18-18 on page 18-64).
- If multiple Roll From paths do not exist, click **Next** and continue with Step 10. The circuit status for the Roll From path changes from DISCOVERED to ROLL_PENDING.

Step 10 In the Pivot/Fixed Point 2 window, click the square that represents the fixed path of the second connection to be rolled.

The path that is not selected is the Roll From path. The Roll From path is deleted after the roll is complete. The path identifier appears in the text box below the graphic image.

Step 11 Click **Next**.

Step 12 In the Circuit Routing Preferences area, uncheck **Route Automatically**.

Step 13 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 14.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.

Step 14 If you checked Fully Protected Path, choose one of the following:

- **Nodal Diversity Required**—Ensures that the primary and alternate paths within the SNCP portions of the complete circuit path are nodally diverse.
- **Nodal Diversity Desired**—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the SNCP portion of the complete circuit path.
- **Link Diversity Only**—Specifies that only fiber-diverse primary and alternate paths for SNCP portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 15 Click **Next**. Beneath Route Review and Edit, node icons appear for you to route the circuit manually.

The green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit.

Step 16 Complete the "DLP-F343 Provision an STM-N Circuit Route" task on page 18-47.

Step 17 Click **Finish**. In the Circuits tab, verify that a new circuit appears.

This circuit is the Roll To circuit. It is designated with the Roll From circuit name appended with ROLL**.

Step 18 Click the **Rolls** tab. Two new rolls now appear on the Rolls tab. For each pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with Step 19.

- If the Roll Valid Signal status is true, a valid signal was found on the new port.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If the signal is not found, refer to the "General Troubleshooting" chapter in the *Cisco ONS 15600 SDH Troubleshooting Guide*. To cancel the roll, see the "DLP-F357 Cancel a Roll" task on page 18-70.
- The roll is a one-way destination roll and the Roll Valid signal status is false. It is not possible to get a Roll Valid Signal status of true for a one-way destination roll.

Note You cannot cancel an automatic roll after a valid signal is found.

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

Step 19 If you selected Manual in Step 5, click each roll and click **Complete** to route the traffic to the new port. If you selected Auto, continue with Step 20.

Note You cannot complete a roll if you cancelled the sibling roll. You must complete the two rolls together.

Step 20 For both manual and automatic rolls, click **Finish** to complete the circuit roll process.

Step 21 Return to your originating procedure (NTP).

DLP-F355 Roll Two Cross-Connects from One Optical Circuit to a Second Optical Circuit

Purpose	This task reroutes a network path using two optical circuits by allowing CTC to select the Roll To path on the second circuit automatically.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Circuits** tab.

Step 3 Press **Ctrl** and click the two circuits that you want to use in the roll process.

The Roll From path will be on one circuit and the Roll To path will be on the other circuit. The circuits must have a DISCOVERED status and must be the same size and direction for you to start a roll. The planned Roll To circuit must not carry traffic.The first Roll To path must be DCC connected to the source node of the Roll To circuit, and the second Roll To path must be DCC connected to the destination node of the Roll To circuit.

Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

Step 5 In the Roll Attributes area, complete the following:

a. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll (required for a 1-way source roll) or **Manual** to create a manual roll (required for 1-way destination roll).

b. From the Circuit Roll Type drop-down list, choose **Dual.**

c. In the Roll From Circuit area, click the circuit that contains the Roll From path.

Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square representing the fixed path of the first cross-connect to be rolled (Figure 18-13 on page 18-58).

This path is a fixed point in the cross-connect involved in the roll process. The path identifier appears in the text box below the graphic image. The path that is not selected contains the Roll From path. The Roll From path is deleted after the roll is completed.

Step 8 Click **Next**.

Step 9 Complete one of the following:

- If multiple Roll From paths exist, the Select Roll From dialog box appears. Select the path from which you want to roll traffic and click **OK** (Figure 18-18 on page 18-64).
- If multiple Roll From paths do not exist, continue with Step 10.

The circuit status for the Roll From path changes from DISCOVERED to ROLL PENDING.

Step 10 In the Pivot/Fixed Point 2 window, click the square that represents the fixed path of the second connection to be rolled.

The path that is not selected is the Roll From path. The Roll From path is deleted after the roll is completed. The path identifier appears in the text box below the graphic image.

Step 11 Click **Next**.

Step 12 Click **Finish**. In the Circuits tab, the Roll From and Roll To circuits change from the DISCOVERED status to ROLL RENDING.

Step 13 Click the **Rolls** tab. Two new rolls now appear on the Rolls tab. For each pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with Step 14.

- If the Roll Valid Signal status is true, a valid signal was found on the new port.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If the signal is not found, refer to the "General Troubleshooting" chapter in the *Cisco ONS 15600 SDH Troubleshooting Guide*. To cancel the roll, see the "DLP-F357 Cancel a Roll" task on page 18-70.
- The roll is a one-way destination roll and the Roll Valid signal status is false. It is not possible to get a Roll Valid Signal status of true for a one-way destination roll.

  Note You cannot cancel an automatic roll after a valid signal is found.

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

Step 14 If you selected Manual in Step 5, click both rolls on the Rolls tab and click **Complete** to route the traffic to the new port. If you selected Auto, continue with Step 15.

Note You cannot complete a roll if you cancelled the sibling roll. You must complete the two rolls together.

Step 15 For both manual and automatic rolls, click **Finish** to complete the circuit roll process.

Step 16 Return to your originating procedure (NTP).

DLP-F356 Delete a Roll

Purpose	This task deletes a roll. Use caution when selecting this option, traffic may be affected. Delete a roll only if it cannot be completed or cancelled in normal ways. Circuits may have a PARTIAL status when this option is selected. See Table 18-3 on page 18-53 for a description of circuit statuses.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go To Network View**.

Step 2 Click the **Circuits** > **Rolls** tabs.

Step 3 Click the rolled circuit that you want to delete.

Step 4 From the Tools menu, choose **Circuits > Delete Rolls**.

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

Step 6 Return to your originating procedure (NTP).

DLP-F357 Cancel a Roll

Purpose	This task cancels a roll. When the roll mode is Manual, you can only cancel a roll before you click the Complete button. When the roll mode is Auto, cancel roll is only allowed before a good signal is detected by the node or before clicking the Force Valid Signal button. A dual or single roll can be cancelled before the roll state changes to ROLL_COMPLETED.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34 NTP-F181 Bridge and Roll Traffic, page 7-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

⚠ **Caution** If you click cancel while performing a Dual roll in Manual mode and have a valid signal detected on both rolls, you will see a dialog box stating that this can cause a traffic hit and asking if you want to continue with the cancellation. Cisco does not recommend cancelling a dual roll once a valid signal has been detected. To return the circuit to the original state, Cisco recommends completing the roll, then using bridge and roll again to roll the circuit back.

Step 1 From the node or network view, click the **Circuits > Rolls** tabs.

Step 2 Click the rolled circuit that you want to cancel.

Step 3 Click **Cancel**.

Step 4 Return to your originating procedure (NTP).

DLP-F358 Provision a Multirate PPM

Purpose	This task provisions multirate PPMs in CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	Required for 4PIO modules
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The ASAP card hosts up to four 4PIO modules. Each 4PIO hosts four SFPs, which provide a fiber interface that must be provisioned as STM-1, STM-4, STM-16, or Gigabit Ethernet. SFPs are called pluggable port modules (PPMs) in CTC.

Step 1 In node view, double-click the ASAP card where you want to provision PPM settings.

Step 2 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 3 In the Pluggable Port Modules area, click **Create**. The Create PPM dialog box appears.

Step 4 In the Create PPM dialog box, complete the following:

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

Step 5 Click **OK**. The newly created port appears in the Pluggable Port Modules area. The row on the Pluggable Port Modules area turns light blue if the PPM is provisioned strictly as an optical PPM, or green if it is provisioned as a DWDM PPM. The Actual Equipment Type column lists the equipment name.

Step 6 Verify that the PPM appears in the list in the Pluggable Port Modules area. If it does not, repeat Steps 3 through 5.

Step 7 Repeat the task to provision a second PPM.

Step 8 Click **OK**.

Step 9 Continue with the "DLP-F391 Provision an Optical Line Rate and Wavelength" task on page 18-107 to provision the line rate.

Step 10 Return to your originating procedure (NTP).

DLP-F359 Change the Optical Line Rate

Purpose	This task changes PPM port rates for the ASAP card. Perform this task if you want to change the port rate on a multirate SFP that is already provisioned.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the ASAP card where you want to edit the PPM port rate.

Step 2 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 3 Click the port with the port rate that you want to change in the Pluggable Ports area. The highlight changes to dark blue.

Step 4 Click **Edit**. The Edit Port Rate dialog box appears.

Step 5 In the Change To field, use the drop-down list to select the new port rate and click **OK**.

Step 6 Click **Yes** in the Confirm Port Rate Change dialog box.

Step 7 Return to your originating procedure (NTP).

DLP-F360 Delete a PPM

Purpose	This task deletes PPM provisioning for SFPs/XFPs on the ASAP card.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Determine if you can delete the PPM. You cannot delete a port on a PPM if it is in service, part of a protection group, has a communications channel termination in use, is a timing source, has circuits, or has overhead circuits. As needed, complete the following procedures and task:

- NTP-F204 Modify or Delete Optical 1+1 Port Protection Settings, page 11-4
- NTP-F205 Change Node Timing, page 11-5
- NTP-F209 Modify or Delete Communications Channel Terminations, page 11-8
- NTP-F177 Modify and Delete Circuits, page 7-2
- NTP-F178 Modify and Delete Overhead Circuits and Server Trails, page 7-3
- DLP-F254 Change the Service State for a Port, page 17-48

Step 2 In node view, double-click the ASAP card where you want to delete PPM settings.

Step 3 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 4 To delete a PPM and the associated ports:

a. Click the PPM line that appears in the Pluggable Port Modules area. The highlight changes to dark blue.

b. Click **Delete**. The Delete PPM dialog box appears.

c. Click **Yes**. The PPM provisioning is removed from the Pluggable Port Modules area and the Pluggable Ports area.

Step 5 Verify that the PPM provisioning is deleted:

- If the PPM was preprovisioned, CTC shows an empty slot in CTC after it is deleted.
- If the SFP/XFP, 1PIO, or 4PIO (PIM) is physically present when you delete the PPM provisioning, CTC transitions to the deleted state, the ports (if any) are deleted, and the PPM is represented as a gray graphic in CTC. The SFP/XFP or PIM can be provisioned again in CTC, or the equipment can be removed, in which case the removal causes the graphic to disappear.

Step 6 If you need to remove the SFP/XFP, see the "DLP-F389 Remove an SFP/XFP" procedure on page 18-105. If you need to remove the 1PIO or 4PIO where the SFP/XFP is installed, see the "DLP-F390 Remove a 1PIO or 4PIO (PIM) Module" procedure on page 18-106."

Step 7 Return to your originating procedure (NTP).

DLP-F361 Provision OSI Routing Mode

Purpose	This task provisions the Open System Interconnection (OSI) routing mode. Complete this task when the ONS 15600 SDH is connected to networks with third party network elements (NEs) that use the OSI protocol stack for data communications network (DCN) communication.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Do not complete this task until you confirm the role of the node within the network. It will be either an Intermediated System (IS) Level 1 or an IS Level 1/Level 2. This decision must be carefully considered. For additional information about OSI provisioning, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15600 SDH Reference Manual*.

Caution Link State Protocol (LSP) buffers must be the same at all NEs within the network, or loss of visibility might occur. Do not modify the LSP buffers unless you confirm that all NEs within the OSI have the same buffer size.

Caution LSP buffer sizes cannot be greater than the Link Access Protocol on the D Channel (LAP-D) maximum transmission unit (MTU) size within the OSI area.

Note For ONS 15600 SDHs, twelve virtual routers can be provisioned. The node primary Network Service Access Point (NSAP) address is also the Router 1 primary manual area address. To edit the primary NSAP, you must edit the Router 1 primary manual area address. After you enable Router 1 on the Routers subtab, the Change Primary Area Address button is available to edit the address.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node where you want to provision the OSI routing mode. If you are already logged in, continue with Step 2.

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

Step 3 Choose a routing mode:

- **Intermediate System Level 1**—The ONS 15600 SDH performs OSI IS functions. It communicates with IS and End System (ES) nodes that reside within its OSI area. It depends upon an IS L1/L2 node to communicate with IS and ES nodes that reside outside its OSI area.

- **Intermediate System Level 1/Level 2**—The ONS 15600 SDH performs IS functions. It communicates with IS and ES nodes that reside within its OSI area. It also communicates with IS L1/L2 nodes that reside in other OSI areas. Before choosing this option, verify the following:
  - The node is connected to another IS Level 1/Level 2 node that resides in a different OSI area.
  - The node is connected to all nodes within its area that are provisioned as IS L1/L2.

Step 4 If needed, change the LSP data buffers:

- L1 LSP Buffer Size—Adjusts the Level 1 link state PDU buffer size. The default is 512. It should not be changed.
- L2 LSP Buffer Size—Adjusts the Level 2 link state PDU buffer size. The default is 512. It should not be changed.

Step 5 Return to your originating procedure (NTP).

DLP-F362 Provision or Modify TARP Operating Parameters

Purpose	This task provisions or modifies the Target Identifier Address Resolution Protocol (TARP) operating parameters including TARP PDU propagation, timers, and loop detection buffer (LDB).
Tools/Equipment	None
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning > OSI > TARP > Config** tabs.

Step 2 Provision the following parameters, as needed:

- TARP PDUs L1 Propagation—If checked (default), TARP Type 1 PDUs that are received by the node and are not excluded by the LDB are propagated to other NEs within the Level 1 OSI area. (Type 1 PDUs request a protocol address that matches a target identifier [TID] within a Level 1 routing area.) The propagation does not occur if the NE is the target of the Type 1 PDU, and PDUs are not propagated to the NE from which the PDU was received.

  Note This parameter is not used when the Node Routing Area (Provisioning > OSI > Main Setup tab) is set to End System.

- TARP PDUs L2 Propagation—If checked (default), TARP Type 2 PDUs received by the node that are not excluded by the LDB are propagated to other NEs within the Level 2 OSI areas. (Type 2 PDUs request a protocol address that matches a TID within a Level 2 routing area.) The propagation occurs if the NE is not the target of the Type 2 PDU, and PDUs are not propagated to the NE from which the PDU was received.

  Note This parameter is only used when the Node Routing Area is provisioned to Intermediate System Level 1/Level 2.

- TARP PDUs Origination—If checked (default), the node performs all TARP origination functions including:
  - TID to NSAP resolution requests (originate TARP Type 1 and Type 2 PDUs)
  - NSAP to TID requests (originate Type 5 PDUs)
  - TARP address changes (originate Type 4 PDUs)

Note TARP Echo and NSAP to TID is not supported.

- TARP Data Cache—If checked (default), the node maintains a TARP data cache (TDC). The TDC is a database of TID to NSAP pairs created from TARP Type 3 PDUs received by the node and modified by TARP Type 4 PDUs (TID to NSAP updates or corrections). TARP 3 PDUs are responses to Type 1 and Type 2 PDUs. The TDC can also be populated with static entries entered on the TARP > Static TDC tab.

Note This parameter is only used when the TARP PDUs Origination parameter is enabled.

- L2 TARP Data Cache—If checked (default), the TIDs and NSAPs of NEs originating Type 2 requests are added to the TDC before the node propagates the requests to other NEs.

Note This parameter is designed for Intermediate System Level 1/Level 2 nodes that are connected to other Intermediate System Level 1/Level 2 nodes. Enabling the parameter for Intermediate System Level 1 nodes is not recommended.

- LDB—If checked (default), enables the TARP loop detection buffer. The LDB prevents TARP PDUs from being sent more than once on the same subnet.

Note The LDB parameter is not used if the Node Routing Mode is provisioned to End System or if the TARP PDUs L1 Propagation parameter is not enabled.

- LAN TARP Storm Suppression—If checked (default), enables TARP storm suppression. This function prevents redundant TARP PDUs from being unnecessarily propagated across the LAN network.
- Send Type 4 PDU on Startup—If checked, a TARP Type 4 PDU is originated during the initial ONS 15600 SDH startup. Type 4 PDUs indicate that a TID or NSAP change has occurred at the NE. (The default setting is not enabled.)
- Type 4 PDU Delay—Sets the amount of time that will pass before the Type 4 PDU is generated when Send Type 4 PDU on Startup is enabled. 60 seconds is the default. The range is 0 to 255 seconds.

Note The Send Type 4 PDU on Startup and Type 4 PDU Delay parameters are not used if TARP PDUs Origination is not enabled.

- LDB Entry—Sets the TARP loop detection buffer timer. The LDB buffer time is assigned to each LDB entry for which the TARP sequence number (tar-seq) is zero. The default is 5 minutes. The range is 1 to 10 minutes.

- LDB Flush—Sets the frequency period for flushing the LDB. The default is 5 minutes. The range is 0 to 1440 minutes.
- T1—Sets the amount of time to wait for a response to a Type 1 PDU. Type 1 PDUs seek a specific NE TID within an OSI Level 1 area. The default is 15 seconds. The range is 0 to 3600 seconds.
- T2—Sets the amount of time to wait for a response to a Type 2 PDU. TARP Type 2 PDUs seek a specific NE TID value within OSI Level 1 and Level 2 areas. The default is 25 seconds. The range is 0 to 3600 seconds.
- T3—Sets the amount of time to wait for an address resolution request. The default is 40 seconds. The range is 0 to 3600 seconds.
- T4—Sets the amount of time to wait for an error recovery. This timer begins after the T2 timer expires without finding the requested NE TID. The default is 20 seconds. The range is 0 to 3600 seconds.

Note Timers T1, T2, and T4 are not used if TARP PDUs Origination is not enabled.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-F363 Add a Static TID-to-NSAP Entry to the TARP Data Cache

Purpose	This task adds a static TID-to-NSAP entry to the TDC. The static entries are required for NEs that do not support TARP and are similar to static routes. For a specific TID, you must force a specific NSAP.
Tools/Equipment	None
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioner or higher

Step 1 In node view, click the **Provisioning > OSI > TARP > Static TDC** tabs.

Step 2 Click **Add Static Entry**.

Step 3 In the Add Static Entry dialog box, enter the following:

- TID—Enter the TID of the NE. (For ONS nodes, the TID is the Node Name parameter on the node view Provisioning > General tab.)
- NSAP—Enter the OSI NSAP address in the NSAP field or, if preferred, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box.

Step 4 Click **OK** to close the Masked NSAP Entry dialog box, if used, and then click **OK** to close the Add Static Entry dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-F364 Remove a Static TID-to-NSAP Entry from the TARP Data Cache

Purpose	This task removes a static TID-to-NSAP entry from the TDC.
Tools/Equipment	None
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioner or higher

Step 1 In node view, click the **Provisioning > OSI > TARP > Static TDC** tabs.

Step 2 Click the static entry that you want to delete.

Step 3 Click **Delete Static Entry**.

Step 4 In the Delete TDC Entry dialog box, click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-F365 Add a TARP Manual Adjacency Table Entry

Purpose	This task adds an entry to the TARP manual adjacency table (MAT). Entries are added to the MAT when the ONS 15600 SDH must communicate across routers or non-SDH NEs that lack TARP capability.
Tools/Equipment	None
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, click the **Provisioning > OSI > TARP > MAT** tabs.

Step 2 Click **Add**.

Step 3 In the Add TARP Manual Adjacency Table Entry dialog box, enter the following:

- Level—Sets the TARP Type Code that will be sent:
  - **Level 1**—Indicates that the adjacency is within the same area as the current node. The entry generates Type 1 PDUs.
  - **Level 2**—Indicates that the adjacency is in a different area than the current node. The entry generates Type 2 PDUs.
- NSAP—Enter the OSI NSAP address in the NSAP field or, if preferred, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box.

Step 4 Click **OK** to close the Masked NSAP Entry dialog box, if used, and then click **OK** to close the Add Static Entry dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-F366 Provision OSI Routers

Purpose	This task enables an OSI router and edits its primary manual area address.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Router 1 must be enabled before you can enable and edit the primary manual area addresses for Routers 2 through 12.

Note The Router 1 manual area address, System ID, and Selector "00" create the node NSAP address. Changing the Router 1 manual area address changes the node's NSAP address.

Note The System ID for Router 1 is the node MAC address. The System IDs for Routers 2 through 12 are created by adding 1 through 12 respectively to the Router 1 System ID. You cannot edit the System IDs.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node of the OSI routers that you want to provision.

Step 2 Click the **Provisioning > OSI > Routers > Setup** tabs.

Step 3 Chose the router you want provision and click **Edit**. The OSI Router Editor dialog box appears.

Step 4 In the OSI Router Editor dialog box:

a. Check **Enable Router** to enable the router and make its primary area address available for editing.

b. Click the manual area address, then click **Edit**.

c. In the Edit Manual Area Address dialog box, edit the primary area address in the Area Address field. If you prefer, click **Use Mask** and enter the edits in the Masked NSAP Entry dialog box. The address (hexadecimal format) can be 8 to 24 alphanumeric characters (0–9, a–f) in length.

d. Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Edit Manual Area Address, and OSI Router Editor.

Step 5 Return to your originating procedure (NTP).

DLP-F367 Provision Additional Manual Area Addresses

Purpose	This task provisions the OSI manual area addresses. One primary and two additional manual areas can be created for each virtual router.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2 DLP-F366 Provision OSI Routers, page 18-78
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **Provisioning** > **OSI** > **Routers** > **Setup** tabs.

Step 2 Chose the router where you want provision an additional manual area address and click **Edit**. The OSI Router Editor dialog box appears.

Step 3 In the OSI Router Editor dialog box:

a. Check **Enable Router** to enable the router and make its primary area address available for editing.

b. Click the manual area address, then click **Add**.

c. In the Add Manual Area Address dialog box, enter the primary area address in the Area Address field. If you prefer, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box. The address (hexadecimal format) can be 2to 24 alphanumeric characters (0–9, a–f) in length.

d. Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Add Manual Area Address, and OSI Router Editor.

Step 4 Return to your originating procedure (NTP).

DLP-F368 Enable the OSI Subnet on the LAN Interface

Purpose	This task enables the OSI subnetwork point of attachment on the LAN interface.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note OSI subnetwork points of attachment are enabled on DCCs when you create DCCs. See the "DLP-F253 Provision RS-DCC Terminations" task on page 17-46 and the "DLP-F314 Provision MS-DCC Terminations" task on page 18-14.

Note If Secure Mode is on, the OSI Subnet is enabled on the backplane LAN port, not the TSC port.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node whose OSI routers you want to provision.

Step 2 Click the **Provisioning > OSI > Routers > Subnet** tabs.

Step 3 Click **Enable LAN Subnet**.

Step 4 In the Enable LAN Subnet dialog box, complete the following fields:

- ESH—Sets the End System Hello (ESH) propagation frequency on ONS nodes that can be provisioned as end system NEs. The field is not used by the ONS 15600 SDH.
- ISH—Sets the Intermediate System Hello PDU propagation frequency. Intermediate system NEs send ISHs to other ESs and ISs to inform them about the IS NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- IIH—Sets the Intermediate System to Intermediate System Hello PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
- IS-IS Cost—Sets the cost for sending packets on the LAN subnet. The IS-IS protocol uses the cost to calculate the shortest routing path. The default IS-IS cost for LAN subnets is 20. It normally should not be changed.
- DIS Priority—Sets the designated intermediate system (DIS) priority. In IS-IS networks, one router is elected to serve as the DIS (LAN subnets only). Cisco router DIS priority is 64. For the ONS 15454 LAN subnet, the default DIS priority is 63. It normally should not be changed.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-F369 Create an IP-Over-CLNS Tunnel

Purpose	This task creates an IP-over-Connectionless Network Layer Service (CLNS) tunnel to allow ONS 15600 SDHs to communicate across equipment and networks that use the OSI protocol stack.
Tools/Equipment	None
Prerequisite Procedures	NTP-F131 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution IP-over-CLNS tunnels require two endpoints. You will create one point on an ONS 15600 SDH. The other end point is generally provisioned on non-ONS equipment including routers and other vendor NEs. Before you begin, verify that you have the capability to create an OSI-over-IP tunnel on the other equipment location.

Step 1 Complete the "DLP-F181 Log into CTC" task on page 16-34 at the node of the OSI routers that you want to provision.

Step 2 Click the **Provisioning > OSI > Tunnels** tabs.

Step 3 Click **Create**.

Step 4 In the Create IP Over OSI Tunnel dialog box, complete the following fields:

- Tunnel Type—Choose a tunnel type:
  - **Cisco**—Creates the proprietary Cisco IP tunnel. Cisco IP tunnels add the CLNS header to the IP packets.
  - **GRE**—Creates a Generic Routing Encapsulation tunnel. GRE tunnels add the CLNS header and a GRE header to the IP packets.

  The Cisco proprietary tunnel is slightly more efficient than the GRE tunnel because it does not add the GRE header to each IP packet. The two tunnel types are not compatible. Most Cisco routers support the Cisco IP tunnel, while only a few support both GRE and Cisco IP tunnels. You generally should create Cisco IP tunnels if you are tunneling between two Cisco routers or between a Cisco router and an ONS node.

Caution Always verify that the IP-over-CLNS tunnel type you choose is supported by the equipment at the other end of the tunnel.

- Node Address—Enter the IP address of the IP-over-CLNS tunnel destination.
- Subnet Mask—Enter the IP address subnet mask of the IP-over-CLNS destination.
- OSPF Cost—Enter the Open Shortest Path First (OSPF) cost for sending packets across the IP-over-CLNS tunnel. The OSPF cost is used by OSPF routers to calculate the shortest path. The default is 110. Normally, it is not be changed unless you are creating multiple tunnel routes and want to prioritize routing by assigning different metrics.
- NSAP—Enter the destination NE or OSI router NSAP address.

Step 5 Click **OK**.

Step 6 Provision the other tunnel endpoint using the documentation for the other equipment.

Step 7 Return to your originating procedure (NTP).

DLP-F370 Remove a TARP Manual Adjacency Table Entry

Purpose	This task removes an entry from the TARP manual adjacency table.
Tools/Equipment	None
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution If TARP manual adjacency is the only means of communication to a group of nodes, loss of visibility will occur when the adjacency table entry is removed.

Step 1 In node view, click the **Provisioning > OSI > TARP > MAT** tabs.

Step 2 Click the MAT entry that you want to delete.

Step 3 Click **Remove**.

Step 4 In the Delete TDC Entry dialog box, click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-F371 Change the OSI Routing Mode

Purpose	This task changes the OSI routing mode.
Tools/Equipment	None
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Do not complete this procedure until you confirm the role of the node within the network. It will be either an IS Level 1 or an IS Level 1/Level 2. This decision must be carefully considered. For additional information about OSI provisioning, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15600 SDH Reference Manual*.

Caution LSP buffers must be the same at all NEs within the network, or loss of visibility could occur. Do not modify the LSP buffers unless you are sure that all NEs within the OSI have the same buffer size.

Caution LSP buffer sizes cannot be greater than the LAP-D MTU size within the OSI area.

Step 1 Verify that all L1/L2 virtual routers on the NE must reside in the same area. This means that all neighboring virtual routers must have at least one common area address.

Step 2 In node view, click the **Provisioning** > **OSI** > **Main Setup** tabs.

Step 3 Choose one of the following routing modes:

- **Intermediate System Level 1**—The ONS 15600 SDH performs OSI IS functions. It communicates with IS and ES nodes that reside within its OSI area. It depends upon an IS L1/L2 node to communicate with IS and ES nodes that reside outside its OSI area.
- **Intermediate System Level 1/Level 2**—The ONS 15600 SDH performs IS functions. It communicates with IS and ES nodes that reside within its OSI area. It also communicates with IS L1/L2 nodes that reside in other OSI areas. Before choosing this option, verify the following:
  - The node is connected to another IS Level 1/Level 2 node that resides in a different OSI area.
  - The node is connected to all nodes within its area that are provisioned as IS L1/L2.

Note Changing a routing mode should be carefully considered. Additional information about OSI systems and protocols are provided in the "Management Network Connectivity" chapter of the *Cisco ONS 15600 SDH Reference Manual*.

Step 4 Although Cisco does not recommend changing the Link State Protocol Data Unit (LSP) buffer sizes, you can adjust the buffers in the following fields:

- L1 LSP Buffer Size—Adjusts the Level 1 link state PDU buffer size.
- L2 LSP Buffer Size—Adjusts the Level 2 link state PDU buffer size.

Step 5 Return to your originating procedure (NTP).

DLP-F372 Edit the OSI Router Configuration

Purpose	This task allows you to edit the OSI router configuration, including enabling and disabling OSI routers, editing the primary area address, and creating or editing additional area addresses.
Tools/Equipment	None
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **Provisioning > OSI > Routers > Setup** tabs.

Step 2 Chose the router you want provision and click **Edit**.

Step 3 In the OSI Router Editor dialog box:

a. Check or uncheck the Enabled box to enable or disable the router.

Note Router 1 must be enabled before you can enable Routers 2 through 12.

b. For enabled routers, edit the primary area address, if needed. The address can be between 8 and 24 alphanumeric characters in length.

c. If you want to add or edit an area address to the primary area, enter the address at the bottom of the Multiple Area Addresses area. The area address can be 2 to 26 numeric characters (0–9) in length. Click **Add**.

d. Click **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-F373 Edit the OSI Subnetwork Point of Attachment

Purpose	This task allows you to view and edit the OSI subnetwork point of attachment parameters. The parameters are initially provisioned when you create a regenerator section DCC (RS-DCC) or multiplex section DCC (MS-DCC), or when you enable the LAN subnet.
Tools/Equipment	None
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, click the **Provisioning > OSI > Routers > Subnet** tabs.

Step 2 Choose the subnet you want to edit, then click **Edit**.

Step 3 In the Edit *subnet type* Subnet *slot/port* dialog box, edit the following fields:

- ESH—The End System Hello PDU propagation frequency. The field is not used by the ONS 15600 SDH.
- ISH—The Intermediate System Hello PDU propagation frequency. An intermediate system NE sends ISHs to other ESs and ISs to inform them about the NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- IIH—The Intermediate System to Intermediate System Hello PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.

Note The IS-IS Cost and DIS Priority parameters are provisioned when you create or enable a subnet. You cannot change the parameters after the subnet is created. To change the DIS Priority and IS-IS Cost parameters, delete the subnet and create a new one.

Click **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-F374 Edit an IP-Over-CLNS Tunnel

Purpose	This task allows you to edit the parameters of an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite procedures	DLP-F369 Create an IP-Over-CLNS Tunnel, page 18-80 DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Changing the IP or NSAP addresses or an IP-over-CLNS tunnel can cause loss of NE visibility or NE isolation. Do not change network addresses until you verify the changes with your network administrator.

Step 1 Click the **Provisioning > OSI > Tunnels** tabs.

Step 2 Click **Edit**.

Step 3 In the Edit IP Over OSI Tunnel dialog box, complete the following fields:

- Tunnel Type—Edit the tunnel type:
  - **Cisco**—Creates the proprietary Cisco IP tunnel. Cisco IP tunnels add the CLNS header to the IP packets.
  - **GRE**—Creates a Generic Routing Encapsulation tunnel. GRE tunnels add the CLNS header and a GRE header to the IP packets.

  The Cisco proprietary tunnel is slightly more efficient than the GRE tunnel because it does not add the GRE header to each IP packet. The two tunnel types are not compatible. Most Cisco routers support the Cisco IP tunnel, while only a few support both GRE and Cisco IP tunnels. You generally should create Cisco IP tunnels if you are tunneling between two Cisco routers or between a Cisco router and an ONS node.

Caution Always verify that the IP-over-CLNS tunnel type you choose is supported by the equipment at the other end of the tunnel.

- Node Address—Enter the IP address of the IP-over-CLNS tunnel destination.
- Subnet Mask—Enter the IP address subnet mask of the IP-over-CLNS destination.
- OSPF Cost—Enter the OSPF cost for sending packets across the IP-over-CLNS tunnel. The OSPF cost is used by OSPF routers to calculate the shortest path. The default is 110. Normally, it is not be changed unless you are creating multiple tunnel routes and want to prioritize routing by assigning different metrics.
- NSAP—Enter the destination NE or OSI router NSAP address.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-F375 Delete an IP-Over-CLNS Tunnel

Purpose	This task allows you to delete an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Deleting an IP-over-CLNS tunnel might cause the nodes to lose visibility or cause node isolation. If node isolation occurs, onsite provisioning might be required to regain connectivity. Always confirm tunnel deletions with your network administrator.

Step 1 Click the **Provisioning > OSI > Tunnels** tabs.

Step 2 Choose the IP-over-CLNS tunnel that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-F376 View IS-IS Routing Information Base

Purpose	This task allows you to view the IS-IS protocol routing information base (RIB). IS-IS is an OSI routing protocol that floods the network with information about NEs on the network. Each NE uses the information to build a complete and consistent picture of a network topology. The IS-IS RIB shows the network view from the perspective of the IS node.
Tools/Equipment	None
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, click the **Maintenance > OSI > IS-IS RIB** tabs.

Step 2 View the following RIB information for Router 1:

- Subnet Type—Indicates the OSI subnetwork point of attachment type used to access the destination address. Subnet types include RS-DCC, MS-DCC, GCC, OSC, and LAN.
- Location—Indicates the OSI subnetwork point of attachment. For DCC subnets, the slot and port are displayed. LAN subnets are shown as LAN.
- Destination Address—The destination NSAP of the IS.
- MAC Address—For destination NEs that are accessed by LAN subnets, the NE MAC address.

Step 3 If additional routers are enabled, you can view their RIBs by choosing the router number in the Router field and clicking **Refresh**.

Step 4 Return to your originating procedure (NTP).

DLP-F377 View ES-IS Routing Information Base

Purpose	This task allows you to view the End System to Intermediate System (ES-IS) protocol RIB. ES-IS is an OSI protocol that defines how end systems (hosts) and intermediate systems (routers) learn about each other. For ESs, the ES-IS RIB shows the IS used to access the OSI network. For ISs, the only OSI level that can be provisioned on the ONS 15600 SDH, the ES-IS RIB shows the ESs connected to the IS node.
Tools/Equipment	None
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, click the **Maintenance > OSI > ES-IS RIB** tabs.

Step 2 View the following RIB information for Router 1:

- Subnet Type—Indicates the OSI subnetwork point of attachment type used to access the destination address. Subnet types include RS-DCC, MS-DCC, GCC, OSC, and LAN.
- Location—Indicates the subnet interface. For DCC subnets, the slot and port are displayed. LAN subnets are shown as LAN.
- Destination Address—The destination IS NSAP.
- MAC Address—For destination NEs that are accessed by LAN subnets, the NE MAC address.

Step 3 If additional routers are enabled, you can view their RIBs by choosing the router number in the Router field and clicking **Refresh**.

Step 4 Return to your originating procedure (NTP).

DLP-F378 Manage the TARP Data Cache

Purpose	This task allows you to view and manage the TDC. The TDC facilitates TARP processing by storing a list of TID to NSAP mappings.
Tools/Equipment	None
Prerequisite procedures	DLP-F181 Log into CTC, page 16-34
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, click the **Maintenance > OSI > TDC** tabs.

Step 2 View the following TDC information:

- TID—The target identifier of the originating NE. For ONS 15600 SDHs, the TID is the name entered in the Node Name/TID field on the Provisioning > General tab.

- NSAP/NET—The Network Service Access Point or Network Element Title of the originating NE.
- Type—Indicates how the TDC entry was created:
  - **Dynamic**—The entry was created through the TARP propagation process.
  - **Static**—The entry was manually created and is a static entry.

Step 3 If you want to query the network for an NSAP that matches a TID, complete the following steps. Otherwise, continue with Step 4.

Note The TID to NSAP function is not available if the TDC is not enabled on the Provisioning > OSI > TARP subtab.

a. Click the **TID to NSAP** button.

b. In the TID to NSAP dialog box, enter the TID you want to map to an NSAP.

c. Click **OK**, then click **OK** on the information message.

d. On the TDC tab, click **Refresh**.

If TARP finds the TID in its TDC it returns the matching NSAP. If not, TARP sends PDUs across the network. Replies will return to the TDC later, and a check TDC later message is displayed.

Step 4 If you want to delete all the dynamically generated TDC entries, click the **Flush Dynamic Entries** button. If not, continue with Step 5.

Step 5 Return to your originating procedure (NTP).

DLP-F379 Export CTC Data

Purpose	This task exports CTC table data for use by other applications such as spreadsheets, word processors, and database management applications. You can also export data from the Edit Circuits window.
Equipment/Tools	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Click the CTC tab containing the information you want to export (for example, the Alarms or Circuits tab).

Step 2 If you want to export detailed circuit information, complete the following:

a. In the Circuits window, choose a circuit and click **Edit** to open it in the Edit Circuits window.

b. In the Edit Circuits window, choose the desired tab: Drops, SNCP Selectors, SNCP Switch Counts, State, or Merge.

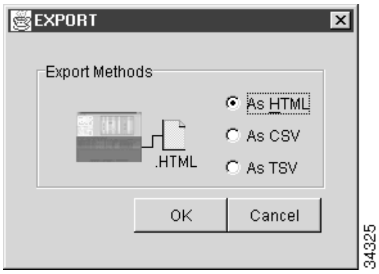
Note Depending upon your configuration, you may or may not see all of the above tabs when you click Edit.

Step 3 From the CTC File menu, click **Export**.

Step 4 In the Export dialog box choose a format for the data (Figure 18-19):

- **As HTML**—Saves the data as an HTML file. The file can be viewed with a web browser without running CTC.
- **As CSV**—Saves the CTC table values as text, separated by commas. You can import CSV data into spreadsheets and database management programs.
- **As TSV**—Saves the CTC table values as text, separated by tabs. You can import TSV data into spreadsheets and database management programs.

Figure 18-19 Selecting CTC Data for Export



Step 5 If you want to open a file in a text editor or word processor application, procedures vary; typically you can use the **File** > **Open** command to display the CTC data, or you can double-click the file name and choose an application such as Notepad.

Text editor and word processor applications display the data exactly as it is exported, including comma or tab separators. All applications that open the data files allow you to format the data.

Step 6 If you want to open the file in spreadsheet and database management applications, procedures vary; typically you need to open the application and choose **File** > **Import**, then choose a delimited file to display the data in cells.

Spreadsheet and database management programs also allow you to manage the exported data.

Note An exported file cannot be opened in CTC.

As the export operation applies to tabular data only, it is not available for the following CTC tabs and subtabs:

- Provisioning > General window
- Provisioning > SNMP window
- Provisioning > Timing window
- Provisioning > Network > Internal Subnet window
- Provisioning > Network > General window
- Provisioning > Security > Policy window
- Provisioning > Security > Access window
- Provisioning > Security > Legal Disclaimer window
- Provisioning > OSI > Main Setup window
- Provisioning > OSI > TARP > Config window

- Maintenance > Database window
- Maintenance > Protection window
- Maintenance > Diagnostic window
- Maintenance > Preferred Copy window
- Maintenance > Timing > Source window

Step 7 Click **OK**.

Step 8 In the Save dialog box, enter a file name in one of the following formats:

- *filename*.htm for HTML files
- *filename*.csv for CSV files
- *filename*.tsv for TSV files

Step 9 Navigate to a directory where you want to store the file.

Step 10 Click **OK**.

Step 11 Return to your originating procedure (NTP).

DLP-F379 Set Up SNMP for a GNE

Purpose	This procedure provisions simple network management protocol (SNMP) parameters so that you can use SNMP network management software with the ONS 15600 SDH.
Tools/Equipment	None
Prerequisite Procedures	NTP-F129 Log into the ONS 15600 SDH GUI, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP** tabs.

Step 2 In the Trap Destinations area, click **Create**.

Step 3 On the Create SNMP Trap Destination dialog box, complete the following fields:

- Destination Node Address—Enter the IP address of your network management system (NMS).
- Community—Enter the SNMP community name. (For more information about SNMP, refer to the "SNMP" chapter in the *Cisco ONS 15600 SDH Reference Manual*.)

Note The community name is a form of authentication and access control. The community name assigned to the ONS 15600 is case-sensitive and must match the community name of the NMS.

- UDP Port—The default User Datagram Protocol (UDP) port for SNMP traps is 162.

- Trap Version—Choose either SNMPv1 or SNMPv2. Refer to your NMS documentation to determine whether to use SNMPv1 or SNMPv2.

Step 4 Click **OK**. The node IP address of the node where you provisioned the new trap destination appears in the Trap Destinations area.

Step 5 Click the node IP address in the Trap Destinations area. Verify the SNMP information that appears in the Selected Destination list.

Step 6 If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If the box is not checked, SET requests are rejected.

Step 7 If you want to set up the SNMP proxy feature to allow network management, message reporting, and performance statistic retrieval across ONS firewalls, click the **Enable SNMP Proxy** check box on the SNMP tab.

Note The ONS firewall proxy feature only operates on nodes running releases 4.6 and later. Using this information effectively breaches the ONS firewall to exchange management information.

Note In ONS 15600 Software R9.0 and later, you can configure IPv6 addresses for SNMPv1/v2 on a GNE, in addition to IPv4 addresses.

For more information about the SNMP proxy feature, refer to the "SNMP" chapter of the *Cisco ONS 15600 SDH Reference Manual*.

Step 8 Click **Apply**.

Step 9 Return to your originating procedure (NTP).

DLP-F380 Set Up SNMP for an ENE

Purpose	This procedure provisions the SNMP parameters for an ONS 15600 SDH configured to be an ENE if you use SNMP proxy on the GNE.
Tools/Equipment	None
Prerequisite Procedures	NTP-F129 Log into the ONS 15600 SDH GUI, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP** tabs.

Step 2 In the Trap Destinations area, click **Create**.

Step 3 On the Create SNMP Trap Destination dialog box, complete the following fields:

- Destination Node Address—Enter the IP address of your NMS.

Note In ONS 15600 Software Release 9.0 and later, you can configure IPv6 addresses for SNMPv2/v3 Trap destinations and SNMPv3 Proxy Targets, in addition to IPv4 addresses.

- Community—Enter the SNMP community name. (For more information about SNMP, refer to the "SNMP" chapter in the *Cisco ONS 15600 SDH Reference Manual*.)

  Note The community name is a form of authentication and access control. The community name assigned to the ONS 15600 is case-sensitive and must match the community name of the NMS.

- UDP Port—The default UDP port for SNMP traps is 162.
- Trap Version—Choose either SNMPv1 or SNMPv2. Refer to your NMS documentation to determine whether to use SNMPv1 or SNMPv2.

Step 4 Click **OK**. The node IP address of the node where you provisioned the new trap destination appears in the Trap Destinations area.

Step 5 Click the node IP address in the Trap Destinations area. Verify the SNMP information that appears in the Selected Destination list.

Step 6 If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If the box is not checked, SET requests are rejected.

Step 7 If you want to set up the SNMP proxy feature to allow network management, message reporting, and performance statistic retrieval across ONS firewalls, click the **Enable SNMP Proxy** check box on the SNMP tab.

Note The ONS firewall proxy feature only operates on nodes running releases 4.6 and later. Using this information effectively breaches the ONS firewall to exchange management information.

For more information about the SNMP proxy feature, refer to the "SNMP" chapter of the *Cisco ONS 15600 SDH Reference Manual*.

Step 8 Click **Apply**.

Step 9 If you are setting up SNMP proxies, you can set up to three relays for each trap address to convey SNMP traps from the NE to the NMS. To do this, complete the following substeps:

a. Click the first trap destination IP address. The address and its community name appear in the Destination fields.

b. If the node you are logged into is an ENE, set the Relay A address to the GNE and type its community name in the community field. If there are NEs between the GNE and ENE, you can enter up to two SNMP proxy relay addresses and community names in the fields for Relay and Relay C. When doing this, consult the following guidelines:

- If the NE is directly connected to the GNE, enter the address and community name of the GNE for Relay A.
- If this NE is connected to the GNE through other NEs, enter the address and community name of the GNE for Relay A and the address and community name of NE 1 for Relay B and NE 2 for Relay C.

The SNMP proxy directs SNMP traps in the following general order:
ENE > RELAY C > RELAY B > RELAY A > NMS. The following parameters also apply:

- If there is are 0 intermediate relays, the order is ENE > RELAY A (GNE) > NMS
- If there is 1 intermediate relay, the order is ENE > RELAY B (NE1) > RELAY A(GNE) > NMS
- If there are 2 intermediate relays, the order is ENE > RELAY C (NE2) > RELAY B (NE 1) > RELAY A (GNE) > NMS.

Step 10 Click **Apply**.

Step 11 Repeat Step 2 through Step 10 for all NEs between the GNE and ENE.

Step 12 Return to your originating procedure (NTP).

DLP-F381 Configure the Node for RADIUS Authentication

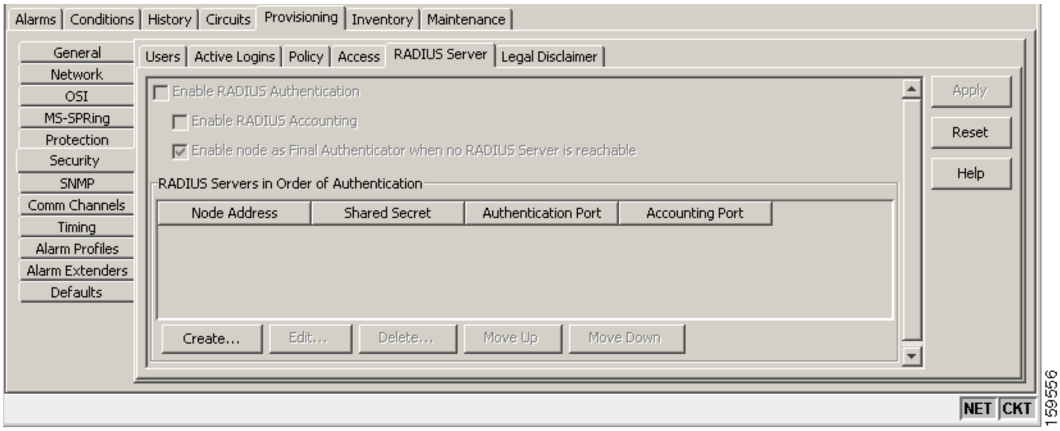
Purpose	This task allows you to configure a node for Remote Authentication Dial In User Service (RADIUS) authentication. RADIUS validates remote users who are attempting to connect to the network.
Tools/Equipment	None
Prerequisite procedures	NTP-F129 Log into the ONS 15600 SDH GUI, page 3-5 Before configuring the node for RADIUS authentication, you must first add the node as a network device on the RADIUS server. Refer to the *User Guide for Cisco Secure ACS for Windows Server* for more information about configuring a RADIUS server.
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution Do not configure a node for RADIUS authentication until after you have added that node to the RADIUS server and added the RADIUS server to the list of authenticators. If you do not add the node to a RADIUS server prior to activating RADIUS authentication, no user will be able to access the node. Refer to the *User Guide for Cisco Secure ACS for Windows Server* for more information about adding a node to a RADIUS server.

Note The following Cisco vendor-specific attribute (VSA) needs to be specified when adding users to the RADIUS server:
shell:priv-lvl=N, where N is:
0 for Retrieve User
1 for Maintenance User
2 for Provisioning User
3 for Super User

Step 1 In node view, click the **Provisioning > Security > RADIUS Server** tabs (Figure 18-20).

Figure 18-20 RADIUS Server Tab



□ Enable RADIUS Authentication

□ Enable RADIUS Accounting

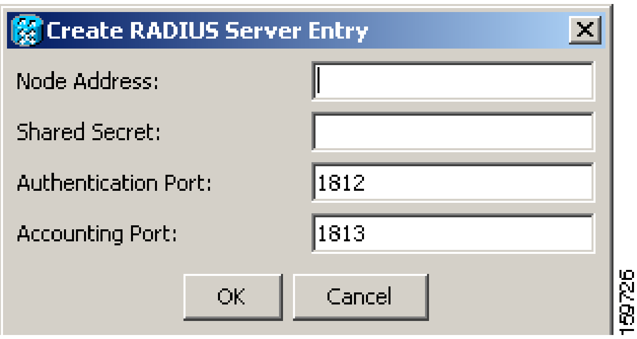
☑ Enable node as Final Authenticator when no RADIUS Server is reachable

RADIUS Servers in Order of Authentication

Node Address	Shared Secret	Authentication Port	Accounting Port

Step 2 Click **Create** to add a RADIUS server to the list of authenticators. The Create RADIUS Server Entry window appears (Figure 18-21).

Figure 18-21 Create RADIUS Server Entry Window



Node Address:

Shared Secret:

Authentication Port: 1812

Accounting Port: 1813

Step 3 Enter the RADIUS server IP address in the node Address field. If the node is an end network element (ENE), enter the IP address of the gateway network element (GNE) in this field.

The GNE passes authentication requests from the ENEs in its network to the RADIUS server, which grants authentication if the GNE is listed as a client on the server.

Note In ONS 15600 Software R9.0 and later, you can configure IPv6 addresses for RADIUS servers, in addition to IPv4 addresses.

Caution Because the ENE nodes use the GNE to pass authentication requests to the RADIUS server, you must add the ENEs to the RADIUS server individually for authentication. If you do not add the ENE node to a RADIUS server prior to activating RADIUS authentication, no user will be able to access the node. Refer to the *User Guide for Cisco Secure ACS for Windows Server* for more information about adding a node to a RADIUS server.

Step 4 Enter the shared secret in the Shared Secret field. A shared secret is a text string that serves as a password between a RADIUS client and RADIUS server.

Step 5 Enter the RADIUS authentication port number in the Authentication Port field. The default port is 1812. If the node is an ENE, set the authentication port to a number within the range of 1860 to 1869.

Step 6 Enter the RADIUS accounting port in the Accounting Port field. The default port is 1813. If the node is an ENE, set the accounting port to a number within the range of 1870 to 1879.

Step 7 Click **OK**. The RADIUS server is added to the list of RADIUS authenticators.

Note You can add up to 10 RADIUS servers to a node’s list of authenticators.

Step 8 Click **Edit** to make changes to an existing RADIUS server. You can change the IP address, the shared secret, the authentication port, and the accounting port.

Step 9 Click **Delete** to delete the selected RADIUS server.

Step 10 Click **Move Up** or **Move Down** to reorder the list of RADIUS authenticators. The node requests authentication from the servers sequentially from top to bottom. If one server is unreachable, the node will request authentication from the next RADIUS server on the list.

Step 11 Click the **Enable RADIUS Authentication** check box to activate remote-server authentication for the node.

Step 12 Click the **Enable RADIUS Accounting** check box if you want to show RADIUS authentication information in the audit trail.

Step 13 Click the **Enable node as Final Authenticator when no RADIUS Server is reachable** check box if you want the node to be the final authenticator. This means that if every RADIUS authenticator is unavailable, the node will authenticate the login rather than locking the user out.

Step 14 Click **Apply** to save all changes or **Reset** to clear all changes.

Step 15 Return to your originating procedure (NTP).

DLP-F382 Delete a Server Trail

Purpose	This task deletes a server trail.
Tools/Equipment	None
Prerequisite Procedures	See Chapter 6, “Create Circuits” for server trail creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Deleting server trails do not impact the circuits provisioned over it as server trail is a logical link. Deleting a server trail is recommended when migrating from IPv4 to IPv6 because the server trails created on a IPv4 network will not work in an IPv6 network. You can recreate server trails after migrating to IPv6 network without deleting the circuits. When you delete a server trail, the circuit state becomes PARTIAL.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > Server Trails** tabs.

Step 3 Click the server trail that you want to delete.

Step 4 Click **Delete**.

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

Note You can use the server trail audit log to recreate a server trail that you may have accidentally deleted. The server trail audit log includes the following parameters:

- Server trail ID
- Peer IP address
- Circuit size
- Protection type
- Number of trails
- Starting VC4/VC3
- SRLG value

You can look at the audit log of the source or destination node and find the entry for the delete call. This log entry has the VC4/VC3 path definitions on the node, peer IP address, and server trail ID. You can then look at the audit log of the peer IP address, locate the delete call for the specific server trail ID, and find the VC4/VC3 path definitions on the node. This would provide you with the required information to recreate the server trail.

Note It is recommended that you delete one server trail at a time as the deletion of multiple trails together may cause CTC to hang and is a time consuming task.

Step 6 Return to your originating procedure (NTP).

DLP-F383 Grant Superuser Privileges to a Provisioning User

Purpose	This task enables a provisioning-level user to perform tasks such as retrieving audit logs, restoring databases, and activating and reverting software loads.
Tools/Equipment	None
Prerequisite Procedures	NTP-F129 Log into the ONS 15600 SDH GUI, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning** > **Defaults** tabs.

Step 2 In the Node Defaults area, choose **NODE**. **security**.**grantPermission**.*.

Step 3 Click in the Default Value column for the default property you are changing and choose **Provisioning** from the drop-down list.

Note If you click **Reset** before you click **Apply**, all values will return to their original settings.

Step 4 Click **Apply**.

A pencil icon appears next to the default name that will be changed as a result of editing the defaults file.

Note You must close your current CTC session and restart a new CTC session for the changes to take effect.

Step 5 Return to your originating procedure (NTP).

DLP-F384 Download an Alarm Severity Profile

Purpose	This task downloads a custom alarm severity profile from a network-drive accessible CD-ROM, floppy disk, or hard disk location.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs

Step 2 To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 3 To access the profile editor from a card view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 4 Click **Load**.

Step 5 If you want to download a profile that exists on the node, click **From Node** in the Load Profile(s) dialog box and complete the following steps:

a. Click the node name you are logged into in the Node Names list.

b. Click the name of the profile in the Profile Names list, such as Default.

Step 6 If you want to download a profile that is stored locally or on a network drive, click **From File** in the Load Profile(s) dialog box. Then complete the following steps:

a. Click **Browse**.

b. Navigate to the file location in the Open dialog box.

c. Click **Open**.

Note The Default alarm profile list contains alarm and condition severities that correspond when applicable to default values established in Telcordia GR-474-CORE.

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

Step 7 Click **OK**. The downloaded profile appears at the right side of the Alarm Profiles window.

Step 8 Right-click anywhere in the downloaded profile column to view the profile editing shortcut menu.

Step 9 Click **Store**.

Step 10 In the Store Profile(s) dialog box, click **To Node(s)** and complete the following steps:

a. Choose the nodes where you want to save the profile:

- If you want to save the profile to only one node, click the node in the Node Names list.
- If you want to save the profile to all nodes, click **Select All**.
- If you do not want to save the profile to any nodes, click **Select None**.
- If you want to update alarm profile information, click **Synchronize**.

b. Click **OK**.

Step 11 Return to your originating procedure (NTP).

DLP-F385 Install the ASAP 1PIO and 4PIO (PIM) Modules

Purpose	This procedure explains how to install the 4-port I/O modules (4PIOs) and 1-port I/O modules (1PIOs), also known as Pluggable Interface Modules (PIMs), in the carrier modules of the ASAP card.
Tools/Equipment	4PIO modules and/or 1PIO modules #2 Phillips screwdriver
Prerequisite Procedures	DLP-F333 Install the ASAP Carrier Modules, page 18-33
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the midplane with your hand or any metal tool, or you could shock yourself.** Statement 181

Caution Always use the supplied ESD wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-left outside edge of the shelf.

Warning **Class 1 laser product.** Statement 1008

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

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

Note For information about the ASAP card, refer to the *Cisco ONS 15600 SDH Reference Manual.*

Step 1 Remove the 1PIO or 4PIO module from the box and antistatic sleeve.

Step 2 Identify the slot on the ASAP card where you want to install the 1PIO or 4PIO module.

Step 3 Carefully slide the module along the top and bottom guide rails into the correct slot.

Step 4 Tighten the screws at the top right and bottom left of the module. You can either hand-tighten the screws or remove the screw covers and use a Phillips screwdriver to tighten the screws.

Figure 18-22 shows the 1PIO module faceplate.

Figure 18-22 1PIO Module Faceplate

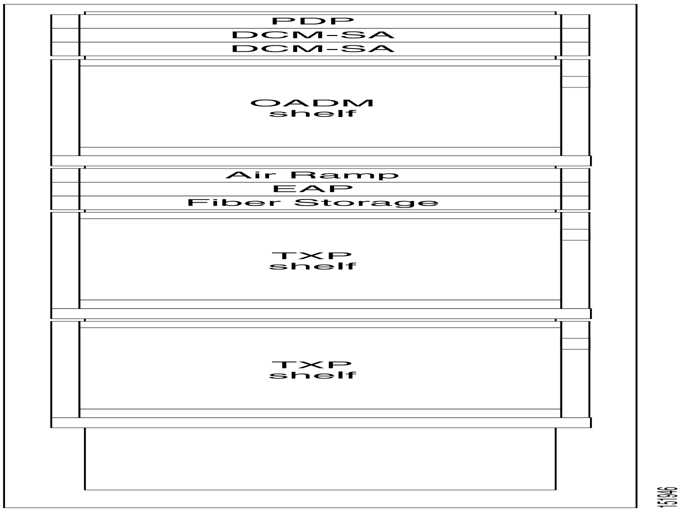
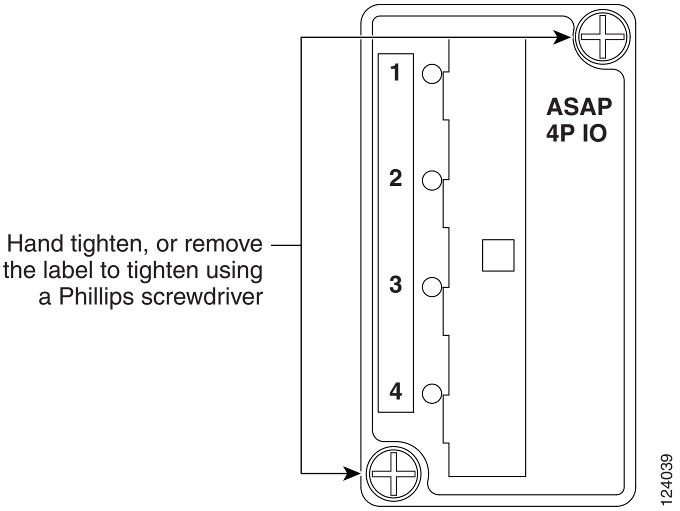


Figure 18-23 shows the 4PIO module faceplate.

Figure 18-23 4PIO Module Faceplate


1
2
3
4
ASAP
4P IO
Hand tighten, or remove the label to tighten using a Phillips screwdriver
124039

Note The LEDs located on the 1PIO and 4PIO will not light until a fixed rate SFP/XFP (PPM) is installed in the associated PPM slot or a multirate optical (MRO) PPM is installed and an optical rate is provisioned. If the port on the PP M does not have a raised alarm, the associated LED will be green in color (meaning the port administrative state is Unlocked-automaticInservice). If the port has an alarm, the LED will be amber in color (meaning the administrative state is Unlocked and a valid signal is not present).

Note If you insert a card into a slot that is provisioned for a different card, all red LEDs turn on and you will see an MEA alarm for that slot when you open CTC.

Step 5 After you have logged into CTC, verify that the card appears in the card view. See Chapter 3, "Connect the PC and Log into the GUI" for CTC information and setup instructions.

Step 6 Return to your originating procedure (NTP).

DLP-F386 Consolidate Links in Network View

Purpose	This task consolidates the data communications channel (DCC), GSS, OTS, and server trail links in the CTC network view.
Tools/Equipment	None
Prerequisite procedures	NTP-F129 Log into the ONS 15600 SDH GUI, page 3-5
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note Global consolidation persists when CTC is launched againbut local consolidation does not.

Step 1 From the View menu, choose **Go to Network View**. CTC shows the link icons by default.

Step 2 Perform one or more of the following steps as needed:

- To toggle link icons on and off, go to Step 3.
- To combine all links in network view, go to Step 4.
- To consolidate a link or links between two nodes, go to Step 5.
- To view information about a consolidated link, go to Step 6
- To access an individual link within a consolidated link, go to Step 7.
- To expand consolidated links, go to Step 8.
- To filter consolidated links by class, go to Step 9.

Step 3 Right-click on the network map and choose **Show Link Icons** to toggle the link icons on and off.

Step 4 To consolidate all the links on the network map (global consolidation):

a. Right-click anywhere on the network map.

b. Choose **Collapse/Expand Links** from the shortcut menu. The Collapse/Expand Links dialog box appears.

c. Click the check boxes for the link classes you want to consolidate.

d. Click **OK**. The selected link classes are consolidated on the network map.

Step 5 To consolidate a link or links between two nodes:

a. Right-click the link on the network map.

b. Choose **Collapse Link** from the shortcut menu. The selected link type consolidates to show only one link.

Note The links consolidate by class. For example, if you select a DCC link for consolidation only the DCC links will consolidate, leaving any other link classes expanded.

Figure 18-24 shows a network view with unconsolidated DCC and PPC links.

Figure 18-24 Unconsolidated Links in Network View

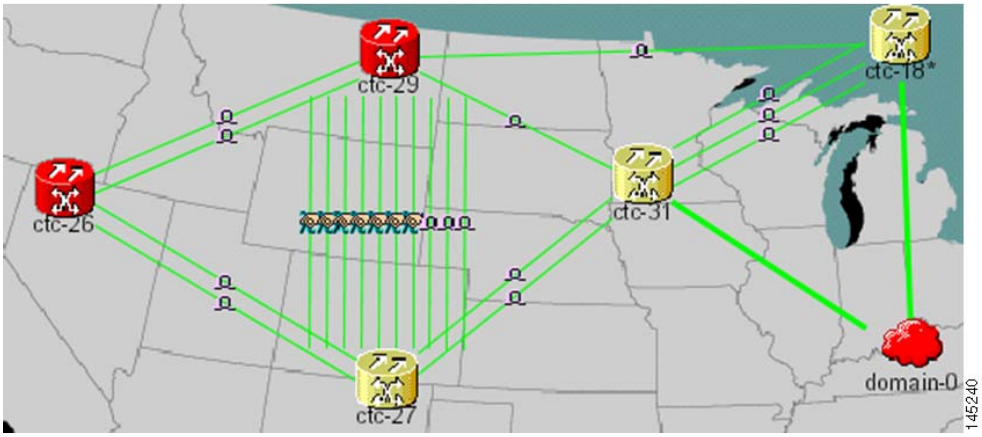


Figure 18-25 shows a network view with globally consolidated links.

Figure 18-25 Consolidated Links in Network View

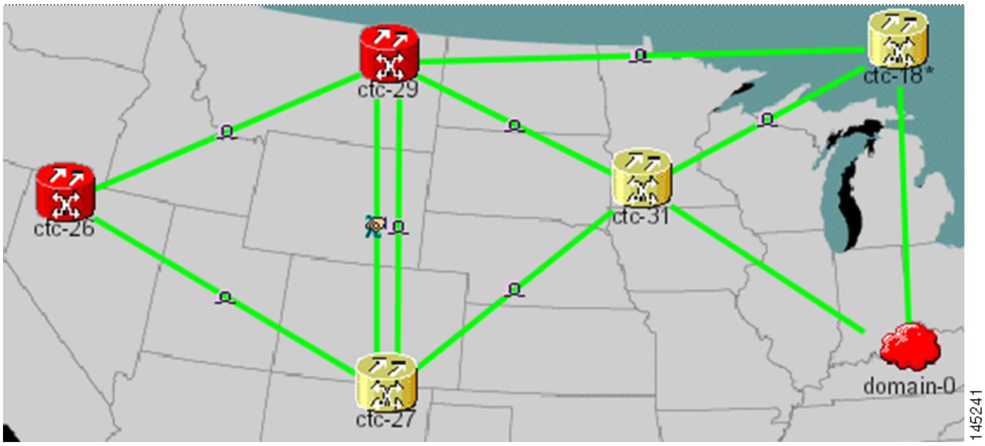
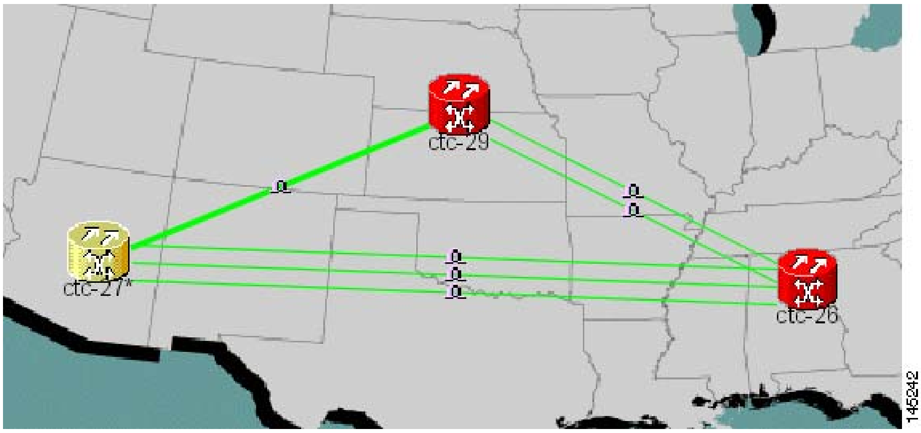


Figure 18-26 shows a different network view with local DCC link consolidation between two nodes.

Figure 18-26 Network View with Local Link Consolidation



Step 6 To view information about the consolidated link, move the mouse over the link (the tooltip displays the number of links and the link class), or click the link to display detailed information on the left side of the window.

Step 7 To access an individual link within a consolidated link (for example, if you need to perform a span upgrade):

a. Right-click the consolidated link. A shortcut menu appears with a list of the individual links.

b. Place the mouse over the selected link. A cascading menu appears where you can select an action for the individual link or navigate to one of the nodes where the link is attached.

Step 8 To expand locally consolidated links, right-click the consolidated link and choose **Expand** *[link class]* **Links** from the shortcut menu where *link class* is DCC, GCC, OTS, PPC, or Server Trail.

Step 9 To filter the links by class:

a. Click the **Link Filter** button in the upper right area of the window. The Link Filter dialog box appears.

The link classes that appear in the Link Filter are determined by the selected Network Scope (Table 18-4) located in the toolbar.

Table 18-4 Link Classes By Network Scope

Network Scope	Displayed Link Classes
ALL	DCC, GCC, OTS, PPC, Server Trail
DWDM	GCC, OTS, PPC
TDM	DCC, PPC, Server Trail

b. Check the boxes next to the links that you want to display.

c. Click **OK**.

Step 10 Return to your originating procedure (NTP).

DLP-F387 Adjust the Java Virtual Memory Heap Size

Purpose	This task allows you to adjust the Java Virtual Memory (JVM) heap size from the default 256 MB to the maximum of 512 MB in order to improve CTC performance.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Windows task bar, click **Start > Settings > Control Panel**. The Windows Control Panel appears.

Step 2 Double-click **System**. The System Properties window appears.

Step 3 Click the **Advanced** tab.

Step 4 Click **Environmental Variables**. The Environmental Variables dialog box appears.

Step 5 In the User Variables area, click **New**. The New User Variable dialog box appears.

Step 6 Type **CTC_HEAP** in the Variable Name field.

Step 7 Type **512** in the Variable Value field.

Step 8 Click **OK**.

Step 9 Reboot your PC.

Step 10 Return to your originating procedure (NTP).

DLP-F388 Install an SFP/XFP

Purpose	This task installs XFPs on the 1PIO modules and installs SFPs on the 4PIO modules (PIMs) on the ASAP card.
Tools/Equipment	SFPs/XFPs appropriate for your network
Prerequisite Procedures	DLP-F333 Install the ASAP Carrier Modules, page 18-33 DLP-F385 Install the ASAP 1PIO and 4PIO (PIM) Modules, page 18-98
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note SFPs and XFPs are generically called pluggable port modules (PPMs) in the CTC software interface.

Step 1 Verify that the SFP or XFP is correct for your network and ASAP card. Refer to the “Card Reference” chapter in the *Cisco ONS 15600 SDH Reference Manual* for more information about SFPs and XFPs.

Step 2 If you are installing an SFP, orient the SFP so that the Cisco serial number label is facing away from the shelf (to the right). If you are installing an XFP, orient the XFP to the left.

Step 3 Unlatch the bail clasp before inserting it into the slot.

Step 4 Slide the SFP or XFP into the slot on the 1PIO or 4PIO (as appropriate) and move the bail clasp to secure the SFP or XFP.

⚠ **Caution** Do not remove the protective caps until you are ready to attach the network fiber-optic cable.

Note Multirate SFPs must be provisioned in CTC; single-rate PPMs do not need to be provisioned. As needed, complete the "DLP-F358 Provision a Multirate PPM" task on page 18-70.

Step 5 Return to your originating procedure (NTP).

DLP-F389 Remove an SFP/XFP

Purpose	This task removes an XFP from a 1PIO module and removes an SFP from a 4PIO module on the ASAP card.
Tools/Equipment	None
Prerequisite Procedures	DLP-F385 Install the ASAP 1PIO and 4PIO (PIM) Modules, page 18-98
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Disconnect the network fiber cable from the SFP/XFP.

Step 2 Release the SFP/XFP from the 1PIO or 4PIO slot by unlatching the bail clasp and swinging it to the left.

Step 3 Slide the SFP/XFP out of the slot.

Step 4 As needed, complete the "DLP-F360 Delete a PPM" task on page 18-72 to delete an SFP/XFP (PPM) from CTC.

Step 5 Return to your originating procedure (NTP).

DLP-F390 Remove a 1PIO or 4PIO (PIM) Module

Purpose	This procedure explains how to remove the 1PIO or 4PIO (PIM) in the carrier modules of the ASAP card.
Tools/Equipment	#2 Phillips screwdriver
Prerequisite Procedures	DLP-F385 Install the ASAP 1PIO and 4PIO (PIM) Modules, page 18-98
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the midplane with your hand or any metal tool, or you could shock yourself.** Statement 181

Warning **Class 1 laser product.**Statement 1008

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

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

Caution Always use the supplied ESD wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-left outside edge of the shelf.

Note For information about the ASAP card, refer to the *Cisco ONS 15600 SDH Reference Manual.*

Step 1 Determine which 1PIO or 4PIO module you want to remove.

Step 2 To remove the module, use your hand to loosen and remove the screws at the top right and bottom left of the module. You can also remove the screw covers and use a Phillips screwdriver to loosen the screws so you can remove them.

Step 3 Carefully pull the module along the top and bottom guide rails and out of the correct slot.

Step 4 Log into CTC and verify that the PIM (1PIO or 4PIO) does not appear in CTC card view. See Chapter 3, "Connect the PC and Log into the GUI" for CTC information and setup instructions.

Step 5 Return to your originating procedure (NTP).

DLP-F391 Provision an Optical Line Rate and Wavelength

Purpose	This task provisions the line rate and wavelength of a multirate PPM. Single-rate SFPs and XFPs do not need line rate provisioning.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the ASAP card where you want to provision the line rate.

Step 2 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 3 In the Pluggable Ports area, click **Create**. The Create Port dialog box appears.

Step 4 In the Create Port dialog box, complete the following:

- Port—Click the PPM number and port number from the drop-down list. The first number indicates the PPM and the second number indicates the port number on the PPM. For example, the first PPM with one port displays as 1-1 and the second PPM with one port displays as 2-1. When a 4PIO or 1PIO (PIM) is present on an ASAP card, the port is identified as *PIM#-PPM#-Port#* (for example 4-4-1). The PIM number can be 1 to 4, the PPM number can be 1 to 4, but the port number is always 1.
- Port Type—Click the type of port from the drop-down list. The port type list displays the supported port rates on your PPM. See Table 18-5 for definitions of the supported rates on the ASAP card.

Table 18-5 PPM Port Types

Card	PIO (PIM)	Port Type
ASAP	4PIO	• STM-1—155 Mbps • STM-4—622 Mbps • STM-16—2.48 Gbps • ETHER—Gigabit Ethernet
	1PIO	• STM-64—9.953 Gbps

Step 5 Click **OK**.

Step 6 Click the **Provisioning > Optical > Line** tabs.

Step 7 Find the port where you want to set the wavelength frequency of the PPM.

Step 8 In the Wavelength drop-down box, select the desired frequency. See Table 18-6 on page 18-112 for definitions of the supported wavelengths on the ASAP card. The supported wavelengths depend on whether the PPM is used for dense wavelength division multiplexing (DWDM).

Step 9 Click **OK**.

Step 10 Repeat Steps 3 through 9 to configure the PPM port rates and wavelengths as needed.

Step 11 Click **OK**. The row on the Pluggable Ports area turns white.

Step 12 Return to your originating procedure (NTP).

DLP-F392 Install Alarm Wires on the CAP/CAP2

Purpose	This task installs the alarm wires on the customer access panel (CAP/CAP2).
Tools/Equipment	Wire-wrap tool (suitable for #22 to #28 AWG alarm wires) #22 to #28 AWG wires Audible alarm cable with DB-15 connector
Prerequisite Procedures	NTP-F113 Install the Bay Power and Ground, page 1-10
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Wrap the alarm wires on the appropriate wire-wrap pins according to local site practice. Figure 18-27 shows the backplane of the ONS 15600 SDH shelf and the location of the alarm pin field on the CAP/CAP2.

Figure 18-27 Rear of the ONS 15600 SDH, Including the CAP/CAP2

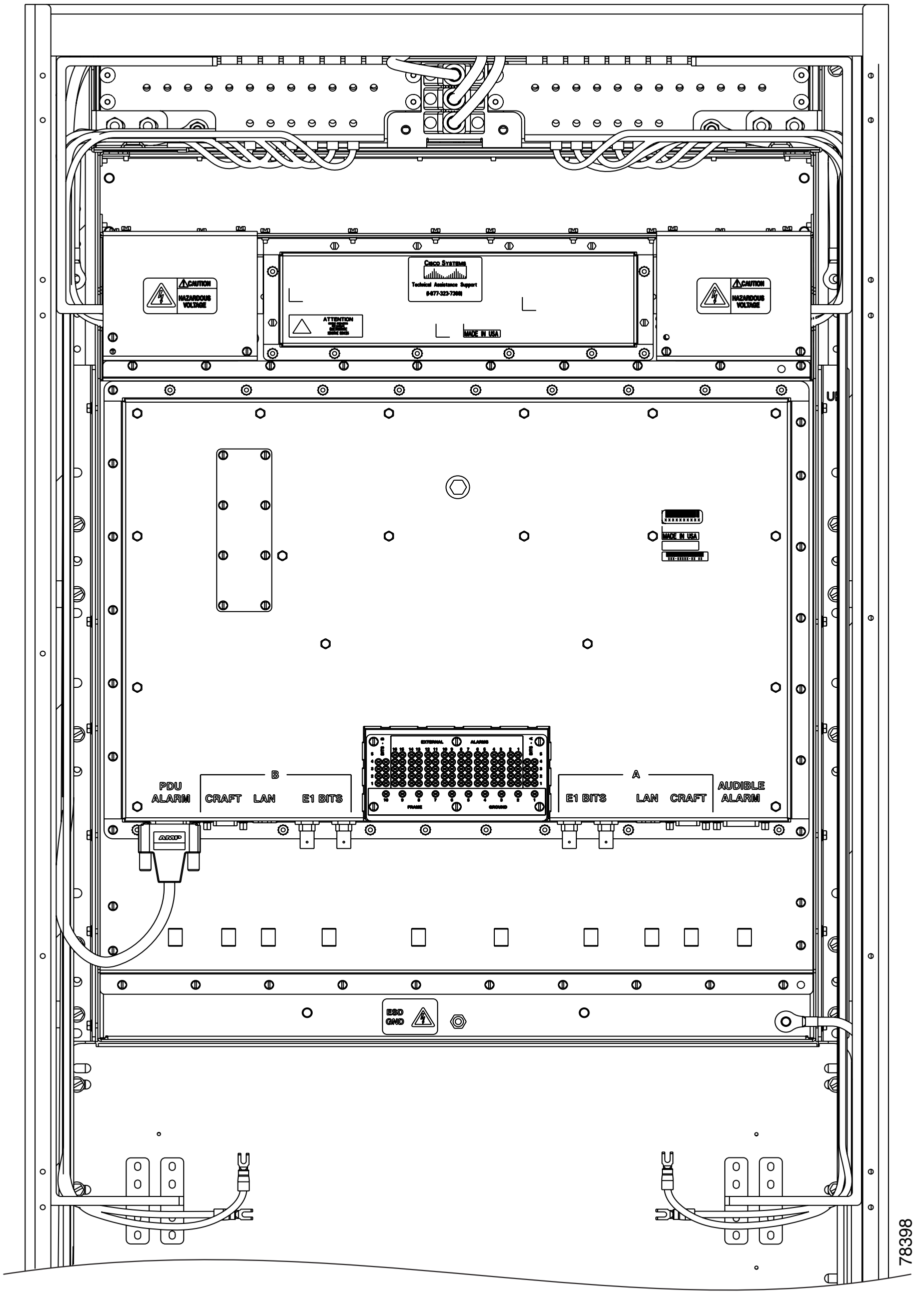


Figure 18-28 shows the CAP/CAP2 faceplate in detail.

Figure 18-28 CAP/CAP2 Faceplate and Connections

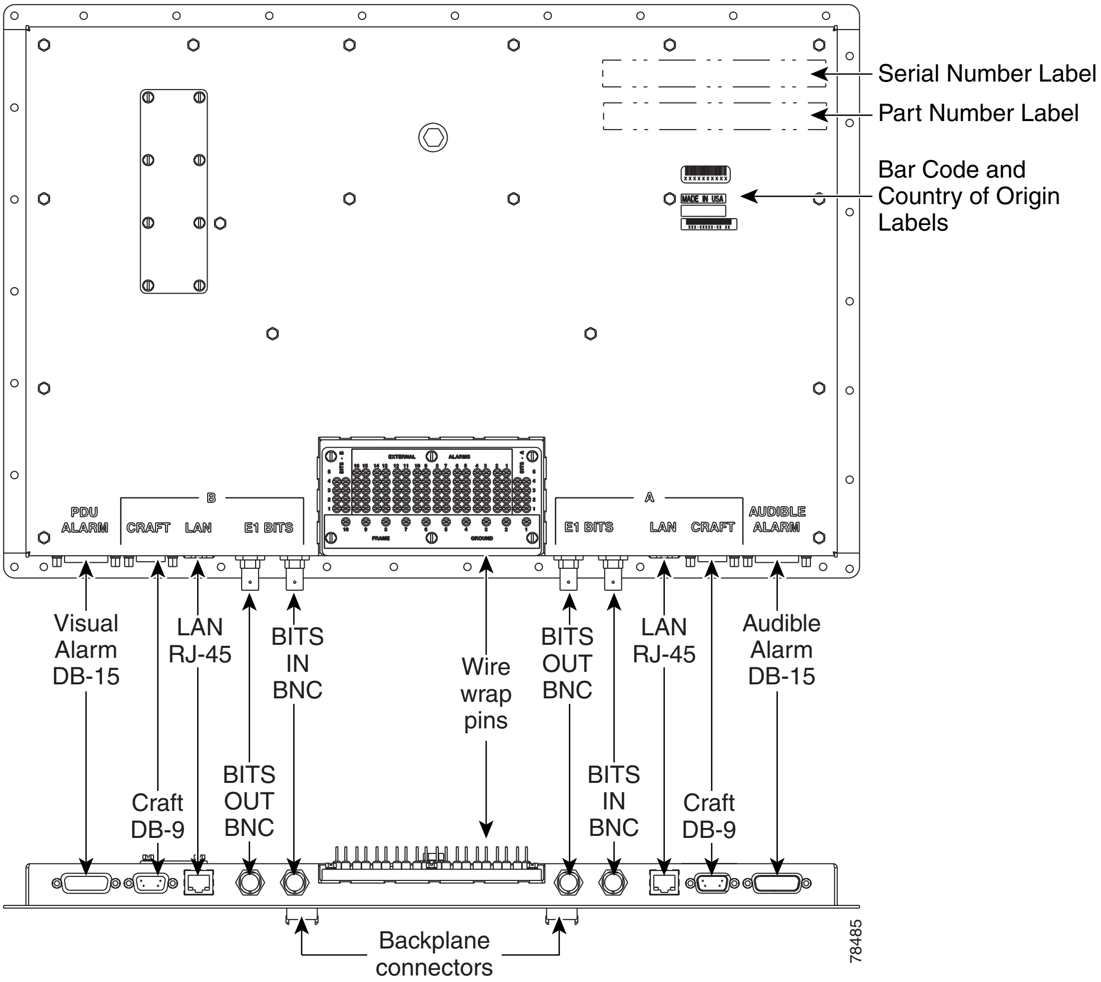
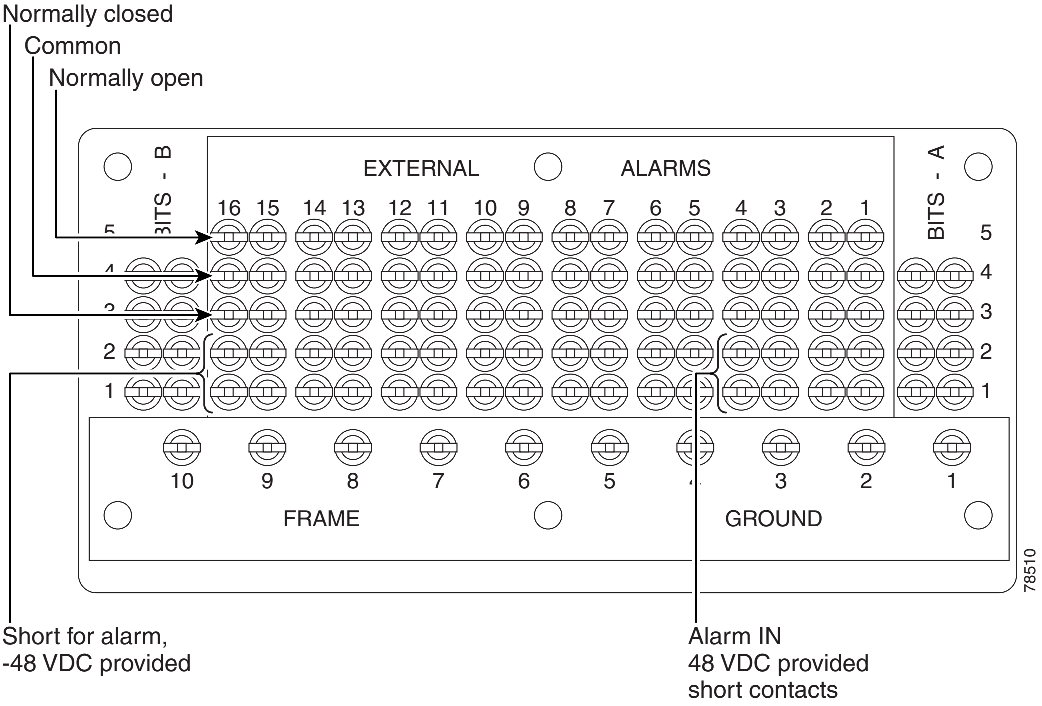


Figure 18-29 shows alarm pin assignments.

Figure 18-29 Alarm Pin Assignments on the CAP/CAP2



See Chapter 9, "Manage Alarms" for instructions about assigning alarms to these pins.

Lace or tie wrap cables to the tie wrap features that are located below the connector pattern, according to local site practice.

Step 2 To install the audible alarm cable, connect a DB-15 connector to the Audible Alarm plug at the lower right of the CAP/CAP2. Connect the other end of the cable to the appropriate audible inputs of the connecting central office alarm circuit.

Step 3 Return to your originating procedure (NTP).

DLP-F393 Change Line Transmission Settings for STM-N Cards

Purpose	This task changes line transmission settings for STM-N cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15600 SDH Reference Manual.*

Step 1 On the shelf graphic, double-click the STM-N card that you want to provision. The card view appears.

Step 2 For STM-16 or STM-64 cards, click the **Provisioning** > **Line** tabs. For the ASAP card, click the **Provisioning > Optical > Line** tabs.

Step 3 As needed, provision the options in Table 18-6 for each STM-N port. (Some options might not be available on every card.)

Table 18-6 STM-N Card Line Settings

Heading	Description	Options
Port	Identifies the port number.	• For an STM-16 card: 1–16 • For an STM-64 card: 1–4 • For an ASAP card: Up to 16 ports, denoted by either a 4PIO (PIM) or 1PIO, followed by port number or (PIM). (Example: 1-3-1 denotes the third port on 4PIO [PIM] Module 1. For a 1PIO, 3-1-1 denotes the port on 1PIO [PIM] Module 3)
Port Name	Provides the ability to assign the specified port a name.	User-defined; name can be up to 32 alphanumeric/special characters (blank by default)
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 (default) • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 (default) • 1E-8 • 1E-9
Provides Sync	(Display only) Indicates that the port has been provisioned as a network element (NE) timing reference on another node.	• Yes (checked) • No (unchecked)
Send Do Not Use	When checked, sends a do not use (DUS) message on the S1 byte	• Yes (checked) • No (unchecked; default)
MS-SPRing Ext. Byte	Chosen extended byte carries information that governs multiplex section shared protection ring (MS-SPRing) protection switches.	• K3 • Z2 • E2 • F1

Table 18-6 STM-N Card Line Settings (continued)

Heading	Description	Options
Admin State	Sets the port service state unless network conditions prevent the change.	• Unlocked—Puts the port in service. The port service state changes to Unlocked-enabled. • Unlocked,automaticInService—Puts the port in automatic in-service. The port service state changes to Unlocked-disabled,automaticInService. • Locked,disabled—Removes the port from service and disables it. The port service state changes to Locked-enabled,disabled. • Locked,maintenance—Removes the port from service for maintenance. The port service state changes to Locked-enabled,maintenance. **Note** CTC will not allow you to change a port service state from Unlocked-enabled to Locked-enabled,disabled. You must first change a port to the Locked-enabled,maintenance service state before putting it in the Locked-enabled,disabled service state.
AINS Soak	Sets the automatic in-service soak period.	Duration of valid input signal, in hh.mm format, after which the card becomes Unlocked-enabled automatically (0 to 48 hours, in 15-minute increments).
SyncMsgIn	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.	• Yes (checked; default) • No (unchecked)
Port Rate	(ASAP card only.) Displays the port rate set for the PPM.	• STM-1 • STM-4 • STM-16 • STM-64 • Ether
Type	Defines the port as SDH or SONET. Sync Msg In and Send Do Not Use must be disabled before the port can be set to SONET.	• SDH (default) • SONET

Table 18-6 STM-N Card Line Settings (continued)

Heading	Description	Options
Service State	Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• Unlocked-enabled—The port is fully operational and performing as provisioned. • Unlocked-disabled,automaticInService—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in the Unlocked-disabled,automaticInService state for the duration of the soak period. After the soak period ends, the port service state changes to Unlocked-enabled. • Locked-enabled,disabled—The port is out-of-service and unable to carry traffic. • Locked-enabled,maintenance—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
SyncStatusMsg	Allows you to view the incoming synchronization status message by clicking **Show**.	• SETS • STU • G811 • G812T • G812L • DUS_SDH (Do not use for timing synchronization)
Reach	(ASAP card only) Provisions the reach value.	(The options that appear in the drop-down list depend on the card.) • Auto Provision—Allows the system to automatically provision the reach from the PPM reach value on the hardware. • SR—Short reach, up to 2 km distance • SR-1—Up to 2 km distance • IR-1—Intermediate reach, up to 15 km distance • IR-2—Up to 40 km distance • LR-1—Long reach, up to 40 km distance) • LR-2—Up to 80 km distance • LR-3—Up to 80 km distance

Table 18-6 STM-N Card Line Settings (continued)

Heading	Description	Options
Band	(STM-64-4-DWDM card only) Sets the ITU band (in this case, C-band) for this card.	C
Wavelength	(ASAP and STM-64-4-DWDM card only) Sets the wavelength frequency (nm).	ASAP card: • First Tunable Wavelength • 1310 • 1550 • 1470 • 1490 • 1510 • 1530 • 1570 • 1590 • 1610 Dense wavelength division multiplexing (DWDM) PPMs also have the following options: • 1530.33 to 1560.61 • ITU spacing

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-F394 Change Threshold Settings for STM-N Ports

Purpose	This task changes threshold settings for STM-N ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-F129 Log into the ONS 15600 SDH GUI, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15600 SDH Reference Manual*.

Step 1 On the shelf graphic, double-click the STM-16, STM-64, or ASAP card that you want to provision. The card view appears.

Step 2 As needed, complete the following:

a. Click **Line**, **Section**, **Path,** or **Physical** to provision the line, section, path, and physical options in Table 18-7 for each STM-N port.

b. Change the selection to Near End/Far End, 15 Min/1Day as necessary.

c. Click **Refresh** to view or modify the thresholds for each selection.

Note Far End section thresholds are not available for the STM-64 card.

Table 18-7 SDH Threshold Options (Line, Section, and Path)

Heading	Description	Options
Port	Port number	1–16 for an STM-16 card, 1–4 for an STM-64 card, 1-1-1 to 4-4-1 for an ASAP port number
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals for Line, Section, or Path (Near and Far End). Select the bullet and click **Refresh**.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals for Line, Section, or Path (Near and Far End). Select the bullet and click **Refresh**. Numeric. The defaults (15 min/1 day) are:
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals for Line, Section, or Path (Near and Far End). Select the bullet and click **Refresh**.
SEFS	Severely errored framing seconds	Numeric. Can be set for 15-minute or one-day intervals for Section (Near and Far End). Select the bullet and click **Refresh**.
FC	Failure count	Numeric. Can be set for 15-minute or one-day intervals for Line or Path (Near and Far End). Select the bullet and click **Refresh**.
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals for Line or Path (Near and Far End). Select the bullet and click **Refresh**.
PSC	Protection Switching Count (Line)	Numeric. Can be set for 15-minute or one-day intervals for Line (Near End). Select the bullet and click **Refresh**.
PSD	Protection Switch Duration (Line)	Numeric. Can be set for 15-minute or one-day intervals for Line (Near End). Select the bullet and click **Refresh**.
PSC-W	Protection Switching Count (Working Line)	Numeric. Can be set for 15-minute or one-day intervals for Line (Near End). Select the bullet and click **Refresh**.

Table 18-7 SDH Threshold Options (Line, Section, and Path) (continued)

Heading	Description	Options
PSD-W	Protection Switch Duration (Working Line)	Numeric. Can be set for 15-minute or one-day intervals for Line (Near End). Select the bullet and click **Refresh**.
PSC-S	(Line) Sets the threshold for the span protection switching count. (PSC-S does not increment on STM-1 cards.)	Numeric. Can be set for 15-minute or one-day intervals for Line (Near End). Select the bullet and click **Refresh**.
PSD-S	(Line) Sets the threshold for the span protection switching duration. (PSD-S does not increment on STM-1 cards.)	Numeric. Can be set for 15-minute or one-day intervals for Line (Near End). Select the bullet and click **Refresh**.
PSC-R	(Line) Sets the threshold for the ring protection switching count. (PSC-R does not increment on STM-1 cards.)	Numeric. Can be set for 15-minute or one-day intervals for Line (Near End). Select the bullet and click **Refresh**.
PSD-R	(Line) Sets the threshold for the ring protection switching duration. (PSD-R does not increment on STM-1 cards.)	Numeric. Can be set for 15-minute or one-day intervals for Line (Near End). Select the bullet and click **Refresh**.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-F395 Change Optics Threshold Settings for STM-N Ports

Purpose	This task changes optics threshold settings for STM-N ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-F129 Log into the ONS 15600 SDH GUI, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15600 SDH Reference Manual*.

Step 1 On the shelf graphic, double-click the STM-16, STM-64, or ASAP card that you want to provision. The card view appears.

Step 2 As needed, complete the following:

a. Click **Optics Thresholds** to provision the options in Table 18-8 for each STM-N port.

b. Select the **TCA** (threshold crossing alert) or **Alarm** radio button.

c. Select a **15 Min** or **1 Day** performance monitoring interval radio button (available for TCA only), and then click **Refresh**.

d. Click **Refresh** to view or modify the thresholds for each selection.

Table 18-8 Optics Threshold Options

Heading	Description	Options
Port	Port number	1–16 for an STM-16 card, 1–4 for an STM-64 card, 1-1-1 to 4-4-1 for an ASAP port number
LBC-HIGH	Laser bias current–maximum. Maximum threshold for LBC.	Numeric percentage of the baseline value
LBC-LOW	Laser bias current–minimum. Minimum threshold for LBC.	Numeric percentage of the baseline value
OPT-HIGH	Optical power transmitted–maximum. Maximum threshold for OPT.	Numeric percentage of the baseline value
OPT-LOW	Optical power transmitted–minimum. Minimum threshold for OPT.	Numeric percentage of the baseline value
OPR-HIGH	Optical power received–maximum. Maximum threshold for OPR.	Numeric percentage of the baseline value
OPR-LOW	Optical power received–minimum. Minimum threshold for OPR.	Numeric percentage of the baseline value
Set OPR	Setting the optical power received (OPR) establishes the received power level as 100 percent. If the receiver power decreases, then the OPR percentage decreases to reflect the loss in receiver power. For example, if the receiver power decreases 3 dBm, the OPR decreases 50 percent.	Click **Set**.
Types	Sets the threshold values of alerts that trigger an alarm or TCA response. To view the provisionable thresholds that generate an Alarm or TCA, choose the type and click **Refresh**.	• TCA (threshold crossing alert) • Alarm
Intervals	Sets the time interval for collecting parameter counts. To change the time interval, choose an interval and click **Refresh**.	• 15 Min • 1 Day

Step 3 Click **Apply**.

Note See Chapter 9, "Manage Alarms" for information about the Alarm Behavior tab, including alarm profiles and alarm suppression.

DLP-F396 Change the STM-N Port ALS Maintenance Settings

Purpose	This task changes the automatic laser shutdown (ALS) maintenance settings for the STM-N ports. This feature is available for STM-16, STM-64, and ASAP cards.
Tools/Equipment	None
Prerequisite Procedures	NTP-F129 Log into the ONS 15600 SDH GUI, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For the default values and domains of user-provisionable card settings, refer to the “Network Element Defaults” appendix in the *Cisco ONS 15600 SDH Reference Manual*.

Step 1 In node view, double-click the STM-16, STM-64, or ASAP card where you want to change the ALS maintenance settings.

Step 2 Click the **Maintenance > ALS** tabs.

Step 3 Modify any of the settings described in Table 18-9 by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value or select and deselect a check box. The provisionable parameters are listed in the options column in the table.

Step 4 Click **Apply**. If the change affects traffic, a warning message appears. Click **Yes** to complete the change.

Table 18-9 STM-N Maintenance Settings

Parameter	Description	Options
Port number	(Display only) Port number	—
ALS Mode	Automatic laser shutdown mode. ALS provides the ability to shut down the TX laser when the RX detects a loss of signal (LOS).	From the drop-down list, choose one of the following: • Disable—Deactivates ALS. • Auto Restart—(Default) ALS is active. The power is automatically shut down when needed and the laser automatically tries to restart using a probe pulse until the cause of the failure is repaired. • Manual Restart—ALS is active, but the laser must be manually restarted when conditions that caused the outage are resolved. • Manual Restart for Test—Manually restarts the laser for testing.

Table 18-9 STM-N Maintenance Settings (continued)

Parameter	Description	Options
Recovery Pulse Duration	Sets the recovery laser pulse duration, in seconds, for the initial, recovery optical power pulse following a laser shutdown.	Numeric. For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15600 SDH Reference Manual*.
Recovery Pulse Interval	Sets the recovery laser pulse interval, in seconds. This is the period of time that must past before the recover pulse is repeated.	Numeric. For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15600 SDH Reference Manual*.
Currently Shutdown	(Display only) Displays the current status of the laser.	Numeric. For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15600 SDH Reference Manual*.
Request Laser Restart	If checked, allows you to restart the laser for maintenance. **Note** Restarting a laser might be traffic-affecting.	Checked or unchecked

Step 5 Return to your originating procedure (NTP).

DLP-F397 Clear All PM Thresholds

Purpose	This task clears and resets all PM thresholds to the default values.
Tools/Equipment	None
Prerequisite Procedures	NTP-F129 Log into the ONS 15600 SDH GUI, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

⚠ **Caution** Pressing the Reset button can mask problems if used incorrectly. This button is commonly used for testing purposes.

Step 1 In node view, double-click the card where you want to view PM thresholds. The card view appears.

Step 2 Click the **Provisioning** > **Threshold** tabs. The subtab names vary depending on the card selected.

Step 3 Click **Reset to Default**.

Step 4 Click **Yes** in the Reset to default dialog box.

Step 5 Verify that the PM thresholds have been reset.

Step 6 Return to your originating procedure (NTP).

DLP-F398 Provision the Designated SOCKS Servers

Purpose	This task identifies the ONS 15600 SDH SOCKS servers in SOCKS-proxy-enabled networks. Identifying the SOCKS servers reduces the amount of time required to log into a node and have all NEs appear in network view (NE discovery time). The task is recommended when the combined CTC login and NE discovery time is greater than five minutes in networks with SOCKS proxy enabled. Long (or failed) login and NE discovery times can occur in networks that have a high ENE-to-GNE ratio and a low number of ENEs with LAN connectivity.
Tools/Equipment	None
Prerequisite Procedures	NTP-F129 Log into the ONS 15600 SDH GUI, page 3-5
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note To complete this task, you must have either the IP addresses or DNS names of all ONS 15454s in the network with LAN access that have SOCKS proxy enabled.

Note SOCKS proxy servers can be any accessible ONS network nodes that have LAN access, including the ONS 15310-MA, ONS 15310-CL,ONS 15327, ONS 15454, ONS 15454 SDH, ONS 15600, and ONS 15600 SDH nodes.

Note You must repeat this task any time that changes to SOCKS proxy server nodes occur, for example, whenever LAN connectivity is added to or removed from a node, or when nodes are added or removed from the network.

Note If you cannot log into a network node, complete the "DLP-F181 Log into CTC" task on page 16-34 choosing the Disable Network Discovery option. Complete this task, then login again with network discovery enabled.

Step 1 From the CTC Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **SOCKS** tab.

Step 3 In the Designated SOCKS Server field, type the IP address or DNS node name of the first ONS 15600 SDH SOCKS server. The ONS 15600 SDH that you enter must have SOCKS proxy server enabled, and it must have LAN access.

Step 4 Click **Add**. The node is added to the SOCKS server list. If you need to remove a node on the list, click **Remove**.

Step 5 Repeat Steps 3 and 4 to add all qualified ONS 15600 SDH nodes within the network. All ONS nodes that have SOCKS proxy enabled and are connected to the LAN should be added.

Step 6 Click **Check All Servers**. A check is conducted to verify that all nodes can perform as SOCKS servers. If so, a check is placed next to the node IP address or node name in the SOCKS server list. An X placed next to the node indicates one or more of the following:

- The entry does not correspond to a valid DNS name.
- The numeric IP address is invalid.
- The node cannot be reached.
- The node can be reached, but the SOCKS port cannot be accessed, for example, a firewall problem might exist.

Step 7 Click **Apply**. The list of ONS 15600 SDH nodes, including ones that received an X in Step 6, are added as SOCKS servers.

Step 8 Click **OK** to close the Preferences dialog box.

Step 9 Return to your originating procedure (NTP).

DLP-F399 Install the CTC Launcher Application from a Release 8.0 Software CD

Purpose	This task installs the CTC Launcher from a Release 8.0 software CD.
Tools/Equipment	None
Prerequisite Procedures	NTP-F129 Log into the ONS 15600 SDH GUI, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Insert the Cisco ONS 15454, Cisco ONS 15454 SDH, Cisco ONS 15310-CL, Cisco ONS 15310-MA, or Cisco ONS 15600 Software Release 8.0 CD into your CD drive.

Step 2 Navigate to the CtcLauncher directory.

Step 3 Save the StartCTC.exe file to a local hard drive.

Step 4 Return to your originating procedure (NTP).

DLP-F400 Install the CTC Launcher Application from a Release 8.0 Node

Purpose	This task installs the CTC Launcher from an ONS 15454 node running Software R8.0
Tools/Equipment	None
Prerequisite Procedures	NTP-F129 Log into the ONS 15600 SDH GUI, page 3-5

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

Step 1 Using a web browser, go to the following address, where node name is the DNS name of a node you are going to access:

```
http://<node-name>/fs/StartCTC.exe
```

The browser File Download window opens.

Step 2 Click **Save** and navigate to the location where you want to save the StartCTC.exe file to a local hard drive.

Step 3 Click **Save**.

Step 4 Return to your originating procedure (NTP).

CHAPTER 19

DLPs F401 to F499

DLP-F401 Connect to ONS Nodes Using the CTC Launcher

Purpose	This task connects the CTC Launcher to ONS nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Start the CTC Launcher:

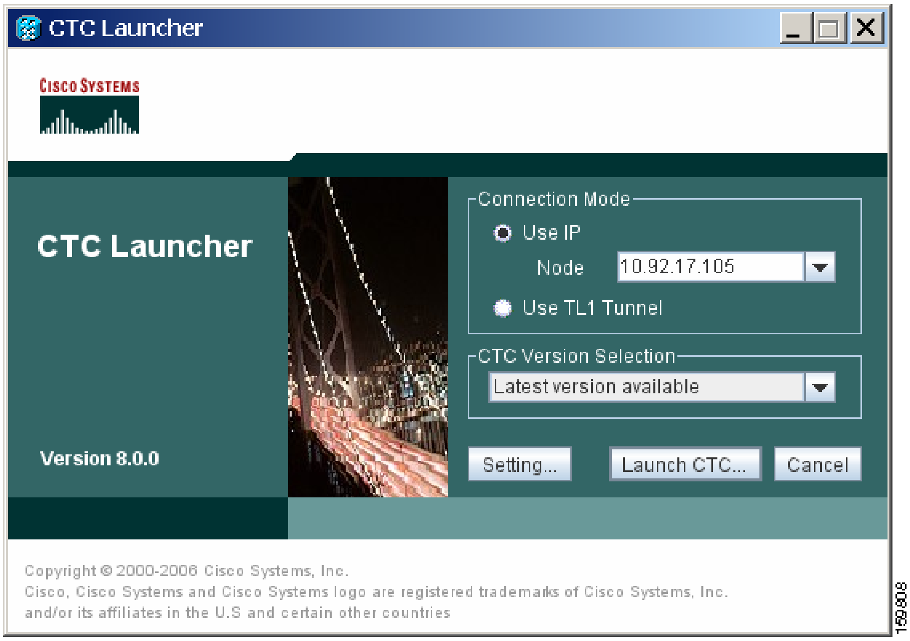
- Windows: navigate to the directory containing the StartCTC.exe file and double-click it. (You can also use the Windows Start menu Run command.)
- Solaris: assuming the StartCTC.exe file is accessible from the current shell path, navigate to the directory containing the StartCTC.exe file and type:

```
% java -jar StartCTC.exe
```

Step 2 In the CTC Launcher dialog box, choose **Use IP**.

Figure 19-1 shows the CTC Launcher window.

Figure 19-1 CTC Launcher Window



Connection Mode

● Use IP

Node 10.92.17.105

○ Use TL1 Tunnel

CTC Version Selection

Latest version available

Copyright © 2000-2006 Cisco Systems, Inc.
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc.
and/or its affiliates in the U.S and certain other countries

Step 3 In the Login Node box, enter the ONS NE node name or IP address. (If the address was entered previously, you can choose it from the drop-down menu.)

Step 4 Select the CTC version you want to launch from the following choices in the drop-down menu:

- Same version as the login node: Select if you want to launch the same CTC version as the login node version, even if more recent versions of CTC are available in the cache.
- Latest version available: Select if you want to launch the latest CTC version available. If the cache has a newer CTC version than the login node, that CTC version will be used. Otherwise the same CTC version as the login node will be used.
- Version x.xx: Select if you want to launch a specific CTC version.

Note Cisco recommends that you always use the "Same version as the login node" unless the use of newer CTC versions is needed (for example, when CTC must manage a network containing mixed version NEs).

Step 5 Click **Launch CTC**. After the connection is made, the CTC Login dialog box appears.

Step 6 Log into the ONS node.

Note Because each CTC version requires particular JRE versions, the CTC Launcher will prompt the user for the location of a suitable JRE whenever a new CTC version is launched for the first time using a file chooser dialog (if a suitable JRE version is not known by the launcher yet). That JRE information is then saved in the user's preferences file. From the selection dialog, select any appropriate JRE directory.

After the JRE version is selected, the CTC will be launched. The required jar files will be downloaded into the new cache if they are missing. The CTC Login window will appear after a few seconds.

Step 7 Return to your originating procedure (NTP).

DLP-F402 Create a TL1 Tunnel Using the CTC Launcher

Purpose	This task creates a TL1 tunnel using the CTC Launcher, and the tunnel transports the TCP traffic to and from ONS ENEs through the OSI-based GNE.
Tools/Equipment	None
Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Double-click the StartCTC.exe file.

Step 2 Click **Use TL1 Tunnel**.

Step 3 In the Open CTC TL1 Tunnel dialog box, enter the following:

- Far End TID—Enter the TID of the ONS ENE at the far end of the tunnel. The TID is the name entered in the Node Name field on the node view Provisioning > General tab.
- Host Name/IP Address—Enter the GNE DNS host name or IP address through which the tunnel will established. This is the third-party vendor GNE that is connected to an ONS node through an OSI DCC network. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.
- Choose a port option:
  - Use Default TL1 Port—Choose this option if you want to use the default TL1 port 3081 and 3082.
  - Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
- TL1 Encoding Mode—Choose the TL1 encoding:
  - LV + Binary Payload— TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient encoding mode. However, you must verify that the GNE supports LV + Binary Payload encoding.
  - LV + Base64 Payload— TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
  - Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
- GNE Login Required—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
- TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 4 Click **OK**.

Step 5 If the GNE Login Required box is checked, complete the following steps. If not, continue Step 6.

a. In the Login to Gateway NE dialog box UID field, enter the TL1 user name.

b. In the PID field, enter the TL1 user password.

c. Click **OK**.

Step 6 When the CTC Login dialog box appears, complete the CTC login.

Step 7 Return to your originating procedure (NTP).

DLP-F403 Create a TL1 Tunnel Using CTC

Purpose	This task creates a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 2 In the TL1 Tunnels window, click **Create**.

Step 3 In the Create CTC TL1 Tunnel dialog box, enter the following:

- Far End TID—Enter the TID of the ONS ENE at the far end of the tunnel. The ENE must be a Cisco ONS NE. The TID is the name entered in the Node Name field on the node view Provisioning > General tab.
- Host Name/IP Address—Enter the GNE DNS host name or IP address through which the tunnel will established. This is the third-party vendor GNE that is connected to an ONS NE with an OSI DCC. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.
- Choose a port option:
  - Use Default TL1 Port—Choose this option if you want to use the GNE default TL1 port. TL1 uses standard ports, such as 3081 and 3082, unless custom TL1 ports are defined.
  - Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
- TL1 Encoding Mode—Choose the TL1 encoding:
  - LV + Binary Payload— TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient. However, you must verify that the GNE supports LV + Binary Payload encoding.
  - LV + Base64 Payload— TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
  - Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.

- GNE Login Required—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
- TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 4 Click **OK**.

Step 5 If the GNE Login Required box is checked, complete the following steps. If not, continue Step 6.

a. In the Login to Gateway NE dialog box UID field, enter the TL1 user name.

b. In the PID field, enter the TL1 user password.

c. Click **OK**.

Step 6 After the CTC Login dialog box appears, log into CTC.

Step 7 Return to your originating procedure (NTP).

DLP-F404 View TL1 Tunnel Information

Purpose	This task views a TL1 tunnel created using the CTC Launcher.
Tools/Equipment	None
Prerequisite Procedures	NTP-F126 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Log into CTC.

Step 2 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 3 In the TL1 Tunnels window, view the information shown in Table 19-1.

Table 19-1 TL1 Tunnels Window

Item	Description
Far End TID	The Target ID of the NE at the far end of the tunnel. This NE is an ONS NE. It is typically connected with an OSI DCC to a third-party vender GNE. CTC manages this NE.
GNE Host	The GNE host or IP address through which the tunnel is established. This is generally a third-party vendor GNE that is connected to an ONS NE with an OSI DCC. CTC uses TCP/IP over a DCN to reach the GNE. The GNE accepts TL1 connections from the network and can forward TL1 traffic to the ENEs.
Port	The TCP port number where the GNE accepts TL1 connections coming from the DCN. These port numbers are standard (such as 3081 and 3082) unless custom port numbers are provisioned on the GNE.

Table 19-1 TL1 Tunnels Window (continued)

Item	Description
TL1 Encoding	Defines the TL1 encoding used for the tunnel: • LV + Binary Payload— TL1 messages are delimited by an LV (length value) header. TCP traffic is encapsulated in binary form. • LV + Base64 Payload— TL1 messages are delimited by an LV header. TCP traffic is encapsulated using the base 64 encoding. • Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
GNE TID	The GNE TID is shown when the GNE requires a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs. If present, CTC asks the user for the ACT-USER user ID and password when the tunnel is opened.
State	Indicates the tunnel state: OPEN—A tunnel is currently open and carrying TCP traffic. RETRY PENDING—The TL1 connection carrying the tunnel has been disconnected and a retry to reconnect it is pending. (CTC automatically attempts to reconnect the tunnel at regular intervals. During that time all ENEs behind the tunnel are unreachable.) (empty)—No tunnel is currently open.
Far End IP	The IP address of the ONS NE that is at the far end of the TL1 tunnel. This information is retrieved from the NE when the tunnel is established.
Sockets	The number of active TCP sockets that are multiplexed in the tunnel. This information is automatically updated in real time.
Retries	Indicates the number of times CTC tried to reopen a tunnel. If a network problem causes a tunnel to go down, CTC automatically tries to reopen it at regular intervals. This information is automatically updated in real time.
Rx Bytes	Shows the number of bytes of management traffic that were received over the tunnel. This information is automatically updated in real time.
Tx Bytes	Shows the number of bytes of management traffic that were transmitted over the tunnel. This information is automatically updated in real time.

Step 4 Return to your originating procedure (NTP).

DLP-F405 Edit a TL1 Tunnel Using CTC

Purpose	This task edits a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 2 In the TL1 Tunnels window, click the tunnel you want to edit.

Step 3 Click **Edit**.

Step 4 In the Edit CTC TL1 Tunnel dialog box, edit the following:

- Use Default TL1 Port—Choose this option if you want to use the GNE default TL1 port. TL1 uses standard ports, such as 3081 and 3082, unless custom TL1 ports are defined.
- Use Other TL1 Port—Choose this option if the GNE uses a different TL1 port. Enter the port number in the box next to the User Other TL1 Port radio button.
- TL1 Encoding Mode—Choose the TL1 encoding:
  - LV + Binary Payload— TL1 messages are delimited by LV (length value) headers and TCP traffic is encapsulated in binary form. Cisco recommends this option because it is the most efficient. However, you must verify that the GNE supports LV + Binary Payload encoding.
  - LV + Base64 Payload— TL1 messages are delimited by LV headers and TCP traffic is encapsulated using Base64 encoding.
  - Raw—TL1 messages are delimited by semi-columns only, and the TCP traffic is encapsulated using Base64 encoding.
- GNE Login Required—Check this box if the GNE requires a a local TL1 ACT-USER login before forwarding TL1 traffic to ENEs.
- TID—If the GNE Login Required box is checked, enter the GNE TID.

Step 5 Click **OK**.

Step 6 If the GNE Login Required box is checked, complete login in the Login to Gateway NE dialog box. If not, continue Step 6.

a. In the UID field, enter the TL1 user name.

b. In the PID field, enter the TL1 user password.

c. Click **OK**.

Step 7 When the CTC Login dialog box appears, complete the CTC login. Refer to login procedures in the user documentation for the ONS ENE.

Step 8 Return to your originating procedure (NTP).

DLP-F406 Delete a TL1 Tunnel Using CTC

Purpose	This task deletes a TL1 tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Tools menu, choose **Manage TL1 Tunnels**.

Step 2 In the TL1 Tunnels window, click the tunnel you want to delete.

Step 3 Click **Delete**.

Step 4 In the confirmation dialog box, click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-F407 Create an SNMPv3 User

Purpose	This procedure creates an SNMPv3 user.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **SNMP > SNMP V3 > User** tabs.

Step 2 Click **Create**.

Step 3 In the Create User dialog box, enter the following information:

- User Name—Specify the name of the user on the host that connects to the agent. The user name must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters.
- Group Name—Specify the group to which the user belongs.
- Authentication
  - Protocol—Select the authentication algorithm that you want to use. The options are NONE, MD5, and SHA.
  - Password—Enter a password if you select MD5 or SHA. By default, the password length is set to a minimum of eight characters.
- Privacy—Initiates a privacy authentication level setting session that enables the host to encrypt the contents of the message that is sent to the agent.
  - Protocol—Select NONE or DES as the privacy authentication algorithm.
  - Password—Enter a password if you select DES.

Step 4 Click **OK** to save the information.

Step 5 Return to your originating procedure (NTP).

DLP-F408 Create MIB Views

Purpose	This procedure creates an SNMPv3 MIB view.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **SNMP** > **SNMP V3** > **MIB views** tabs.

Step 2 Click **Create**.

Step 3 In the Create Views dialog box, enter the following information:

- Name—Name of the view.
- Subtree OID—The MIB subtree which, when combined with the mask, defines the family of subtrees.
- Bit Mask—A family of view subtrees. Each bit in the bit mask corresponds to a sub-identifier of the subtree OID.
- Type—Select the view type. Options are Include and Exclude. Type defines whether the family of subtrees that are defined by the subtree OID and the bit mask combination are included or excluded from the notification filter.

Step 4 Click **OK** to save the information.

Step 5 Return to your originating procedure (NTP).

DLP-F409 Create Group Access

Purpose	This procedure creates a user group and configures the access parameters for the users in the group.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **SNMP** > **SNMP V3** > **Group Access** tabs.

Step 2 Click **Create**.

Step 3 In the Create Group Access dialog box, enter the following information:

- Group Name—The name of the SNMP group, or collection of users, who share a common access policy.

- Security Level—The security level for which the access parameters are defined. Select from the following options:
  - noAuthNoPriv—Uses a user name match for authentication.
  - AuthNoPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
  - AuthPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption based on the CBC-DES (DES-56) standard, in addition to authentication.

  If you select authNoPriv or authPriv for a group, the corresponding user must be configured with an authentication protocol and password, with privacy protocol and password, or both.
- Views
  - Read View Name—Read view name for the group.
  - Notify View Name—Notify view name for the group.
- Allow SNMP Sets—Select this check box if you want the SNMP agent to accept SNMP SET requests. If this check box is not selected, SET requests are rejected.

Note SNMP SET request access is implemented for very few objects.

Step 4 Click **OK** to save the information.

Step 5 Return to your originating procedure (NTP).

DLP-F410 Configure SNMPv3 Trap Destination

Purpose	This procedure provisions SNMPv3 trap destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **SNMP > SNMP V3 > Trap Destinations (V3)** tabs.

Step 2 Click **Create**.

Step 3 In the Configure SNMPv3 Trap dialog box, enter the following information:

- Target Address—Target to which the traps should be sent. Use an IPv4 or an IPv6 address.
- UDP Port—UDP port number that the host uses. Default value is 162.
- User Name—Specify the name of the user on the host that connects to the agent.
- Security Level—Select one of the following options:
  - noAuthNoPriv—Uses a user name match for authentication.
  - AuthNoPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.

  - AuthPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption based on the CBC-DES (DES-56) standard, in addition to authentication.

- Filter Profile—Select this check box and enter the filter profile name. Traps are sent only if you provide a filter profile name and create a notification filter. This field is optional and traps can also be sent without providing a filter profile and create a notification filter. For more information, see "DLP-F412 Create Notification Filters" task on page 19-12.
- Proxy Traps Only—If selected, forwards only proxy traps from the ENE. Traps from this node are not sent to the trap destination identified by this entry.
- Proxy Tags—Specify a list of tags. The tag list is needed on a GNE only if an ENE needs to send traps to the trap destination identified by this entry, and wants to use the GNE as the proxy.

Step 4 Click **OK** to save the information.

Step 5 Return to your originating procedure (NTP).

DLP-F411 Delete SNMPv3 Trap Destination

Purpose	This procedure deletes an SNMPv3 trap destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > SNMP> SNMPv3 > Trap Destination** tabs.

Step 2 In the Trap Destinations area, select the trap destination you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-F412 Create Notification Filters

Purpose	This procedure creates SNMPv3 notification filters. The notification filters are used to filter the notifications or traps, which should or should not be transmitted to the management target.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **SNMP** > **SNMP V3** > **Notification Filters** tabs.

Step 2 Click **Create**.

Step 3 In the Create Notify dialog box, enter the following information:

- Filter Profile Name—Specify a name for the filter.
- Subtree OID—The MIB subtree which, when combined with the mask, defines the family of subtrees.
- Bit Mask—A family of view subtrees. Each bit in the bit mask corresponds to a sub-identifier of the subtree OID.
- View Type—Select the view type. Options are Include and Exclude. Type defines whether the family of subtrees that are defined by the subtree OID and the bit mask combination are included or excluded from the notification filter.

Step 4 Click **OK** to save the information.

Step 5 Return to your originating procedure (NTP).

DLP-F413 Manually Configure the SNMPv3 Proxy Forwarder Table

Purpose	This procedure creates an entry in the SNMPv3 Proxy Forwarder Table.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In network view, click **Provisioning** > **SNMPv3**.

Step 2 In the SNMPv3 Proxy Server area, complete the following:

- Select the GNE to be used as the SNMPv3 proxy server from the drop-down list.
- Select the **Enable IPv6 Target/Trap** check box if the nodes and the NMS stations are on an IPv6 network.

Step 3 In the SNMPv3 Proxy Forwarder Table area, click **Manual Create**.

Step 4 In the Manual Configuration of SNMPv3 Proxy Forwarder dialog box, enter the following information:

- Target IP Address—Target to which the request should be forwarded. Use an IPv4 or an IPv6 address.
- Context Engine ID—The context engine ID of the ENE to which the request is to be forwarded. The context engine ID should be the same as the context engine ID of the incoming request.
- Proxy Type—Type of SNMP request that needs to be forwarded. The options are Read and Write.
- Local User Details—The details of the local user who proxies on behalf of the ENE user.
  - User Name—Specify the name of the user on the host that connects to the agent.
  - Local Security Level—Select the security level of the incoming requests that are to be forwarded. The options are noAuthNoPriv, AuthNoPriv, and AuthPriv.
- Remote User Details—User to which the request is forwarded.
  - User Name—Specify the user name of the remote user.
  - Remote Security Level—Select the security level of the outgoing requests. The options are noAuthNoPriv, AuthNoPriv, and AuthPriv.
- Authentication
  - Protocol—Select the authentication algorithm you want to use. The options are NONE, MD5, and SHA.
  - Password—Enter the password if you select MD5 or SHA.
- Privacy—Enables the host to encrypt the contents of the message that is sent to the agent.
  - Protocol—Select NONE or DES as the privacy authentication algorithm.
  - Password—Enter the password if you select DES. The password should not exceed 64 characters.

Step 5 Click **OK** to save the information.

Step 6 Return to your originating procedure (NTP).

DLP-F414 Automatically Configure the SNMPv3 Proxy Forwarder Table

Purpose	This procedure creates an entry in the SNMPv3 Proxy Forwarder Table.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In network view, click **Provisioning > SNMPv3** tabs.

Step 2 In the SNMPv3 Proxy Server area, complete the following:

- Select the GNE to be used as the SNMPv3 proxy server from the drop-down list.

- Select the **Enable IPv6 Target/Trap** check box if the nodes and the NMS stations are on an IPv6 network.

Step 3 In the SNMPv3 Proxy Forwarder Table area, click **Auto Create**.

Step 4 In the Automatic Configuration of SNMPv3 Proxy Forwarder dialog box, enter the following information:

- Proxy Type—Select the type of proxies to be forwarded. The options are Read and Write.
- Security Level—Select the security level for the incoming requests that are to be forwarded. The options are:
  - noAuthNoPriv—Uses a username match for authentication.
  - AuthNoPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
  - AuthPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption based on the CBC-DES (DES-56) standard, in addition to authentication.
- Target Address List—Select the proxy destination.
- Local User Name—Select the user name from the list of users.

Note When you configure SNMPv3 Proxy Forwarder Table automatically, the default_group is used on the ENE. The default_group does not have write access. To enable write access and allow SNMP sets, you need to edit the default_group on ENE.

Step 5 Click **OK** to save the settings.

Step 6 Return to your originating procedure (NTP).

DLP-F415 Manually Configure the SNMPv3 Proxy Trap Forwarder Table

Purpose	This procedure creates an entry in the SNMPv3 Proxy Trap Forwarder Table.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In network view, click **Provisioning > SNMPv3** tabs.

Step 2 In the SNMPv3 Proxy Server area, complete the following:

- Select the GNE to be used as the SNMPv3 proxy server from the drop-down list.
- Select the **Enable IPv6 Target/Trap** check box if the nodes and the NMS stations are on an IPv6 network.

Step 3 In the SNMPv3 Proxy Trap Forwarder Table area, click **Manual Create**.

Step 4 In the Manual Configuration of SNMPv3 Proxy Trap Forwarder dialog box, enter the following information:

- Remote Trap Source—Select the IP address from which the traps are sent. If the IP address is not listed, enter the IP address manually.
- Context Engine ID—Specify the context engine ID of the ENE from which traps need to be forwarded. This field is automatically populated if the source of trap is selected. If the source of trap is not specified, you need to manually enter the context engine ID.
- Target Tag—Specify the tag name. The tag identifies the list of NMS that should receive the forwarded traps. Traps are forwarded to all GNE Trap destinations whose proxy tags list contains this tag.
- Remote User Details
  - User Name—Specify the user name.
  - Security Level—Select the security level for the user. The options are noAuthNoPriv, AuthNoPriv, and AuthPriv.
- Authentication—Select the authentication algorithm.
  - Protocol—Select the authentication algorithm you want to use. The options are NONE, MD5, and SHA. Default is None.
  - Password—Enter the password if you select MD5 or SHA.
- Privacy—Enables the host to encrypt the contents of the message that is sent to the agent.
  - Protocol—Select NONE or DES as the privacy authentication algorithm. Encryption is disabled if NONE is selected.
  - Password—Enter the password if you select DES. The password should not exceed 64 characters.

Step 5 Click **OK** to save the information.

Step 6 Return to your originating procedure (NTP).

DLP-F416 Automatically Configure the SNMPv3 Proxy Trap Forwarder Table

Purpose	This procedure creates an entry in the SNMPv3 Proxy Trap Forwarder Table automatically.
Tools/Equipment	None
Prerequisite Procedures	DLP-F181 Log into CTC, page 16-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In network view, click **Provisioning > SNMPv3** tabs.

Step 2 In the SNMPv3 Proxy Server area, complete the following:

- Select the GNE to be used as the SNMPv3 proxy server from the drop-down list.

- Select the Enable IPv6 Target/Trap check box if the nodes and the NMS stations are on an IPv6 network.

Step 3 In the **SNMPv3 Proxy Trap Forwarder Table** area, click **Auto Create**.

Step 4 In the Automatic Configuration of SNMPv3 Proxy Trap Forwarder dialog box, enter the following information:

- Target Tag—Specify the tag name. The tag identifies the list of NMS that should receive the forwarded traps. All GNE Trap destinations that have this tag in their proxy tags list are chosen.
- Source of Trap—The list of ENEs whose traps are forwarded to the SNMPv3 Trap destinations that are identified by the Target Tag.

Step 5 Click **OK** to save the information.

Step 6 Return to your originating procedure (NTP).

APPENDIX A

CTC Information and Shortcuts

This appendix describes how to navigate in the Cisco Transport Controller (CTC) and change CTC table data. It also describes menu and tool options and the shelf inventory data presented in CTC. For information about CTC, refer to the "Cisco Transport Controller Operation" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Note If network discovery is enabled on the node, CTC searches each node in the network for more recent versions of the CTC software. If a more recent version is discovered, CTC gives you the option of downloading the newer version to your PC. For more information about the automatic version search, refer to the "Cisco Transport Controller Operation" chapter in the *Cisco ONS 15600 SDH Reference Manual*.

Display Node, Card, and Network Views

CTC provides three views of the ONS platform:

- Node view appears when you first log into an ONS 15600 SDH. This view shows a graphic of the ONS 15600 SDH shelf and provides access to tabs and subtabs that you use to manage the node.
- Card view provides access to individual ONS 15600 SDH cards. This view shows a graphic of the card and provides access to tabs and subtabs that you use to manage the card.
- Network view shows all the nodes in a ring. A Superuser can set up this feature so each user will see the same network view, or the user can create a custom view with maps. This view provides access to tabs and subtabs that you use to manage the network. Network view can contain domains. A domain is used to isolate nodes or groups of nodes for easier maintenance. Double-clicking a domain shows all the nodes in the domain; nodes connected to the domain are grayed out.

Table A-1 lists different actions for changing CTC views.

Table A-1 Change CTC Views

To display:	Perform one of the following:
Node view	• Log into a node; node view is the default view. • In network view, double-click a node icon, or right-click the node and choose **Open Node**. • From the CTC View menu, choose **Go To Other Node**, then choose the node you want from the shortcut menu. • Use the arrows on the CTC toolbar to navigate up or down views. For example, in network view select a node and click the down arrow.
Home view (node view of the first node you logged into in a network)	• From the CTC View menu, choose **Go To Home View**.
Card view	• In node view, double-click a card or right-click the card and choose **Open Card**. • In node view, single-click a card icon, then select **Go To Selected Object View** from the View menu. • Use the arrows on the CTC toolbar to navigate up or down. For example, in node view select a card and then click the down arrow.
Network view	• In node view, click the up arrow on the CTC toolbar. • From the View menu, choose **Go To Network View**.

CTC Window

Different navigational methods are available within the CTC window to access views and perform management actions. You can double-click and right-click objects in the graphic area and move the mouse over nodes, cards, and ports to view popup status information.

CTC Menu and Toolbar Options

The CTC window menu bar and toolbar provide primary CTC functions. Table A-2 shows the actions that are available from the CTC menu and toolbar.

Table A-2 CTC Menu and Toolbar Options

Menu	Menu Option	Toolbar	Description
File	Add Node	➕	Adds a node to the current session. See the "DLP-F183 Add a Node to the Current Session or Login Group" task on page 16-37.
	Delete Selected Node	➖	Deletes a node from the current session.
	Lock CTC	🔒	Locks CTC without closing the CTC session. A user name and password are required to reopen CTC.
	Print	🖨	Prints CTC data. See the "DLP-F336 Print CTC Data" task on page 18-36.
	Export	⬆	Exports CTC data. See the "DLP-F379 Export CTC Data" task on page 18-88.
	Exit	↔	Closes the CTC session. The exit icon only appears in the File menu.
Edit	Preferences	✋	Displays the Preferences dialog box: • General tab—Allows you to change event defaults and manage preferences. • Login Node Group tab—Allows you to create login node groups. See the "DLP-F307 Create Login Node Groups" task on page 18-9. • Map—Allows you to customize the network view. See the "DLP-F223 Change the Network View Background Color" task on page 17-21 and the "DLP-F225 Apply a Custom Network View Background" task on page 17-22. • Circuit—Allows you to change the color of circuit spans. See the "DLP-F218 Change Active and Standby Span Color" task on page 17-17. • Firewall—Sets the Internet Inter-ORB Protocol (IIOP) listener ports for access to the ONS 15600 SDH through a firewall. See the "NTP-F136 Set Up the ONS 15600 SDH for Firewall Access" procedure on page 4-8. • JRE—Allows you to select a different Java Runtime Environment (JRE) when CTC restarts. • SOCKS—Allows you to choose the ONS 15600 SDH SOCKS servers in SOCKS-proxy-enabled networks. See the "DLP-F398 Provision the Designated SOCKS Servers" task on page 18-121.

Table A-2 CTC Menu and Toolbar Options (continued)

Menu	Menu Option	Toolbar	Description
View	Go To Previous View	⇦	Displays the previous CTC view.
	Go To Next View	⇨	Displays the next CTC view. Available only after you navigate to a previous view. Go to Previous and Go to Next is similar to forward/backward navigation in a web browser.
	Go To Parent View	⇧	References the CTC view hierarchy: network view, node view, and card view. In card view, this command displays the node view; in node view, the command displays network view. Not available in network view.
	Go To Selected Object View	⇩	Displays the object selected in the CTC window.
	Go To Home View	🏠	Displays the login node in node view.
	Go To Network View	⧉	Displays the network view.
	Go To Other Node	🌐	Displays a dialog box allowing you to type in the node name or IP address of a network node that you want to view.
	Show Status Bar	—	Displays or hides the status bar at the bottom of the CTC window.
	Show Tool Bar	—	Displays or hides the CTC toolbar.
—	—	⊖	Zooms out the network view area (toolbar only).
—	—	⊕	Zooms in the network view area (toolbar only).
—	—	🔍	Zooms in a selected network view area (toolbar only).

Table A-2 CTC Menu and Toolbar Options (continued)

Menu	Menu Option	Toolbar	Description
Tools	Circuits	—	Displays the following options: - Repair Circuits—Repairs incomplete circuits following replacement of the ONS 15600 SDH alarm interface panel (AIP). Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for more information. - Reconfigure Circuits—Allows you to reconfigure circuits. See the "NTP-F182 Reconfigure Circuits" procedure on page 7-6 for more information. - Merge Circuits—Merges multiple circuits. See the "NTP-F183 Merge Circuits" procedure on page 7-7. - Set Path Selector Attributes—Allows you to edit subnetwork connection protection ring (SNCP) circuit path selector attributes. See the "DLP-F264 Edit SNCP Circuit Path Selectors" task on page 17-55. - Set Circuit State—Allows you to change a circuit state. See the "DLP-F313 Change a Circuit Service State" task on page 18-13. - Roll Circuit—Allows you to reroute live traffic without interrupting service. See the "NTP-F181 Bridge and Roll Traffic" procedure on page 7-5. - Delete Rolls—Removes rolls that are not deleted by CTC after a roll has been completed. See the "DLP-F356 Delete a Roll" task on page 18-69. - Upgrade OCHNC—(ONS 15454 only) Upgrades OCHNCs created in earlier software releases to OCHCCs. Refer to the *Cisco ONS 15454 DWDM Procedure Guide* for more information. - Show RPR Circuit Ring—(ONS 15454 only) Shows the RPR ring for the circuit selected on the Circuits window.
	Overhead Circuits	—	Displays the Repair IP Tunnels option, which fixes circuits that are in the PARTIAL status as a result of node IP address changes. Refer to the "NTP-F178 Modify and Delete Overhead Circuits and Server Trails" procedure on page 7-3.
	Topology Upgrade	—	Displays the following options: - Convert SNCP to MS-SPRing (This option does not apply to the ONS 15600 SDH)—Converts SNCP to multiplex-section shared protection ring (MS-SPRing). - Convert Unprotected to SNCP (This option does not apply to the ONS 15600 SDH)—Converts a point-to-point or linear ADM to SNCP.
	Manage VLANs	—	Displays a list of VLANs that have been created and allows you to delete or create new VLANs. (This option does not apply to the ONS 15600 SDH.)
	Open TL1 Connection		Displays the TL1 session dialog box so you can create a TL1 session to a specific node. Refer to the *Cisco ONS SDH TL1 Command Guide*.
	Open IOS Connection		(Not applicable to ONS 15600 SDH.) Displays the Cisco IOS command line interface dialog box if a Cisco IOS capable card (ML1000-2, ML100T-12, or ML100X-8) is installed in the node. Refer to the *Ethernet Card Software Feature and Configuration Guide*.
	Update CTC	—	Allows you to update CTC to a newer version, if a newer version was found during network discovery.

Table A-2 CTC Menu and Toolbar Options (continued)

Menu	Menu Option	Toolbar	Description
Help	Contents and Index	—	Displays the online help window.
	User Manuals	—	Displays the Cisco ONS 15600 SDH documentation.
	About CTC	—	Displays the software version and the nodes in the CTC session.
—	Network Scope	—	The network scope drop-down list has three options: DWDM (ONS 15454s only) ,TDM, or All. If you choose DWDM, dense wavelength division multiplexing (DWDM) and hybrid nodes appear on the network view map. If you choose TDM, time division multiplexing (TDM) and hybrid nodes appear on the network view map. If you choose All, every node in the network appears on the network view map.
—	Link Filter	▽	Opens the Link Filter dialog box, which allows you to choose which link classes display on the non-detail network map. The available classes vary according to the selected network scope. • ALL—DCC, GCC, OTS, PPC, server trail • DWDM—GCC, OTS, PPC • TDM—DCC, PPC, server trail
—	—	⊞	Opens the Collapse/Expand Links dialog box, which allows you to globally expand or consolidate network view links based on link type.
—	—	⚠ ⚠	Opens the CTC Alerts dialog box, which shows the status of certain CTC background tasks. When the CTC Alerts toolbar icon contains a red triangle, unread notifications exist. When there are no unread notifications, the CTC Alerts toolbar icon contains a gray triangle (see the Toolbar column for comparison). Notifications include: • Network disconnection • Send-PDIP inconsistency—CTC discovers a new node that does not have a SEND-PDIP setting consistent with the login node. • Circuit deletion status—Reports when the circuit deletion process completes if you choose "Notify when complete" as described in the "DLP-F293 Delete Circuits" task on page 17-83. The CTC Alerts window always reports circuit deletion errors. • Conditions retrieval error • Software download failure You can save a notification by clicking the Save button in the CTC Alerts dialog box and navigating to the directory where you want to save the text file. By default, the CTC Alerts dialog box opens automatically. To disable automatic popup, see the "DLP-F309 Configure the CTC Alerts Dialog Box for Automatic Popup" task on page 18-11.

CTC Mouse Options

Table A-3 shows mouse navigation techniques in CTC.

Table A-3 CTC Mouse Options

Technique	Description
Double-click	• Node in network view—Displays the node view. • Domain in network view—Displays the domain view. • Card in node view—Displays the card view. • Alarm/Event—Displays the object that raised the alarm or event. • Circuits—Displays the Edit Circuit window.

Table A-3 CTC Mouse Options (continued)

Technique	Description
Right-click	• Network view graphic area—Displays a menu that you can use to create a new domain; change the position and zoom level of the graphic image; save the map layout (if you have a Superuser security level); reset the default layout of the network view; set, change, or remove the background image and color; collapse and expand links; and save or reset the node position. • Domain in network view—Displays a menu that you can use to open a domain, show the domain overview, rename the domain, and delete the domain. • Node in network view—Displays a menu where you can open the node, go to the node domain, reset the node icon position to the longitude and latitude set on the Provisioning > General tabs, provision circuits, and update circuits with a new node. • Span in network view—Displays a menu where you can view information about the source and destination ports, the span's protection scheme, and the span's optical level. You can also display the Circuits on Span dialog box, which displays additional span information and allows you to perform SNCP protection switching. If a MS-SPRing is provisioned, you can display the PCA circuits. You can also expand and collapse links. • Card in node view—Displays a menu where you can open, delete, hard and soft reset, and change cards. The card you select determines the commands that appear. • Card in card view—Displays a menu that you can use to reset the card, or go to the parent view (node view). • Empty slot in node view—Displays a menu that allows you to add (preprovision) a card.
Move mouse cursor	• Over node in network view—Displays a summary of node alarms and provides a warning if the node icon has been moved out of the map range. • Over span in network view—Displays circuit (node, slot, port) bandwidth and protection information. • Over domain in network view—Displays domain name and the number of nodes in the domain. • Over card in node view—Displays card type, card status, highest-level alarm, and alarm profile status. The ONS 15600 SDH ASAP card displays the Protocol Independent Multicast (PIM) and pluggable port modules (PPM). • Over card in node view—Displays card type, card status, and alarm profile status. • Over card port in node view—Displays port number and/or name, port service state, PPM, and alarm profile status.

Node View Shortcuts

Table A-4 shows actions on ONS 15600 SDH cards that you can perform by moving your mouse over the CTC window.

Table A-4 Node View Card Shortcuts

Action	Shortcut
Display card information	Move your mouse over cards in the graphic to display tooltips with the card type, card status (active or standby), the highest level of alarm (if any), and the alarm profile used by the card.
Open, reset, or delete a card	Right-click a card. Choose **Open Card** to display the card in card view, **Hard-reset Card** to perform a hard reset on the card, **Soft-reset Card** to perform a soft reset of the card, or **Delete Card** to delete it.
Preprovision a slot	Right-click an empty slot. Select the card type you want to provision the slot for from the shortcut menu.
Change a card	Right-click an STM-N card and choose **Change Card**. In the Change Card dialog box, select the card type. Change card retains all card provisioning.
Change view	Right-click on the area outside the node to display a menu that allows you to return to the parent view.

Network View Shortcuts

Right-click the network view graphic area or a node, span, or domain to display shortcut menus. Table A-5 lists the actions that are available from the network view.

Table A-5 Network Management Tasks in Network View

Action	Task
Open a node	Do any of the following: • Double-click a node icon. • Right-click a node icon, and choose **Open Node** from the shortcut menu. • Click a node and choose **Go To Selected Object View** from the CTC View menu. • From the View menu, choose **Go To Other Node**. Select a node from the Select Node dialog box. • Double-click a node alarm or event in the Alarms or History tabs.
Move a node icon	Press the **Ctrl** key and the left mouse button simultaneously and drag the node icon to a new location.
Reset node icon position	Right-click a node and choose **Reset Node Position** from the shortcut menu. The node icon moves to the position defined by the longitude and latitude fields on the Provisioning > General tabs in node view.
Consolidate links	Right-click on a link and choose **Consolidate/Expand** from the shortcut menu. For more detailed instructions, see Chapter 11, "Change Node Settings."

Table A-5 Network Management Tasks in Network View (continued)

Action	Task
Provision a circuit	Right-click a node. From the shortcut menu, choose **Provision Circuit To** and select the node where you want to provision the circuit. For circuit creation procedures, see Chapter 6, "Create Circuits."
Update circuits with new node	Right-click a node and choose **Update Circuits With New Node** from the shortcut menu. Use this command when you add a new node and want to pass circuits through it.
Display a link endpoint	Right-click a span. From the shortcut menu, choose **Go To** [<node> | <port> | <slot>] for the drop port you want to view. CTC displays the card in card view.
Display span properties	Do any of the following: • Move mouse over a span; the properties appear near the span. • Click a span; the properties appear in the upper left corner of the window. • Right-click a span; the properties appear at the top of the shortcut menu.
Perform an SNCP protection switch for all circuits on a span	Right-click a network span and click **Circuits**. In the Circuits on Span dialog box, switch options appear in the SNCP Span Switching field.
Upgrade terminal to linear	Right-click a span and choose **Upgrade Protection** > **Terminal to Linear** from the shortcut menu. See the "NTP-F210 Convert a Point-to-Point to a Linear ADM Automatically" procedure on page 12-1.

Table Display Options

Table A-6 shows table display options, which include rearranging or hiding CTC table columns and sorting table columns by primary or secondary keys.

Table A-6 Table Display Options

Action	Click Shortcut	Right-Click Shortcut Menu
Resize column	Click while dragging the column separator to the right or left.	—
Rearrange column order	Click while dragging the column header to the right or left.	—
Reset column order	—	Choose **Reset Columns Order/Visibility**.
Hide column	—	Choose **Hide Column**.
Display a hidden column	—	Choose **Show Column >** *column-name*.
Display all hidden columns	—	Choose **Reset Columns Order/Visibility**.
Sort table (primary)	Click a column header; each click changes sort order (ascending or descending).	Choose **Sort Column**.

Table A-6 Table Display Options (continued)

Action	Click Shortcut	Right-Click Shortcut Menu
Sort table (secondary sorting keys)	Press the **Shift** key and simultaneously click the column header.	Choose **Sort Column (incremental)**.
Reset sorting	—	Choose **Reset Sorting**.
View table row count	—	View the number after **Row count=**; it is the last item on the shortcut menu.

Equipment Inventory

In node view, the Inventory tab displays ONS 15600 SDH equipment information, including:

- Location—Where the equipment is installed, either chassis or slot number.
- Eqpt Type—The equipment type, for example, FAN_TRAY or STM-16.
- Admin State—Changes the card service state unless network conditions prevent the change. For more information about card states, refer to the “Enhanced State Model” appendix of the *Cisco ONS 15600 SDH Reference Manual.*
  - Unlocked—Puts the card in the Unlocked-enabled service state.
  - Locked,maintenance—Puts the card in the Locked-enabled,maintenance service state.
- Service State—Displays the current card service state, which is an autonomously generated state that gives the overall condition of the card. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State. For more information about card states, refer to the “Administrative and Service States” appendix of the *Cisco ONS 15600 SDH Reference Manual.* Actual Eqpt Type—The actual equipment type, for example, FTA or STM16-LR.
- HW Part #—Hardware part number; this number is printed on the top of the card or equipment piece.
- HW Rev—Hardware revision number.
- Serial #—Equipment serial number; this number is unique to each card.
- CLEI Code—Common Language Equipment Identifier code.
- User Code—A text entry field that allows the user to type a 20-character ASCII code to further identify cards.
- Bootroom Rev—Displays the boot read-only memory (ROM) revision number.
- Product ID—Displays the manufacturing product identifier for a hardware component, such as a fan tray, chassis, or card.
- Version ID—Displays the manufacturing version identifier for a fan tray, chassis, or card.

INDEX