

Cisco NCS 2000 Series Control Card and Node Configuration Guide, Release 11.x.x

First Published: 2019-03-08

Last Modified: 2026-04-02

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

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: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco 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.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

Full Cisco Trademarks with Hardware License ?

PREFACE **Cisco NCS Documentation Roadmap** ix

PREFACE **New and Changed Information** xvii

CHAPTER 1 **Installing the Cisco NCS 2000 Series** 1

Installing the Cisco NCS 2000 Series 1

CHAPTER 2 **Installing the Control Cards** 3

Card Compatibility 4

Cards Supported in Cisco NCS Software 4

Safety Labels 7

TNC and TNCE Card 7

Control Card Workflow Diagram 7

Related Procedures for TNC and TNCE Cards 9

TSC and TSCE Cards 9

Related Procedures for TSC and TSCE Cards 10

TNCS Card 10

TNCS-O Card 11

Operating Modes for TNC, TNCE, TNCS, or TNCS-O cards 13

TNCS-2 and TNCS-2O Cards 13

Support for OTDR 15

OTDR Training 17

Control Card Workflow Diagram 17

Related Procedures for TNCS and TNCS-O Cards 21

Digital Image Signing 21

DIS Identification 21

Related Procedures for DIS 21

Control Card Reset 22

Control Card Database 22

NTP-G313 Installing and Configuring the TNC, TNCE, TSC, TSCE, TNCS, TNCS-O, TNCS-2, and TNCS-2O Card 23

DLP-G604 Installing the TNC, TNCE, TSC, TSCE, TNCS-2, TNCS-2O, TNCS-O, or TNCS Card 24

DLP-G605 Provisioning PPM and Port for the TNC, TNCE, TNCS-2, TNCS-2O, and TNCS Cards 29

DLP-G606 Configuring UDC and VoIP for the TNC, TNCE, TNCS-2, TNCS-2O, and TNCS/TNCS-O Cards 30

DLP-G788 Configuring Operating Mode for the TNC, TNCE, TNCS, TNCS-O, TNCS-2, and TNCS-2O Cards 31

DLP-G774 Changing the Frame Type on the OSC 32

Accessing and Configuring the Controller Cards Using Link-Local Address 33

NTP-G278 Upgrade an Older Controller Card to a Newer Controller Card 34

LCD or ECU Hot Plug-In 37

Insert an LCD/ECU of Release prior to 11.0 in a Release 11.0 Chassis 38

Insert an LCD/ECU of Release 11.0 in a Release prior to 11.0 Chassis 38

Upgrade the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O Card to the TNCS-2 or TNCS-2O Card 39

Dual Shelf Control - Upgrade the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O Card to the TNCS-2 or TNCS-2O Cards 40

Dual Shelf Control - Upgrade Control Card to TNCS-2 or TNCS-2O Card 42

Single Shelf Control - Upgrade Control Card to TNCS-2 or TNCS-2O Card 42

Single Shelf Control - Upgrade Control Card with Release 11.0 43

Downgrade the TNCS-2 and TNCS-2O Cards to TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O Cards 44

Dual Shelf Control - Downgrade Control Cards to TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O Card 45

Dual Shelf Control - Downgrade A Single TNCS-2 or TNCS-2O Card to the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O Card 47

Single Shelf Control - Downgrade Control Card with Software prior to Release 11.0 48

CHAPTER 3 **Connecting the PC and Logging into the GUI 51**

Connecting the PC and Logging into the GUI 51

CHAPTER 4 **Managing the Shelf 53**

NTP-G139 Verifying Cisco Transport Planner Reports and Files 54

Cisco Transport Planner Node Setup Information and Files 55

NTP-G22 Verifying Common Card Installation 56

NTP-G250 Verifying Digital Image Signing (DIS) Information 57

NTP-G144 Provisioning a Multishelf Node 59

Duplicate Node Controller 61

NTP-G23 Create Users and Assign Privileges 62

DLP-G54 Create a Local User on a Single Node Using CTC 63

DLP-G55 Creating a New User on Multiple Nodes 64

Setting Maximum Password Length Using CTC 65

NTP-G24 Setting Up Node Identification Information 66

NTP-G25 Setting Battery Power Monitor Thresholds 68

NTP-G26 Setting Up CTC Network Access 69

DLP-G56 Provisioning IP Settings 70

DLP-G439 Provisioning the Designated SOCKS Servers 74

DLP-G57 Setting the IP Address, Default Router, and Network Mask Using the LCD 75

DLP-G264 Enabling Node Security Mode 78

DLP-G58 Creating a Static Route 80

DLP-G59 Setting Up or Changing Open Shortest Path First Protocol 81

DLP-G60 Setting Up or Changing Routing Information Protocol 83

NTP-G194 Setting Up EMS Secure Access to the Node 84

NTP-G27 Setting Up the Node for Firewall Access 85

NTP-G28 Creating FTP Host 87

DLP-G61 Provisioning the IIOP Listener Port on the NCS 88

DLP-G62 Provisioning the IIOP Listener Port on the CTC Computer 88

NTP-G132 Provisioning OSI 89

DLP-G283 Provisioning OSI Routing Mode 90

DLP-G284 Provisioning the TARP Operating Parameters 92

DLP-G285 Adding a Static TID-to-NSAP Entry to the TARP Data Cache 94

DLP-G287 Adding a TARP Manual Adjacency Table Entry 95

DLP-G288 Provisioning OSI Routers 96

DLP-G289 Provisioning Additional Manual Area Addresses 97
DLP-G290 Enabling the OSI Subnet on the LAN Interface 98
DLP-G291 Creating an IP-Over-CLNS Tunnel 99
NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File 100
NTP-G320 Configuring the Node as a Non-DWDM Network 105
DLP-G348 Using the Cisco Transport Planner Shelf Layout Report 106
NTP-G31 Installing the DWDM Dispersion Compensating Units 107
NTP-G239 Managing Passive Units and Passive Shelves 108
DLP-G543 Adding Passive Units or Passive Shelves Manually 109
DLP-G544 Deleting a Passive Unit or Passive Shelf 110
DLP-G792 Performing a Firmware Upgrade on Passive Shelves 111
DLP-G793 Performing Upgrade on Fiber Shuffle 112
DLP-G762 Associating Passive Units or Passive Shelves to USB Ports 113
NTP-G152 Creating and Verifying Internal Patchcords 114
NTP-G242 Creating an Internal Patchcord Manually 116
NTP-G354 Creating an Internal Patchcord Manually Using the Trunk to Trunk (L2) Option 117
DLP-G547 Creating an Internal Patchcord Manually Using the OCH-Trunk to OCH-Filter Option 118
DLP-G548 Creating an Internal Patchcord Manually Using the OCH-Filter to OCH-Filter Option 120
DLP-G549 Creating an Internal Patchcord Manually Using the OTS to OTS Option 122
DLP-G531 Creating an Internal Patchcord Manually Using the Optical Path Option 125
DLP-G355 Deleting an Internal Patchcord 126
NTP-G209 Creating, Editing, and Deleting Optical Sides 127
DLP-G491 Creating an Optical Side 128
DLP-G492 Editing an Optical Side 128
DLP-G480 Deleting an Optical Side 129
NTP-G38 Provisioning OSC Terminations 130
NTP-G37 Running Automatic Node Setup 132
NTP-G163 Upgrading Nodes in Single-Shelf Mode to Multishelf Mode 134
DLP-G730 Editing the Shelf ID of the Subtending Shelf in a Multishelf Configuration Using the LCD 136

CHAPTER 5 **Synchronizing Node Timing** 139
Synchronizing Node Timing 139

CHAPTER 6 Provisioning Security 141

Provisioning Security 141

APPENDIX A Card Specifications 143

APPENDIX B SNMP 145

APPENDIX C CTC Enhancements, Operations, and Shortcuts 147

APPENDIX D Network Element Defaults 149



Cisco NCS Documentation Roadmap

To quickly access publications of Cisco NCS Release 11.x.x, see the Documentation Roadmap.

Note Starting with Release 11.1.4, ONS 15454 M12 chassis and TCC3 card are not supported on the ONS 15454 DWDM and WSON software packages. You must not attempt to upgrade ONS 15454 M12 nodes from a previous release to Release 11.1.4.

Note Cisco ONS 15454 M2 chassis has reached its end-of-life status. For more information, see the Retirement Notification page.

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`Courier font`	Terminal sessions and information the system displays appear in `courier` font.
`Bold Courier font`	Bold Courier font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.

Convention	Description
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x | y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document uses the following conventions for reader alerts:



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



Tip Means *the following information will help you solve a problem.*



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



Timesaver Means *the described action saves time.* You can save time by performing the action described in the paragraph.



Warning **Means *reader be warned.* In this situation, you might perform an action that could result in bodily injury.**

Cisco NCS Documentation Roadmap

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

Cisco NCS Documentation Roadmap

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

Cisco NCS Documentation Roadmap

Varning!

VIKTIGA SÄKERHETSANVISNINGAR

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

SPARA DESSA ANVISNINGAR

Figyelem

FONTOS BIZTONSÁGI ELOÍRÁSOK

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

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение

ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ

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

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告

重要的安全性说明

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

请保存这些安全性说明

警告

安全上の重要な注意事項

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

これらの注意事項を保管しておいてください。

주의

중요 안전 지침

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

이 지시 사항을 보관하십시오.

Cisco NCS Documentation Roadmap

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

Cisco NCS Documentation Roadmap

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 כדי 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**

Where to Find Safety and Warning Information

For safety and warning information, refer to the Regulatory Compliance and Safety Information document that accompanied the product. This publication describes the international agency compliance and safety information. It also includes translations of the safety warnings.

Cisco NCS 2000 Series cards are classified as Laser Class 1 or 1M as per IEC 60825-1 and Hazard Level 1M as per IEC 60825-2.

Figure 1: Class 1M Laser Product Label



Cisco NCS Documentation Roadmap

Figure 2: Class 1M Laser Product Label



Complies with 21 CFR 1040.10 and 1040.11 except for conformance with IEC 60825-1 Ed. 3., as described in Laser Notice No. 56, dated May 8, 2019.

Conforme à la norme 21 CFR 1040.10 et 1040.11, sauf conformité avec la norme IEC 60825-1 Ed. 3., comme décrit dans l'avis relatif au laser no. 56, daté du 8 Mai 2019.

366295

Statement 291



New and Changed Information

This table summarizes the new and changed information for Release 11.12, and tells you where the features are documented.

Table 1: New and Changed Features - R11.12

Feature	Description	Where Documented
Secure Unique Device Identification (SUDI) SUDI 2099 Certificates for WSE, MR-MXP, and 400G XP Cards	This enhancement allows you to extend the usage of WSE, MR-MXP and 400G-XP-LC cards with encryption functionality beyond year 2029. This extended validity helps to avoid encryption and card upgrade failures.	*Cisco NCS 2000 Series Line Card Configuration Guide* SUDI 2099 Certificate for WSE, MR-MXP, and 400G-XP-LC Cards
MCH Custom Alien Wavelength and MEDIA CHANNEL OCH NC circuit management through CTC	The feature allows you to create an MCH custom alien wavelength and the associated MEDIA CHANNEL OCH NC circuit specifying the following parameters through CTC: • Signal width • Modulation guard band • Filtering guard band This functionality enables you to create a medial channel of any spectrum size, for example, signal width of 34.20 GHz, modulation GB of 1.71 GHz, and filtering GB of 4.92 GHz.	*Cisco NCS 2000 Series Network Configuration Guide, Release 11.x.x* MCH Custom Alien Bandwidth Parameters
GMPLS Hybrid circuit between NCS 4000 and 400G-XP-LC-CFP2	This enhancement allows you to create a GMPLS Hybrid circuit connection between NCS 4000 and NCS 2000 with 400G-XP-LC-CFP2 transponder.	*Cisco NCS 2000 Series Network Configuration Guide* DLP-G800 Create an Link Management Protocol (LMP) Link Using CTC

Feature	Description	Where Documented
Dynamic Power Allocation on 200G-CK-LC and 400G-XP-LC Cards	This feature allows you to dynamically allocate power based on the line card operating mode. This maximises the usage of the NCS 2015 chassis slots in a 2+2 PSU configuration.This feature is supported on the 200G-CK-LC and 400G-XP-LC cards.	*Cisco NCS 2000 Series Line Card Configuration Guide* 200G-CK-LC Card 400G-XP-LC Card
Fiber Shuffle Upgrade	This feature allows you to upgrade the Boot ROM version, OS Kernel, and Uboot version of the fiber shuffle through CTC.	*Cisco NCS 2000 Series Control Card and Node Configuration Guide* DLP-G793 Performing Upgrade on Fiber Shuffle
Pluggables Support	• QSFP-100G-FR-S pluggable is supported on 400G-XP-LC card. • CPAK-100G-FR pluggable is supported on 200G-CK-LC and MR-MXP cards	*Installing the GBIC, SFP, SFP+, QSFP, XFP, CXP, CFP and CPAK Optical Modules in Cisco NCS Platforms* Compatibility by Card QSFP Specifications CPAK Description and Specifications

This table summarizes the new and changed information for Release 11.1.1.2, and tells you where the features are documented.

Table 2: New and Changed Features - R11.1.1.2

Feature	Description	Where Documented
OTDR Enhancements	Optical Time Domain Reflectometer (OTDR) supports the Refractive Index (RI) and Backscatter Coefficient (BS) parameters for OTDR scan.	*Manage the Node* DLP-G786 Perform OTDR Scan
GCC0 Transparency in REGEN Mode	The GCC0 enable in REGEN mode is supported on the 400G-XP-LC card.	*Cisco NCS 2000 Series Line Card Configuration Guide* 400G-XP-LC Card

This table summarizes the new and changed information for Release 11.1, and tells you where the features are documented.

Table 3: New and Changed Features - R11.1

Feature	Description	Where Documented
Submarine Line Terminal Equipment (SLTE)	In Submarine Line Terminal Equipment (SLTE) topology, the channel SMR (CH SMR) card of NCS 2000 node aggregates channels from transponders, say NCS 1004. If there is more than one channel SMR card, they are connected by the 1*6 AD-CFS passive module. The aggregated channels from this passive module are transmitted to the fan-out module that covers signals from other geographical locations and SMR card. The channels are then transmitted to the SLTE SMR card that faces the submarine system.	*Cisco NCS 2000 Series Network Configuration Guide* Understanding SLTE
400G-XP-LC Enhancements	The OPM_PEER_ODU2 and OPM_PEER_ODU2e slice modes are available on Slice 2 when the 400G-XP-LC card is configured in the MXP mode for any trunk configuration. These slice modes support interoperability with a peer 10x10G-LC card. The peer 10x10G-LC card can only be installed in an even slot of the Cisco NCS 2006 or Cisco NCS 2015 chassis. The payloads supported on the 10x10G-LC card are OTU2, OTU2e, OC192/STM64, and 10GE.	*Cisco NCS 2000 Series Line Card Configuration Guide* 400G-XP-LC Card
GMPLS Enhancements	• Restoration is supported on Regen NCS 1004. • Manages greater than 50dB high span loss from validation. • Supports 200G QPSK from NCS 1004.	*Cisco NCS 2000 Series Network Configuration Guide* DLP-G800 Create an LMP Link Using CTC
LOGO Expert Mode	When the Expert mode is configured for an optical side, spectral parameters such as Linear XT avg, Linear XT Stdev, Non-linear XT avg and Non-linear XT Stdev are used by the control plane for optical validation. These parameter values are obtained from the XML file. These spectral values must not be modified, unless instructed by the Cisco TAC representative.	*Cisco NCS 2000 Series Network Configuration Guide* *LOGO Expert Mode*

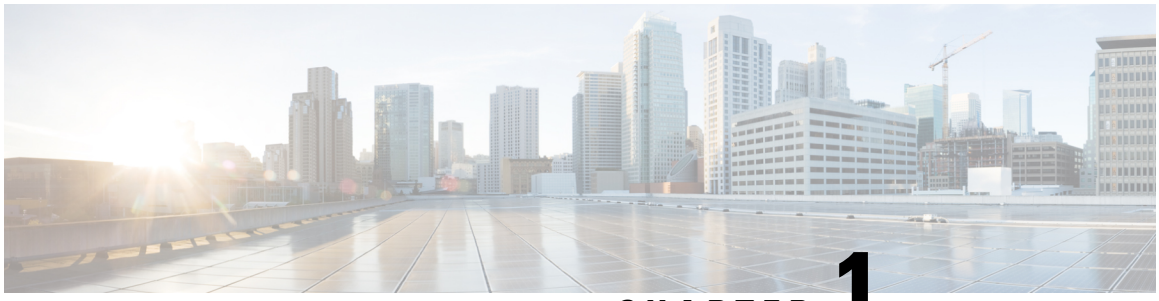
This table summarizes the new and changed information for Release 11.0, and tells you where the features are documented.

Table 4: New and Changed Features - R11.0

Feature	Description	Where Documented
OTNXC encryption	The OTNXC operating mode on the 400G-XP-LC card supports encryption.	*Cisco NCS 2000 Series Line Card Configuration Guide* NTP-G367 Provisioning Encryption on 400G-XP-LC Card
Third party certificates for encryption	The 400G-XP-LC card supports the generation of a Certificate Signing Request (CSR) and the installation of Locally Significant Certificates (LSCs) that can be used to authenticate the peer card connection. Third party certificates also referred to as Locally Significant Certificates (LSCs) are certificates that are signed by a Certification Authority (CA) other than Cisco Certificate Authority. LSCs allow customers to have their own Public Key Infrastructure (PKI) to provide better security, to have control of their own CA, and to define policies, restrictions, and usages on the generated certificates.	*Cisco NCS 2000 Series Line Card Configuration Guide* NTP-G363 Provisioning LSC on Cards
ANS APC Skipping	The upgraded NE update XML file imported on the CTC for the respective node will import the new ANS parameters and settings for the new degree or modules. The existing ANS parameters or module settings are not affected. This prevents unintended changes to the APC corrections to the existing degree and its associations.	*Cisco NCS 2000 Series Network Configuration Guide* Automatic Node Setup
TNCS-2 and TNCS-2-O Control Cards	The TNCS-2 and TNCS-2O are new control cards compatible with all chassis types such as, Cisco NCS 2002, Cisco NCS 2006, and Cisco NCS 2015.	*Cisco NCS 2000 Series Control Card and Node Configuration Guide* TNCS 2 and TNCS 2O Cards
TNCS-O Card Support	The TNCS-O card is supported on the NCS 2002.	*Cisco NCS 2000 Series Control Card and Node Configuration Guide* TNCS-O Card

Feature	Description	Where Documented
400G-XP-LC enhancements	• The new payloads supported for the MXP operating mode are FC-10G, FC-8G, and 40G. • The OPM_2x40G_2x10G slice mode can be configured in the MXP operating mode for 40GE payloads. • LLDP support—The source MAC address of 10 or 100GE ports can be retrieved after an LLDP packet is received on the client port. LLDP filtering is enabled or disabled on the 10GE or 100GE ports using the Provisioning > Line > Ethernet tab in CTC.	*Cisco NCS 2000 Series Line Card Configuration Guide* 400G-XP-LC Card
NCS 1004 Alien	Two variants of 300G , such as 300G_3bps and 300G_3.4375bps are added in the wavelength drop-down list.	*Cisco NCS 2000 Series Network Configuration Guide* DLP-G800 Create an LMP Link Using CTC
8QAM Support on non-SSON	In non-SSON, the user can force the wavelength by checking the wavelength configuration check box and choosing the wavelength from the drop-down list.	*Cisco NCS 2000 Series Network Configuration Guide* Provision GMPLS Optical Channel Network Connections Using Non-SSON
OTDR Support for TNCS-2O Cards	A TNCS-2O card has an optical module that provides Optical Time Domain Reflectometer (OTDR) measurement, ORL measurement, and standard Optical Service Channel (OSC) capability on two ports. These capabilities are available for upto four ports for each shelf; one shelf can have two TNCS-2O cards.	*Cisco NCS 2000 Series Network Configuration Guide* • Provisioning OTDR *Manage the Node* • NTP-G357 Perform OTDR Scan and OTDR Event Scan
Regenerator Constraints Support	For using a regenerator, the optical path needs to be validated. If the optical validation fails, then, the regenerator cannot be used, and the circuit creation fails. If validation is not supported, pre-validated paths are calculated offline and provided as a constraint to the control plane, while setting up the main and restored paths.	*Cisco NCS 2000 Series Network Configuration Guide*

New and Changed Information



CHAPTER 1

Installing the Cisco NCS 2000 Series

This chapter has information on installing NCS 2000 Series.

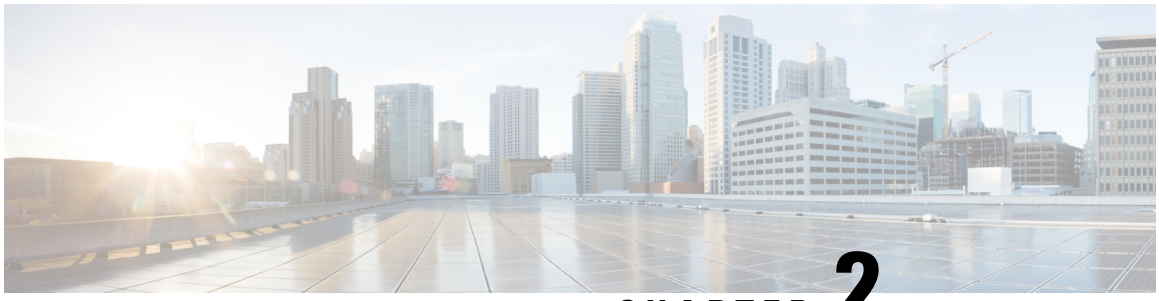
- Installing the Cisco NCS 2000 Series, on page 1

Installing the Cisco NCS 2000 Series

For information on installing the Cisco NCS 2000 series, see:

Cisco NCS 2000 Series Hardware Installation Guide

Installing the Cisco NCS 2000 Series



CHAPTER 2

Installing the Control Cards

Note Starting with Release 11.1.4, ONS 15454 M12 chassis and TCC3 card are not supported on the ONS 15454 DWDM and WSON software packages. You must not attempt to upgrade ONS 15454 M12 nodes from a previous release to Release 11.1.4.

This chapter describes the common control cards needed for the Cisco NCS 2000 Series platforms and provides installation and card turn up procedures.

- Card Compatibility, on page 4
- Cards Supported in Cisco NCS Software, on page 4
- Safety Labels, on page 7
- TNC and TNCE Card, on page 7
- TSC and TSCE Cards, on page 9
- TNCS Card, on page 10
- TNCS-O Card, on page 11
- TNCS-2 and TNCS-2O Cards, on page 13
- Support for OTDR, on page 15
- Control Card Workflow Diagram, on page 17
- Related Procedures for TNCS and TNCS-O Cards, on page 21
- Digital Image Signing, on page 21
- DIS Identification, on page 21
- Control Card Reset, on page 22
- Control Card Database, on page 22
- NTP-G313 Installing and Configuring the TNC, TNCE, TSC, TSCE, TNCS, TNCS-O, TNCS-2, and TNCS-2O Card, on page 23
- NTP-G278 Upgrade an Older Controller Card to a Newer Controller Card, on page 34
- LCD or ECU Hot Plug-In , on page 37
- Upgrade the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O Card to the TNCS-2 or TNCS-2O Card, on page 39
- Downgrade the TNCS-2 and TNCS-2O Cards to TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O Cards, on page 44

Card Compatibility

Note The DB-9 console port of the node controller works only on the active control card of the GNE or ENE and not on the standby control card. The DB-9 console port also does not work in control cards installed in the sub-tending shelves. The console port is available on all control cards except the TNCS-2 and TNCS-2O cards.

Table 5: Platform and Software Release Compatibility for Control Cards

Card Name	R10.0	R10.1	R10.3	R10.5	R10.5.2	R10.6.1, R10.6.2, R10.7, R10.8, and R10.9	R11.x.x
TNC/TSC	NCS 2002, NCS 2006	NCS 2002, NCS 2006	NCS 2002, NCS 2006	NCS 2002, NCS 2006	NCS 2002, NCS 2006	NCS 2002, NCS 2006	NCS 2002, NCS 2006
TNCE/TSCE	NCS 2002, NCS 2006	NCS 2002, NCS 2006	NCS 2002, NCS 2006	NCS 2002, NCS 2006	NCS 2002, NCS 2006	NCS 2002, NCS 2006	NCS 2002, NCS 2006
TNCS	No	No	No	NCS 2015	NCS 2006, NCS 2015	NCS 2002, NCS 2006, NCS 2015	NCS 2002, NCS 2006, and NCS 2015
TNCS-O	No	No	No	No	NCS 2006, NCS 2015	NCS 2006 and NCS 2015	NCS 2002, NCS 2006, and NCS 2015
TNCS-2	No	No	No	No	No	No	NCS 2002, NCS 2006, and NCS 2015
TNCS-2O	No	No	No	No	No	No	NCS 2002, NCS 2006, and NCS 2015

Cards Supported in Cisco NCS Software

There are two types of NCS nodes:

- Flex NCS Node: Node that supports Flex Spectrum functionality and up to 96 channels in the ITU-T C band.

- Fixed Grid NCS Node: Node that supports fixed 80 channels in the ITU-T C band.

The following table lists the cards that are supported in Flex NCS and Fixed Grid NCS nodes.

Node Type	Control Cards	Amplifier Cards	Add/Drop Units	Transponder and Muxponder Cards
Flex NCS	• TNC • TSC • TNCE • TSCE • TNCS • TNCS-O • TNCS-2 • TNCS-2O	• OPT-AMP-C • EDRA-1-xx • EDRA-2-xx • OPT-EDFA-17 • OPT-EDFA-24 • RAMAN-CTP • RAMAN-COP	• 16-WXC-FS • 15216-MD-48-ODD • 15216-MD-48-EVEN • 15216-MD-48-CM • MF-4X4-COFS • MF-16AD-CFS • MF-DEG-5 • MF-UPG-4 • MF-MPO-8LC • PSM • 17 SMR9 FS • 24 SMR9 FS • 34 SMR9 FS • SMR20 FS • SMR20 FS CV • 12-AD-FS • 16-AD-FS • MF-MPO-16LC • MF-2MPO-ADP • MF-16AE-CFS • MF-10AD-CFS • PPMESH8-5AD • MF-DEG-5-CV • MF-UPG-4-CV • MF-M16LC-CV • MF-MPO-20LC • NCS2K-MF-6AD-CFS • NCS2K-MF-8X10G-FO	• 100G-LC-C • 100G-ME-C • 100G-CK-C • 100ME-CKC • 10x10G-LC • CFP-LC • AR_MXP • AR_XPE • WSE • 40G-MXP • 100GS-CK-LC • 200G-CK-LC • MR-MXP • 40E-MXP-C • 40ME-MXP-C • 400G-XP-LC

Node Type	Control Cards	Amplifier Cards	Add/Drop Units	Transponder and Muxponder Cards
Fixed Grid NCS	• TNC • TSC • TNCE • TSCE • TNCS • TNCS-O • TNCS-2 • TNCS-2O	• OPT-PRE • OPT-BST • OPT-BST-E • OPT-AMP-17-C • OPT-AMP-C • OPT-RAMP-C • OPT-RAMP-CE • OPT-EDFA-17 • OPT-EDFA-24 • RAMAN-CTP • RAMAN-COP • OSCM • OSC-CSM • TDC-CC • TDC-FC • 15216 FBG DCU	• 80-WXC-C • 15216-MD-40-ODD • 15216-MD-40-EVEN • 15216-MD-48-ODD • 15216-MD-48-EVEN • 15216-MD-48-CM • 15216-MD-ID-50 • 40-WXC-C • 40-SMR1-C • 40-SMR2-C • 15216-EF-40-ODD • 32WSS • 40-WSS-C • 40-WSS-CE • PSM • 40-MUX • 32-DMX • 40-DMX-CO • 40-DMX-CE • 15216-EF-40-EVEN • 15454-PP-MESH-4 • 15454-PP-MESH-8 • 15454-PP-4-SMR • NCS2K-MF-8X10G-FO • NCS2K-MF-MPO-20LC • 15216-MD-48-ODDE • 15216-MD-EVENE • 15216-MD-48-CME	All the transponder and muxponder cards.

Note NCS2K-S, NCS2K-F, and NCS2K-L packages are not supported in ONS 15454 M12 during upgrade from any release preceding to R11.x and later.

Note The MF-4X4-COFS patch panel supports only fixed grid and can support up to 96 channels.

Safety Labels

For information about safety labels, see the "Safety Labels" section.

TNC and TNCE Card

(Cisco NCS 2002 and Cisco NCS 2006)

The TNC or TNCE cards are provisioned as active and standby in the NCS 2006 shelf, and as a stand-alone card in the NCS 2002 shelf. The TNC or TNCE cards serve as the processor card for the node.

On the NCS 2006 shelf, install redundant TNC or TNCE cards in slots 1 and 8. If the active TNC or TNCE card fails, the system traffic switches to the redundant TNC or TNCE card.

On the NCS 2002 shelf, install the stand-alone TNC or TNCE cards in slot 1. The TNC or TNCE cards support line cards in slots 2 and 3.

The NCS 2006 shelf has dual power supply. The TNC or the TNCE card monitors both supply voltage inputs on the NCS 2006 shelf. The TNC or TNCE card raises an alarm if one of the supply voltage inputs has a voltage out of the specified range.

You can insert and remove the TNC or TNCE card without impacting the system traffic, even when the system is online.

Note The TNC and TNCE cards are not supported on NCS 2015. When these cards are inserted into the active or standby slots of the NCS 2015 chassis, the cards do not start and become active.

For more information about the TNC and TNCE cards, see http://www.cisco.com/en/US/prod/collateral/optical/ps5724/ps2006/data_sheet_c78-602903.html.

Control Card Workflow Diagram

Workflow Diagram

The following figure shows the workflow diagram of the TNC/TSC/TNCE/TSCE card on the NCS 2006 shelf. The diagram provides information on the tasks required to install and configure the TNC/TSC/TNCE/TSCE card.

Figure 3: Control Card Workflow Diagram

Related Procedures for TNC and TNCE Cards

- NTP-G313 Installing and Configuring the TNC, TNCE, TSC, TSCE, TNCS, TNCS-O, TNCS-2, and TNCS-2O Card, on page 23
- NTP-G22 Verifying Common Card Installation
- NTP-G51 Verify DWDM Node Turn Up
- NTP-G103 Backing Up the Database
- NTP-G104 Restoring the Database
- NTP-G106 Resetting Cards Using CTC
- NTP-G280 Modifying Threshold Settings for the TNC and TNCE Cards
- NTP-G277 Provision Alarms and Controls on the TNC, TNCE, TSC, or TSCE Card
- NTP-G279 Monitor TNC and TNCE Card Performance
- NTP-G250 Verifying Digital Image Signing (DIS) Information

TSC and TSCE Cards

(Cisco NCS 2002 and Cisco NCS 2006)

The TSC or TSCE card is provisioned as active and standby in the NCS 2006 shelf, and as a stand-alone card in the NCS 2002 shelf. The TSC and TSCE card serves as the processor card for the shelf.

On the NCS 2006 shelf, install redundant TSC and TSCE cards in slots 1 and 8. If the active TSC or TSCE card fails, system traffic switches to the redundant TSC or TSCE card.

On the NCS 2002 shelf, install the stand-alone TSC and TSCE cards in slot 1. The TSC and TSCE card support line cards in slots 2 and 3.

The NCS 2006 shelf has dual power supply. The TSC and TSCE card monitors both supply voltage inputs on the NCS 2006 shelf. The TSC and TSCE card raises an alarm if one of the supply voltage inputs has a voltage out of the specified range.

You can insert and remove the TSC and TSCE card without impacting the system traffic, even when the system is online.

The TSC and TSCE card does not support optical service channel (OSC) and SFP ports.

Note The TNC, TNCE, TSC, and TSCE cards cannot be inserted in the same shelf.

The TSC and TSCE card is not supported on NCS 2015. When the card is inserted into the active or standby slots of the NCS 2015 chassis, the card does not start and become active.

For more information about the TSC and TSCE card, see http://www.cisco.com/en/US/prod/collateral/optical/ps5724/ps2006/data_sheet_c78-602903.html.

Related Procedures for TSC and TSCE Cards

- NTP-G22 Verifying Common Card Installation
- NTP-G51 Verify DWDM Node Turn Up
- NTP-G103 Backing Up the Database
- NTP-G104 Restoring the Database
- NTP-G106 Resetting Cards Using CTC
- NTP-G280 Modifying Threshold Settings for the TNC and TNCE Cards
- NTP-G279 Monitor TNC and TNCE Card Performance
- NTP-G250 Verifying Digital Image Signing (DIS) Information

TNCS Card

(NCS 2002, NCS 2006, NCS 2015)

The TNCS cards are provisioned as active and standby in the Cisco NCS 2002, NCS 2006, or NCS 2015 shelves. The TNCS cards serve as the processor card for the node.

On the NCS 2015 shelf, the TNCS cards can be installed in slots 1 and 17. On the NCS 2006 shelf, the cards can be installed in slots 1 and 8. On the NCS 2002 shelf, the card can be installed in slot 1. If the active TNCS card fails, system traffic switches to the redundant TNCS card.

The NCS 2015 shelf is powered by DC power modules with 3+1, 2+2, 2+1, or 1+1 redundancy. A minimum of one power module is required to turn up the chassis. The number of power modules to be connected is dependent on the chassis load. The TNCS cards raise an alarm if one of the supply voltage inputs has a voltage out of the specified range.

You can insert and remove the TNCS cards even when the system is online, without impacting the system traffic.

Note When a TNCS card provisioned with OC3/STM-1 or GIGE payloads is replaced with a TNCS-O card, the PROV-MISMATCH, RS-EOC, EOC-E and SIGLOSS alarms are raised due to incompatibility of the payloads provisioned on the TNCS card. FE is the only payload supported on the TNCS-O card.

Perform the following steps on the TNCS card before you replace a TNCS card with a TNCS-O card:

- Delete incompatible payloads (OC3/STM-1 or GIGE) on the TNCS card.
- Delete any synchronization service related to the OSC port.

For more information about the TNCS cards, see http://www.cisco.com/en/US/prod/collateral/optical/ps5724/ps2006/data_sheet_c78-602903.html.

TNCS-O Card

(NCS 2002, NCS 2006, NCS 2015)

The TNCS-O card is provisioned as active and standby in the Cisco NCS 2006 or NCS 2015 shelves. On the NCS 2015 shelf, the TNCS-O card can be installed in slots 1 and 17. On the NCS 2006 shelf, the card can be installed in slots 1 and 8. If the active TNCS-O card fails, the system switches to the redundant TNCS-O card.

Note The TNCS-O control card is not supported on a node that has ONS 15454 as node controller and NCS 2006 or NCS 2015 as subtending shelf controllers.

A TNCS-O card has an optical module that provides Optical Time Domain Reflectometer (OTDR) measurement, ORL measurement, and standard Optical Service Channel (OSC) capability on two ports. These capabilities are available on up to four ports for each shelf; a shelf can have two TNCS-O cards. OTDR scan and OSC transmission can run in parallel on different ports.

The TNCS-O cards support only Fast Ethernet (FE) and wavelength of 1518 nm in OSC transmissions.

Note OC-3 and ONE-GE payloads are not supported by the TNCS-O card.

The OTDR feature in the TNCS-O card lets you do the following:

- Inspect the transmission fiber.
- Identify discontinuities or defect on the fiber.
- Measure the distance and magnitude of defects like insertion loss, reflection loss, and so on.
- Monitor variations in scan values and configured threshold values periodically.

The OTDR measurement ranges are:

- Zone #1
- Zone #2
- Zone #3
- Zone #4
- Expert Mode
- Auto mode

The following table shows the OTDR performance in different operating ranges:

Operating Range	Distance Range [Km]	Distance Accuracy [m]	Loss Accuracy [dB]		Reflection Accuracy [dB]		Measurement Time [s]
			Typ.	W.C.	Typ.	W.C.	
Zone #1	0.001 - 1	+/- 1	+/- 0.2	+/- 2	3	4	180
Zone #2	0.001 - 25	+/- 2	+/- 0.2	+/- 2	2	4	180
Zone #3	0.001 - 80	+/- 10	+/- 0.5	+/- 2	1	4	180
Zone #4	0.001 - 100	+/- 20	+/- 0.5	+/- 2	1	4	180

The following table shows the maximum dynamic range of the TNCS-O OTDR in the different zones. The maximum dynamic range of the TNCS-O OTDR includes the total insertion loss, including the optical attenuation at the faceplate connector, not shown in the OTDR trace.

Operating Range	Max [dB]
Zone #1	2.5
Zone #2	8
Zone #3	17
Zone #4	21

The OSC transmission ranges are:

- Standard range: 12 - 43 dB
- Reduced range: 5 - 30 dB

Note The TNCS-O cards are not interoperable with TNC or TNCE cards. TNCS-O cards are interoperable only with a TNCS or another TNCS-O card over a fiber span. However, the OTDR functionality is available only if a TNCS-O card is connected to another TNCS-O card over a fiber span.

Note The OTDR feature of TNCS-O and TNCS-2O cards is not supported over DWDM network configuration having PSM card at the line side of booster amplifier. In this configuration, the PSM Working (W) and Protect (P) ports are connected to the fiber. The OTDR signal is split into both W and P fibers and back reflected light from both the fibers leads to inconsistent OTDR results.

For more information about the TNCS-O cards, see http://www.cisco.com/c/en/us/products/collateral/optical-networking/ons-15454-series-multiservice-transport-platforms/data_sheet_c78-602903.html.

Operating Modes for TNC, TNCE, TNCS, or TNCS-O cards

The control cards can be configured either in TNC or TNCO operating mode. The TNC mode is the default operating mode for the cards. A card is configured in TNCO mode if the actual card that is to be inserted into a shelf is a TNCS-O card.

Note The creation of OC-3 or ONE-GE payloads is rejected in the TNCO mode.

The PROV_MISMATCH alarm is raised in case of a provisioning mismatch. For more information on the PROV_MISMATCH alarm, see *Cisco NCS 2000 Series Troubleshooting Guide, Release 10.x.x*.

TNCS-2 and TNCS-2O Cards

(NCS 2002, NCS 2006, NCS 2015)

The TNCS-2 and TNCS-2O cards are provisioned as active in the NCS 2002 chassis, and as active and standby in the NCS 2006 or NCS 2015 chassis.

Note When the TNCS-2 or TNCS-2O control card is removed and re-inserted from the NCS 2002 chassis, the detection of fan-tray assembly (FTA) takes 5 to 7 minutes.

On the NCS 2015 shelf, the TNCS-2 and TNCS-2O cards can be installed in slots 1 and 17.

On the NCS 2006 shelf, the cards can be installed in slots 1 and 8.

On the NCS 2002 shelf, the cards can be installed in slot 1.

You can insert and remove the TNCS-2 and TNCS-2O cards without affecting the system traffic, even when the system is online.

The card has the following features:

- The TNCS-2 and the TNCS-2O cards work in redundant mode with another TNCS-2, TNCS-2O, TNCS, TNCSO, or TNCE cards.
- The TNCS-2 and the TNCS-2O cards can replace each other and the TNCS, TNCSO, or TNC-E cards in any NCS 2002, NCS 2006, or NCS 2015 chassis. When the TNCS, TNCSO, or TNCE cards are provisioned with the OC-3 payload and are being replaced by the TNCS-2/TNCS-2O card, the OC-3 payload provisioning has to be removed on the TNC-E/TNCS/TNCS-O card before replacing the card with the TNCS-2/TNCS-2O card.

Note When the TNCS-2/TNCS-2O card is replacing a pre-provisioned card with OC-3 payload on a chassis, the PROV-MISMATCH/MEA alarm is raised.

- The TNCS-2O has an optical module that performs Optical Time Domain Reflectometry (OTDR) functions with the internal module on two OSC ports 3, 4.
- Synchronous Ethernet is supported on all GE and FE ports of the TNCS-2 and the TNCS-2O cards.

- The TNCS-2 control card has OSC ports 1 and 2 available and the TNCS-2O has a total of four OSC ports available with FE and GE support. OC-3 support is not available on either of the cards.
- The TNCS-2 and TNCS-2O cards address CPU EOL and SDRAM supply issues on the existing controller cards.
- The TNCS-2 and the TNCS-2O cards supports a secure boot.
- The TNCS-2 and TNCS-2O cards exhibit chassis control functions including the control of power supplies, fans, ECU, optical modules, clock synchronization, and line card configuration. It can also configure the field programmable devices present in the TNCS-2 or TNCS-2O card.
- The TNCS-2 and TNCS-2O cards support environment monitoring and alarm reporting features.
- The TNCS-2 and TNCS-2O cards support multishelf management (MSM) as other control cards.
- The TNCS-2 or TNCS-2O cards can be inserted based on SSC into an existing MSM node with the node controller (NC) having one of TNCS, TNCS-O, TNCE, or TSCE control cards. The TNCS-2 card is supported on SSC to a NC having a TCC3 control card.

Note The TNCS-2O card is not supported on SSC to a NC having a TCC3 control card.

Note The TNCS-2 and TNCS-2O cards are not supported on the ONS 15454 chassis.

Note The TNCS-2 and TNCS-2O cards cannot be installed in the chassis that runs software earlier than R11.0.

- All packages are supported on the TNCS-2 and TNCS-2O cards.

The **Lamp Test** button is not available on the TNCS-2 and TNCS-2O cards.

Note When the EMS port is configured with 10 Mbps speed for TNCS-2 and TNCS-2O cards, it causes unicast storm control over the EMS peer port connected to the switch. However, when the storm controller is enabled on the EMS port for unicast packets on the switch, the EMS link goes down.

Table 6: The TNCS-2 and TNCS-2O cards support the following shelf control options:

Standby Slot	Active Slot	Support
TSC	TNCS-2O	Not Supported
TSC-E	TNCS-2O	Not Supported
TNC	TNCS-2O	Not Supported
TNC-E	TNCS-2O	Yes

Standby Slot	Active Slot	Support
TNCS	TNCS-2O	Yes
TNCS-O	TNCS-2O	Yes
TNCS-2	TNCS-2O	Yes
TSC	TNCS-2	Not Supported
TSC-E	TNCS-2	Not Supported
TNC	TNCS-2	Not Supported
TNC-E	TNCS-2	Yes
TNCS	TNCS-2	Yes
TNCS-O	TNCS-2	Yes
TNCS-2O	TNCS-2	Yes

Power Settings of TNCS-O and TNCS-2O OTDR Ports

OTDR ports of TNCS-O and TNCS-2O operate in two modes:

- High Power
- Low Power

These power changes occur based on the settings of the **Max Expected Span Loss** parameter. If the **Max Expected Span Loss** parameter is set to 28 dB or less, OTDR ports operate in low power and if the **Max Expected Span Loss** parameter is set to more then 28 dB, OTDR ports operate in high power.

After changing the value of **Max Expected Span Loss** parameter, you must perform **Launch ANS** from CTC as it is an ANS parameter.

Support for OTDR

Optical Time Domain Reflectometer (OTDR) is used to detect faults in an optical fiber link of a communication network. OTDR functionality is supported on TNCS-O and TNCS-2O control cards.

From Release 11.0, the OTDR functionality support is extended to NCS 2002.

The OTDR feature on the TNCS-O and TNCS-2O cards lets you do the following:

- Inspect the transmission fiber.
- Identify discontinuities or defect on the fiber.
- Measure the distance and magnitude of defects like insertion loss, reflection loss, and so on.
- Monitor variations in scan values and configured threshold values periodically.

The OTDR measurement ranges are:

- Zone #1

- Zone #2
- Zone #3
- Zone #4
- Expert Mode
- Auto mode

The following table shows the OTDR performance in different operating ranges:

Operating Range	Distance Range [Km]	Distance Accuracy [m]	Loss Accuracy [dB]		Reflection Accuracy [dB]		Measurement Time [s]
			Typ.	W.C.	Typ.	W.C.	
Zone #1	0.001 - 1	+/- 1	+/- 0.2	+/- 2	3	4	180
Zone #2	0.001 - 25	+/- 2	+/- 0.2	+/- 2	2	4	180
Zone #3	0.001 - 80	+/- 10	+/- 0.5	+/- 2	1	4	180
Zone #4	0.001 - 100	+/- 20	+/- 0.5	+/- 2	1	4	180

The following table shows the maximum dynamic range of OTDR in the different zones. The maximum dynamic range of OTDR includes the total insertion loss, including the optical attenuation at the faceplate connector, not shown in the OTDR trace.

Operating Range	Max [dB]
Zone #1	2.5
Zone #2	8
Zone #3	17
Zone #4	21

You can start a scan in auto mode requesting for the new reflection loss report or for both (legacy and new reflection loss reports). You can select, either the new loss reflection scan or normal scan. The TL1 command used for this operation is available here TL1 Command Guide.

Note The OTDR feature of TNCS-O and TNCS-2O cards is not supported over DWDM network configuration having PSM card at the line side of booster amplifier. In this configuration, the PSM Working (W) and Protect (P) ports are connected to the fiber. The OTDR signal is split into both W and P fibers and back reflected light from both the fibers leads to inconsistent OTDR results.

Note When an OTDR hybrid scan is initiated on the TNCS-2O card, UDC partial packet loss occurs while the scan is in progress. The UDC packet loss stops once the OTDR hybrid scan is completed.

OTDR Training

In R10.8, OTDR scan performances are improved using specific parameters of fiber plant such as span length, span loss, equipment insertion loss, reflection contributions, and major events on the fiber. This calibration operation is called OTDR training.

OTDR training is executed with the following rules.

- OTDR training is executed on both the Tx fiber and Rx fiber.
- OTDR training results are used to execute the composite scan.
- OTDR training is embedded in the scan operation.
- OTDR training takes up to 2 minutes in fast mode and up to 10 minutes in hybrid mode.
- OTDR training results in calibration file, fast span trace, and identification of fiber end.

Note High reflection location is not available if detected during ORL training.

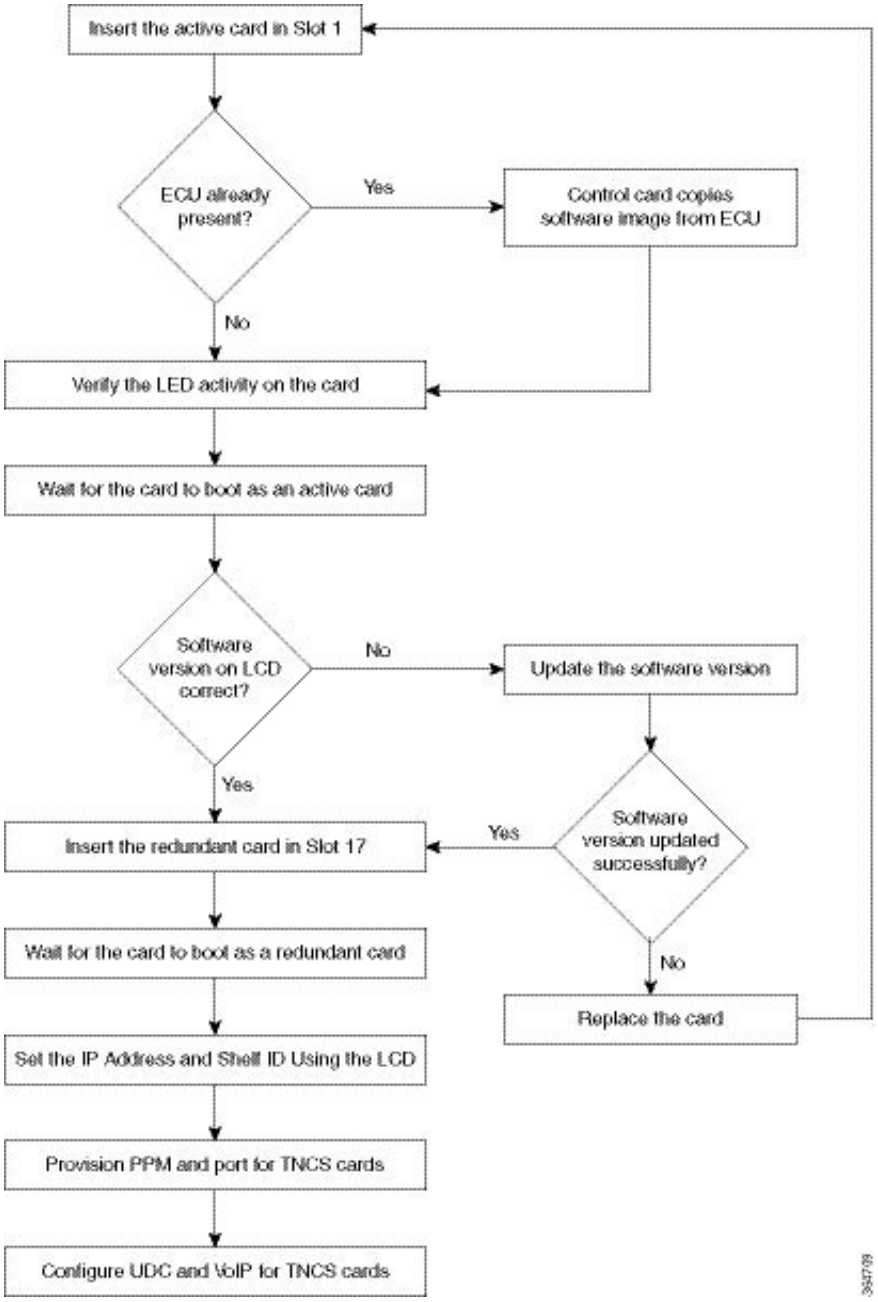
You can configure a periodic ORL training in the Rx direction, even for a single PPM. The TL1 command used for this operation is available here TL1 Command Guide.

Control Card Workflow Diagram

Note From Release 10.62 onwards, the new node must be connected to the laptop before node turn up.

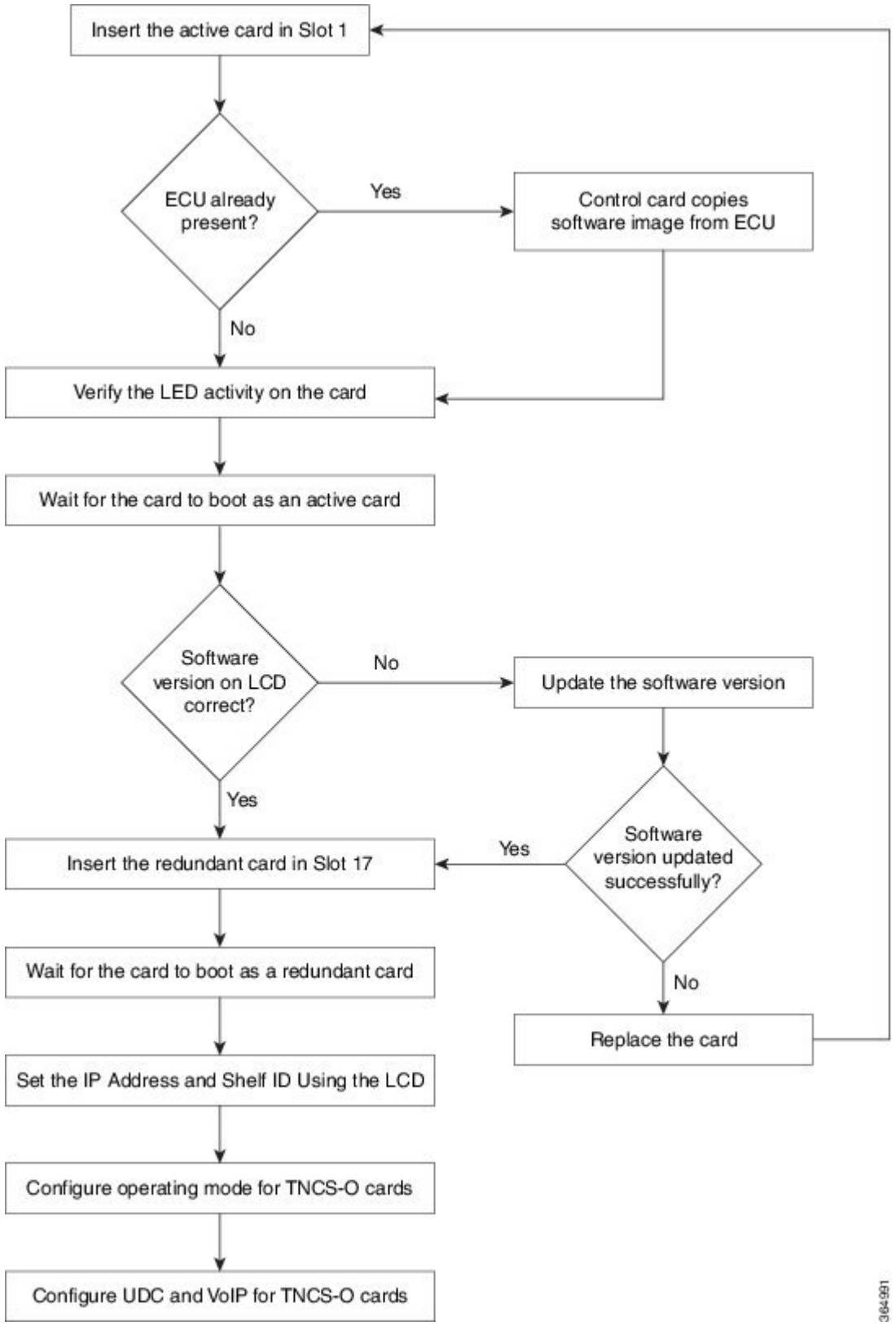
The following figure shows a workflow that describes the tasks required to install and configure the TNCS card.

Figure 4: TNCS Card Workflow



The following figure shows a workflow that describes the tasks required to install and configure the TNCS-O card.

Figure 5: TNCS-O Card Workflow


Insert the active card in Slot 1
ECU already present?
Yes
Control card copies software image from ECU
No
Verify the LED activity on the card
Wait for the card to boot as an active card
Software version on LCD correct?
No
Update the software version
Yes
Software version updated successfully?
Yes
Insert the redundant card in Slot 17
No
Replace the card
Wait for the card to boot as a redundant card
Set the IP Address and Shelf ID Using the LCD
Configure operating mode for TNCS-O cards
Configure UDC and VoIP for TNCS-O cards
364991

Related Procedures for TNCS and TNCS-O Cards

- NTP-G313 Installing and Configuring the TNC, TNCE, TSC, TSCE, TNCS, TNCS-O, TNCS-2, and TNCS-2O Card, on page 23
- NTP-G277 Provision Alarms and Controls on the TNC, TNCE, TNCS, TSC, or TSCE Card

Digital Image Signing

(Cisco NCS 2000 Series)

The DIS feature complies with the new U.S. Government Federal Information Processing Standard (FIPS) 140-3 to provide security for all software provided on the Cisco NCS 2000 Series platforms. This standard requires software to be digitally signed and verified for authenticity and integrity prior to load and execution.

DIS focuses on software security and provides increased protection from attacks and threats to Cisco NCS 2000 Series products. DIS verifies software integrity and provides assurance that the software has not been tampered with or modified. Digitally signed Cisco software provides counterfeit protection.

New controller cards, such as TNC/TNCE/TSC/TSCE/TNCS/TNCS-O, provide services that authenticate the origin of the software running on the Cisco NCS 2000 Series platforms.

DIS Identification

Digitally signed software can be identified by the last three characters appended to the working version and protected version field in CTC. The DIS conventions can be viewed under the working version displayed in the **Maintenance** > **Software** tab in CTC. For example, 9.2.0 (09.20-X10C-29.09-SDA) and 9.2.0 (09.20-010C-18.18-SPA).

The significance of the three characters appended to the software version is explained in the following table:

Character	Meaning
S (first character)	Indicates that the package is signed.
P or D (second character)	Production (P) or Development (D) image. • Production image—Software approved for general release. • Development image—development software provided under special conditions for limited use.
A (third character)	This third character indicates the version of the key used for signature generation. The version changes when a key is revoked and a new key is used. The values of the version key varies from A to Z.

Related Procedures for DIS

To verify DIS, see NTP-G250 Verifying Digital Image Signing (DIS) Information

Control Card Reset

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

You can apply a soft reset from CTC to either an active or standby control card without affecting traffic. If you need to perform a hard reset on an active control card, put the control card into standby mode first by performing a soft reset.

Note Hard reset can also be performed on the TNC/TNCE/TSC/TSCE/TNCS/TNCS-O card through CTC and TL1 interface. Before performing the hard reset, bring the TNC/TNCE/TSC/TSCE/TNCS/TNCS-O card to maintenance mode.

When you reset the standby control card, the system traffic is not affected. When you reset the active control card, traffic switches to the standby card if the standby card is present and in the ready standby state. If the standby card is not in the ready standby state, traffic does not switch, and results in loss of system traffic and management connectivity until the card reboots completely.

Caution When you reset the TNC/TNCE/TSC/TSCE card on the NCS 2002 or NCS 2006 shelf or the TNCS/TNCS-O card on the NCS 2006 or NCS 2015 shelf in simplex control mode (when the standby control card is not present), loss of management connectivity happens until the card reboots. The system traffic loss may occur depending on the line card and traffic type.

Control Card Database

When dual control cards are installed in the NCS 2000 Series shelf each control card hosts a separate database; therefore, the protect card database is available if the database on the working control card fails. You can also store a backup version of the database on the workstation running CTC. This operation should be part of a regular maintenance program at approximately weekly intervals, and should also be completed when preparing NCS 2000 Series for a pending natural disaster, such as a flood or fire. The configuration details are stored in the database of the control card. The database restore from a TNC and TNCE cards to a TSC and TSCE cards or vice versa is not supported.

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

NTP-G313 Installing and Configuring the TNC, TNCE, TSC, TSCE, TNCS, TNCS-O, TNCS-2, and TNCS-2O Card

Purpose	This procedure describes how to install and configure the TNC, TNCE, TSC, TSCE, or TNCS/TNCS-O/TNCS-2/TNCS-2O card.
Tools/Equipment	Redundant TNC/TNCE/TSC/TSCE/TNCS/TNCS-O/TNCS-2/TNCS-2O cards on NCS 2006 shelf (required) Stand-alone TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O/TNCS-O card on NCS 2002 shelf (required) Redundant TNCS/TNCS-O/TNCS-2/TNCS-2O cards on the NCS 2015 shelf.
Prerequisite Procedures	Install Power and Ground. See the Hardware Installation Guide.
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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 NCS 2000 Series shelf assemblies. For detailed instructions on how to wear the ESD wristband, refer to the *Electrostatic Discharge and Grounding Guide for Cisco NCS 2000 Series*.

Note If you install a card incorrectly, the FAIL LED flashes continuously.

Procedure

Step 1 Complete the DLP-G604 Installing the TNC, TNCE, TSC, TSCE, TNCS-2, TNCS-2O, TNCS-O, or TNCS Card, on page 24.

Step 2 Complete theDLP-G788 Configuring Operating Mode for the TNC, TNCE, TNCS, TNCS-O, TNCS-2, and TNCS-2O Cards, on page 31.

Step 3 Complete the DLP-G605 Provisioning PPM and Port for the TNC, TNCE, TNCS-2, TNCS-2O, and TNCS Cards, on page 29.

Step 4 Complete the DLP-G606 Configuring UDC and VoIP for the TNC, TNCE, TNCS-2, TNCS-2O, and TNCS/TNCS-O Cards, on page 30.

Step 5 Complete the DLP-G605 Provisioning PPM and Port for the TNC, TNCE, TNCS-2, TNCS-2O, and TNCS Cards, on page 29.

Note
Step 3, on page 23 and Step 5, on page 24 do not apply to TNCS-O cards.

Stop. You have completed this procedure.

DLP-G604 Installing the TNC, TNCE, TSC, TSCE, TNCS-2, TNCS-2O, TNCS-O, or TNCS Card

This task installs active and standby cards on the Cisco NCS 2006 or Cisco NCS 2015 shelf.

This task installs active and standby cards on the Cisco ONS 15454 M6 or Cisco NCS 2015 shelf.

Purpose	(Cisco NCS 2000 Series) This task installs two TNC/TNCE/TSC/TSCE/TNCS-2O/TNCS-2 cards on the NCS 2006 shelf, two TNCS/TNCS-O/TNCS-2/TNCS-2O cards on the NCS 2006 or NCS 2015 shelf, and a stand-alone TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O card on the NCS 2002 shelf. Install and initialize the TNC/TNCE/TSC/TSCE/TNCS/TNCS-2/TNCS-2O/TNCS-O card before installing any other line cards into the shelf assemblies. On the NCS 2006 shelf, install the TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O/TNCS/TNCS-O cards in slots 1 and 8 for redundancy. On the Cisco NCS 2015 shelf, install the TNCS/TNCS-O cards in slots 1 and 17 for redundancy. On the NCS 2002 shelf, install the stand-alone TNC/TNCE/TSC/TSCE/TNCS-2 card in slot 1.
Tools/Equipment	Two TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O/TNCS/TNCS-O cards for the NCS 2006 shelf, two TNCS/TNCS-2/TNCS-2O/TNCS-O cards for the Cisco NCS 2015 shelf, and one TNC/TNCE/TSC/TSCE/TNCS-2 card for the NCS 2002 shelf.
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note The NCS 2002 shelf supports stand-alone control cards such as TNC, TSC, TNCE, TNCS, TNCS-O, TNCS-2, TNCS-2O, or TSCE. During replacement or removal of the control card, ensure that the optical fibers are not disturbed. The fibers must be correctly routed in the retention feature mounted on the front side of the shelf.

Note Node discovery fails when the control card of a NCS 2002 node is replaced with a control card running a later software version because the NCS 2002 node loses it node IP and node name. However, there is no loss of traffic and the provisioning database.

Caution Do not remove the control cards during the software installation process, which is indicated by the alternate flashing of the FAIL and ACT/STBY LEDs. Removing the control cards during the software installation process corrupts the system memory.

Note Allow each control card to boot completely before installing the redundant control card.

Note You cannot insert the control cards in other slots due to mechanical constraints. To identify the card slot, match the symbol placed on the lower side of the card front panel with the symbol on the shelf.

Note The firmware upgrade of the OTDR functionality of the TNCS-O card might take up to 1 hour and 15 minutes, depending on the node configuration. An automatic retry mechanism is available in case of any issue during the upgrade. During the firmware upgrade, the TNCS-O card is fully functional except for the OTDR feature, which is not available until the completion of the firmware upgrade.

From Release 11.0, the firrmware upgrade of the OTDR functionality of the TNCS-2 and TNCS-2O cards might take 30 mins.

Procedure

Step 1 Open the latches or ejectors of the first control card that you will install.

Step 2 Use the latches or ejectors to firmly slide the card horizontally along the guide rails until the card plugs into the receptacle at the back of the slot (slot 1 or 8 in the NCS 2006 shelf, slot 1 or 17 in the NCS 2015 shelf, and slot 1 in the NCS 2002 shelf).

Note
The cards slide vertically in the NCS 2015 shelf.

Step 3 Verify that the card is inserted correctly, and close the latches or ejectors on the card.

If you insert a card into a slot assigned for a different card, all LEDs turn off.

Step 4 If needed, verify the LED activity on the control card.

- The red FAIL LED, PWR LED turn on briefly.
- The red FAIL LED turns on for about 10 seconds.

- The red FAIL LED and the amber ACT/STBY LED turn on for about 30 seconds.
- The red FAIL LED blinks for about 10 seconds.
- The red FAIL LED turns on for about 15 seconds.
- All the LEDs including the CRIT, MAJ, MIN, REM, SYNC, and ACO LEDs blink once and turn off for about 10 seconds.
- ACT/STBY LED blinks for about 1 second.
- All the LEDs including the CRIT, MAJ, MIN, REM, SYNC, and ACO LEDs turn off for about 10 seconds.
- The ACT/STBY, ACO, and PWR LEDs turn on.
- The boot process is complete when the PWR LEDs turn green and the amber ACT/STBY LED remains on. The ACT/STBY LED turns green if this is the first control card installed, but turns amber if this is the second control card installed.

Note
It might take up to four minutes for the power alarms to clear.

Note
Alarm LEDs might be on. After completing the control card installation, log in to CTC and click the Alarms tab to display the alarms raised on the card. For procedure to clear the alarm, see the Troubleshooting Guide.

Note
During the control card initialization, the SFTWDOWN alarm appears twice. The alarm clears after the control card boots completely.

Note
If the FAIL LED is on continuously, see the note in Step 8 about the control card automatic upload.

Figure 6: Installing TNC and TNCE Cards on the NCS 2006 Shelf

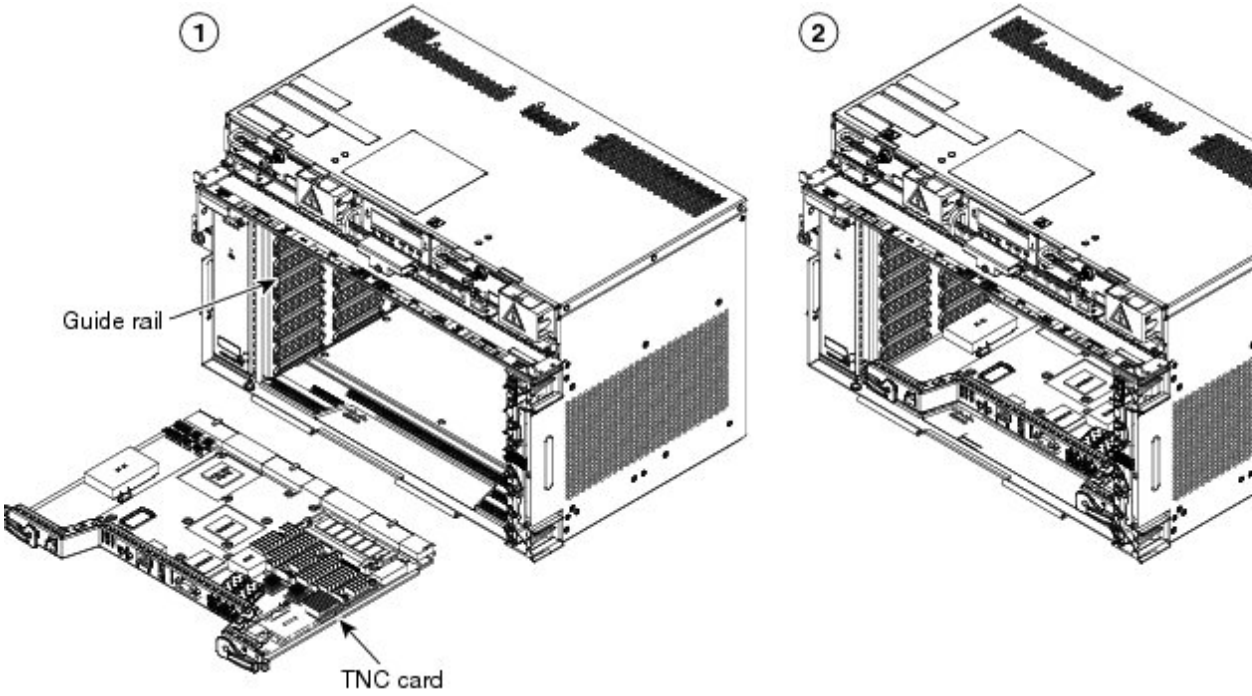
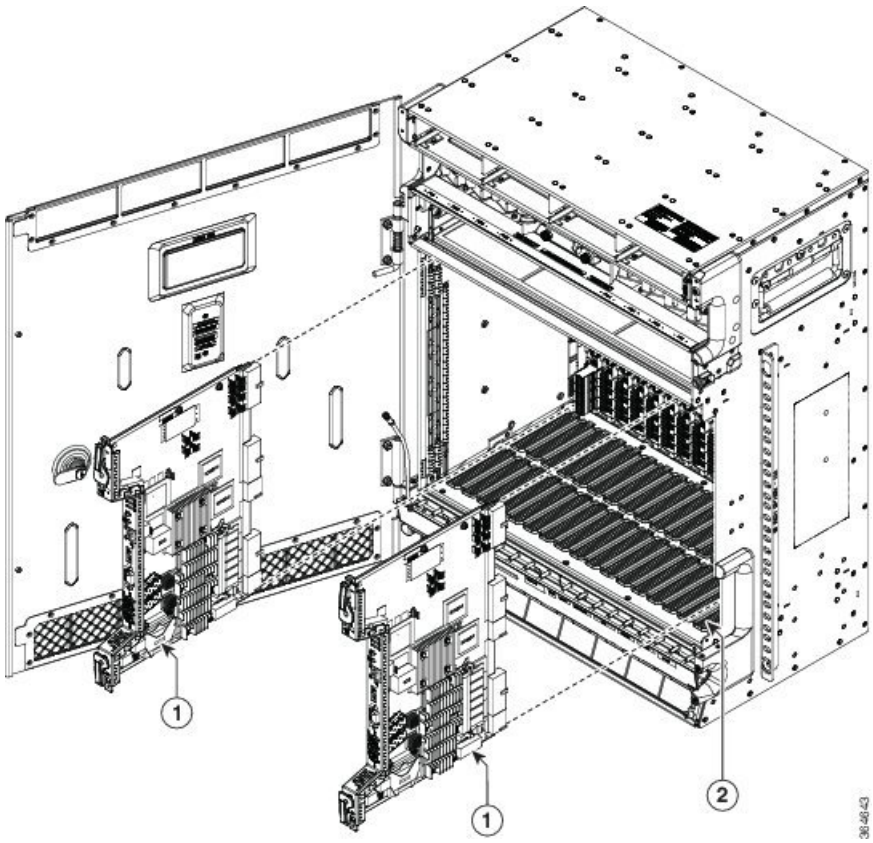


Figure 7: Installing TNCS/TNCS-O Cards on the NCS 2015 Shelf



1	TNCS/TNCS-O Card	2	Guide Rail

Step 5 Verify that the ACT/STBY LED is green if this is the first powered-up control card installed or amber if this is the second powered-up control card. The IP address, temperature of the node, and time of day appear on the LCD. The default time and date is 12:00 AM, January 1, 1970.

Step 6 The LCD cycles through the IP address (the default is 192.1.0.2), node name, and software version. Verify that the correct software version is shown on the LCD. The software text string indicates the node type (SDH or SONET) and software release. (For example: SDH 09.20-05L-20.10 indicates it is an SDH software load, Release 9.2. The numbers following the release number do not have any significance.)

Step 7 If the LCD shows the correct software version, continue with Step 8. If the LCD does not show the correct software version, refer to your next level of technical support, upgrade the software, or remove the control card and install a replacement card. Refer to the release-specific software upgrade document to replace the software.

Step 8 (NCS 2006 or NCS 2015 shelf only) Repeat Steps 1 through 7 for the redundant control card.

Note
If you install a standby control card that has a different software version than the active control card, the standby control card copies the software version from the one in the active control card. When the standby card is first inserted, the LEDs follow the normal boot-up sequence. However, after the red FAIL LED turns on for about 5 seconds, the FAIL LED and the ACT/STBY LED begin to flash alternately for up to 30 minutes. After loading the new software, the upgraded control cards LEDs repeat the appropriate bootup sequence, and the amber ACT/STBY LED turns on.

Step 9 Return to your originating procedure.

DLP-G605 Provisioning PPM and Port for the TNC, TNCE, TNCS-2, TNCS-2O, and TNCS Cards

Purpose	(Cisco NCS 2000 Series)This task provisions a PPM and port on TNC, TNCE, TNCS, TNCS-2, and TNCS-2O cards. PPMs are created to support the OSC function.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Note If the card in the shelf is configured in TNCO operating mode, PPM and port is automatically provisioned on the card.

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf view), double-click the TNC, TNCE, TNCS, TNCS-2, TNCS-2O, or TNCS-O cards where you want to provision PPM and port 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—Choose 1 or 2 from the PPM drop-down list.
- PPM Type—Displays the PPM associated with the chosen PPM in the above step.

Step 5 Click **OK**. The newly created PPM appears in the Pluggable Port Modules area. The row in the Pluggable Port Modules area becomes white when the PPM is inserted and the Actual Equipment Type column lists the name of PPM.

Step 6 In the Pluggable Ports area, click**Create** . The Create Port dialog box appears.

Step 7 In the Create Ports dialog box, complete the following:

- Port—Choose the port you want to configure from the Port drop-down list.
- Port Type—Choose the port type, such as OC-3, FE, or ONE-GE from the Port Type drop-down list.

Note

When changing the port type from OC-3 or FE, to ONE-GE is traffic affecting.

Note
The OC-3 port type is not supported on the TNCS-2 & TNCS-2O cards.

Note
OC-3 can be configured only on PPM port 1. FE and ONE-GE can be configured on both the ports. If the port type is FE, then disable ALS before provisioning OSC on that port.

Step 8 Click **OK**. The newly created port appears in the Pluggable Ports area. The port type you provisioned is listed in the Rate column.

Step 9 Repeat Steps 3 through 8 to provision another PPM and port on the TNC, TNCE, TNCS-2, TNCS-2O, or TNCS cards.

Step 10 Return to your originating procedure (NTP).

DLP-G606 Configuring UDC and VoIP for the TNC, TNCE, TNCS-2, TNCS-2O, and TNCS/TNCS-O Cards

Purpose	(Cisco NCS 2000 Series)This task configures UDC and VoIP traffic for the TNC, TNCE, TNCS-2, TNCS-2O, and TNCS/TNCS-O cards.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log into CTC • NTP-G38 Provisioning OSC Terminations • DLP-G605 Provisioning PPM and Port for the TNC, TNCE, TNCS-2, TNCS-2O, and TNCS Cards, on page 29
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Note LLDP traffic associated with specific MAC addresses is not passed across UDC.

Note Each TNC, TNCE, TNCS-2, TNCS-2O, and TNCS/TNCS-O card supports UDC/VoIP configuration. You can configure UDC or VoIP on the two SFP ports present on the TNC, TNCE, TNCS-2, TNCS-2O, and TNCS cards. The TNC, TNCE, TNCS-2, TNCS-2O, and TNCS cards support the UDC/VoIP configuration only when OSC is provisioned on the SFP ports.

Note If two nodes are connected through the fiber and if the TNC, TNCE, TNCS-2, TNCS-2O, and TNCS/TNCS-O cards in one node have UDC configuration, the TNC, TNCE, TNCS-2, TNCS-2O, and TNCS/TNCS-O cards in the other node must also have UDC configuration. The same rule applies to VoIP configuration.

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf view), double-click the TNC, TNCE, TNCS, TNCS-2, TNCS-2O, or TNCS-O cards where you want to configure UDC and VoIP.

Step 2 Click the **Provisioning** > **UDC / VOIP** tabs.

Step 3 From the Service Type drop-down list, choose UDC or VOIP.

Note
You can configure UDC or VoIP on only one SFP port at a time per TNC, TNCE, TNCS-2, TNCS-2O, or TNCS card. If you want to configure UDC or VoIP on the second SFP port, choose NONE from the Service Type drop-down list for the first port and then choose UDC or VoIP for the second port.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-G788 Configuring Operating Mode for the TNC, TNCE, TNCS, TNCS-O, TNCS-2, and TNCS-2O Cards

Purpose	(Cisco NCS 2000 Series)This task configures the operating mode for the TNC, TNCE, TNCS, and TNCS-O cards.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log in to CTC
Required/As Needed	As Needed
Onsite/Remote	Onsite or Remote
Security Level	None

The TNC mode supports the TNC, TNC-E and TNCS cards, the TNCS-O mode supports only the TNCS-O card, and no card mode supports the TSC and TSC-E cards.

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf view), double-click the control card where you want to configure the card mode.

Step 2 Click **Provisioning** > **Card** tab.

Step 3 From the Mode drop-down list, choose TNC or TNCO.

Note
The card is configured to TNC mode by default.

Note
If the actual card to be inserted is TNCS-O card, configure the card in TNCO mode.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-G774 Changing the Frame Type on the OSC

Purpose	This task changes the frame type on the OSC.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Note TNCS-O cards support only FE payload. Hence, OSC payload cannot be changed on TNCS-O cards.

Procedure

Step 1 Delete the OC-3, STM1, FE, or ONE_GE OSC communication channel. See DLP-G186 Delete an OSC Termination.

Step 2 Click **Provisioning** > **WDM-ANS** > **Internal Patchcords**.

Step 3 Choose the internal patchcord that is associated with OSC and click **Delete**.

Step 4 Delete the OSC payload on the TNC/TNCE/TNCS-2/TNCS-2O/TNCS card.

a) In node view (single-shelf mode) or shelf view (multishelf view), double-click the TNC/TNCE/TNCS card where you want to delete the OSC payload.

b) Click the **Provisioning** > **Pluggable Port Modules** tabs.
c) In the Pluggable Ports area, choose the OSC payload that you want to delete and click **Delete**.

Step 5 Provision the OSC payload on the TNC/TNCE/TNCS-2/TNCS-2O/TNCS card. See DLP-G605 Provisioning PPM and Port for the TNC, TNCE, and TNCS Cards.

Note
OC-3/STM1 can be configured only on port 1. FE and ONE-GE can be configured on both the ports.

Step 6 Provision the internal patchcord from the OSC on the TNC/TNCE/TNCS/TNCS-2/TNCS-2O card to the corresponding line card. See Virtual Patchcords.

Step 7 Provision the OSC communication channel. See NTP-G38 Provisioning OSC Terminations.

Step 8 Repeat the above steps for the other node.

Step 9 Return to your originating procedure (NTP).

Accessing and Configuring the Controller Cards Using Link-Local Address

Table 7: Feature History

Feature Name	Release Information	Feature Description
Accessing the Controller Cards using Link-Local Address	Cisco NCS 2000 Release 11.13	You can now use the link-local subnet address to access and configure the controller cards. This approach is helpful when you do not have admin privileges to the laptop through which the controller card is configured. Ensure that the controller card and the laptop are on the same subnet.

This topic describes how to access controller cards in factory mode with link-local subnet IP address (169.254.0.2) when you don't have administrative access to the laptop to configure the controller cards using the default IP address (192.1.0.2).

Procedure

Step 1 Disable the Wi-Fi connection on your laptop.

Step 2 Check and ensure that NCS 2000 is in default factory mode.

Step 3 Connect the laptop ethernet port to either the controller card front port, the ECU EMS port, or the ECU craft port which enables the laptop OS (Windows, Mac, or Linux) to assign the IP address (169.254.0.2) in the link-local subnet.

Note
The initial DHCP discovery phase run by the laptop will fail because the controller card does not support it.

Step 4 Ping the link-local address in the Command Prompt to verify the connectivity between NCS 2000 and the laptop.

Step 5 Use the default username and password values to log into CTC for NCS2000.

Step 6 After logging in, **Change Password** dialog box prompts you to change the password.

Step 7 Change the password for your Username:

a) Enter the old password in the **Old Password** field.
b) Enter the new password in the **New Password** and **Confirmation New Password** fields.
c) Check the **Change password in all other nodes in the background check box**.
d) Select the required Applicable Nodes from the list.
e) Click **OK**.

Step 8 In the node view (single-shelf mode) or multishelf view (multishelf mode), click the **Maintenance** > **Database** tabs.

Step 9 Click **Rebuild DB** and click **Yes** on the dialog box to exit from the factory mode.

Step 10 In the node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Network** > **General** tabs.

Step 11 Configure the new IP address:

a) Enter the IP address in the **Node Address** field.
b) Enter the subnet mask in the **Net/Subnet Mask Length** field.
c) Enter the gateway address in the **Default Router** field.
d) Click **Apply**.

NCS 2000 reboots to activate the new IP address.

Step 12 Disconnect the ethernet.

Step 13 Connect NCS 2000 to the site LAN using the EMS port.

Step 14 Enable the Wi-Fi connect on your laptop, and verify that the NCS 2000 chassis is correctly managed locally and remotely using the assigned IP address.

Step 15 The remote admin can now start deployment of the node.

NTP-G278 Upgrade an Older Controller Card to a Newer Controller Card

Purpose	This procedure upgrades an older controller card to a newer controller card. See the #unique_36 to upgrade the TNCS Card to TNCS-O Card.
Tools/Equipment	Two TSCE/TNC/TNCE/TNCS/TNCS-O (Two of the new controller cards to be used as active and standby cards.)
Prerequisite Procedures	"DLP-G46 Log into CTC" in the "Connect the PC and Log into the GUI" document.

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

The table below lists the matrix of the controller cards that can be upgraded.

Card	New Card
TSC	TSC-E
	TNC
	TNC-E
	TNCS
	TNCS-O
TSC-E	TNC
	TNC-E
	TNCS
	TNCS-O
TNC	TNC-E
	TNCS
	TNCS-O
TNC-E	TNCS
	TNCS-O
TNCS	TNCS-O

Note Downgrade procedures from a newer controller card to older controller card are not supported. Log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Note If the old controller is TNC/TNC-E/TNCS and you want to upgrade to TNCS-O, the old controller cards should be provisioned only with an FE payload on both the PPM ports. If the TNC/TNC-E/TNCS controller card has a different payload provisioned such as OC-3/1GIGE, you must delete the OSC, payload, and the PPM.

This procedure also applies to TSC/TNC/TSC-E/TNC-E upgrades to the TNCS/TNCS-O card for an M6 shelf.

Before you begin

- M2 supports only TSC, TSC-E, TNC, TNC-E, TNCS, TNCS-2, TNCS-2O, and TNCS-O controller cards.
- M6 supports only TSC, TSC-E, TNC, TNC-E, TNCS,TNCS-2, TNCS-2O, and TNCS-O controller cards.
- M15 supports only TNCS, TNCS-2, TNCS-2O, and TNCS-O controller cards.

Procedure

Step 1 Verify that the node you are upgrading has R 10.x.x/ R11.0 installed. The software version is displayed in the upper left corner of the window.

Step 2 Back up the database before beginning the upgrade.

Step 3 Physically replace the standby older controller card with the newer controller card. task

a) Check the LED on the faceplate. The ACT/STBY LED on the faceplate of the controller card indicates whether the card is in active or standby mode. A green ACT/STBY LED indicates an active card and an amber light indicates a standby card.
b) Open the ejectors on the standby old controller card.
c) Slide the card out of the slot. This raises the IMPROPRMVL alarm, which clears when the upgrade is complete.
d) Right-click the slot from which the old controller card was ejected out.
e) Click **Delete Card** to delete the old controller card from CTC.

Note
If the old controller card is not deleted from the CTC shelf view before inserting the new controller card, the MEA (card mismatch) alarm appears on that slot.

f) Open the ejectors on the new controller card to be installed.
g) Slide the new controller card into the slot along the guide rails.
h) Close the ejectors.
i) In CTC node view, Ldg (loading) appears on the newly installed controller card.

Note
It takes approximately 10 minutes for the active old controller card to copy the system software and database to the newly installed controller card. During this operation, the LEDs on the new controller card flash Fail and then the active/standby LED flashes. When the transfer completes, the new controller card reboots and goes into standby mode after approximately three minutes. Do not remove the card from the shelf during a database transfer.

Caution
If your active old controller card resets during the upgrade before the new controller card is in full standby mode, remove the new controller card immediately.

Step 4 When the newly installed controller card is in standby, right-click the active old controller card in CTC.

Step 5 From the pull-down menu, click **Reset Card**.

Wait for the old controller card to reboot. The standby new controller card is switched to active mode. The old controller card verifies that it has the same database as the new controller card and then switches to standby.

Step 6 Verify that the remaining old controller card is now in standby mode (the ACT/STBY LED changes to amber).

Step 7 Physically replace the remaining old controller card with the second new controller card.

a) Open the ejectors on the old controller card.
b) Slide the card out of the slot. This raises the IMPROPRMVL alarm, which clears when the upgrade is complete.
c) Right-click the slot from which the old controller card was ejected out.
d) Click **Delete Card** to delete the old controller card from CTC.

   If the old controller card is not deleted from the CTC shelf view before inserting the TNC card, the MEA (card mismatch) alarm appears on that slot.

e) Open the ejectors on the new controller card.
f) Slide the new controller card into the slot along the guide rails.
g) Close the ejectors.

The second new controller card boots up. The second new controller card must also copy the database. Do not remove the card from the shelf during a database transfer.

Step 8 If power-related alarms occur after the second new controller card is installed, check the voltage on the RJ-45 LAN port. Refer to the troubleshooting guide for information on clearing the alarms.

Stop. You have completed this procedure.

LCD or ECU Hot Plug-In

Purpose	This procedure upgrades or downgrades the LCD or ECU (in case of NCS 2015) inserted into a node.
Tools/Equipment	One LCD (incase of NCS 2006) or ECU (in case of NCS 2015) having a USB device with Release 11.0 and one LCD (incase of NCS 2006) or ECU (in case of NCS 2015) having a USB device with Release prior to 11.0.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Before you begin

The following procedure is applicable on the NCS 2006 and NCS 2015 chassis. These scenarios apply to the LCD in case of the NCS 2006 and the ECU in case of the NCS 2015.

Note In the case, the user is unaware of the Release version of the LCD or ECU being plugged-in into the chassis, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call TAC (1 800 553-2447).

Insert an LCD/ECU of Release prior to 11.0 in a Release 11.0 Chassis

Procedure

Step 1 Ensure the LCD/ECU present in the chassis is of Release 11.0.

Step 2 Eject the LCD/ECU operating with Release 11.0 from the chassis.

Step 3 Insert the new LCD/ECU with a Release prior to 11.0. The USBSYNC alarm is raised indicating the USB Sync procedure. Wait for USBSYNC alarm to clear.

Stop. You have completed this procedure.

Insert an LCD/ECU of Release 11.0 in a Release prior to 11.0 Chassis

Caution When an LCD or ECU of release 11.0 onwards is inserted into a chasis with a release prior to 11.0, the downgrade of LCD to release prior to 11.0 will not be successful and the node will reboot. The chassis will not be in a usable condition.

Note

- For NCS 2006 platform, this scenario is applicable only for LCD module.
- For NCS 2015 platform, this scenario is applicable only for ECU module. (as for NCS 2015 platform, the USB is on ECU)

In this case, follow the below steps to make the chassis usable:

Procedure

Step 1 Ensure the LCD or ECU present in the chassis is with release 11.0 onwards and the USB sync is complete.

Wait, if the USB sync is not complete.

Step 2 Download any release prior to release 11.0 into the protect partition on the node and follow the NCS 2000 downgrade process steps.

The LCD or ECU gets formatted with the dosFs1.0 file system after you complete the downgrade process. The LCD or ECU is now ready to be inserted in any chassis running prior to release 11.0.

Note
In case of any help, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call TAC (1 800 553-2447).

Upgrade the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O Card to the TNCS-2 or TNCS-2O Card

Purpose	This procedure upgrades the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card to the TNCS-2 or TNCS-2O card.
Tools/Equipment	Two TNCS-2/TNCS-2O cards.
Prerequisite Procedures	"DLP-G46 Log into CTC" in the Connect the PC and Log into the GUI document. "NTP-U488 Back Up the Cisco NCS Software Database" "DLP-U546 Download the NCS Software" "DLP-U548 Activate the New Cisco NCS Software" "NTP-U489 Upgrade the Cisco NCS 2000 Software" Access the above procedures in the Cisco NCS 2000 Series Upgrade Guide document.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Caution Please make sure that the LCD/ECU are plugged-in and then proceed. The USB is located in the LCD module in NCS 2006 and ECU module in NCS 2015. Do not pull-out any of the above mentioned devices while performing upgrade procedure. It is not recommended to initiate any card replacement procedure without the LCD/ECU.

Upgrade as needed:

Dual Shelf Control - Upgrade the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O Card to the TNCS-2 or TNCS-2O Cards

A dual shelf control scenario is when a Cisco NCS 2006 or Cisco NCS 2015 has two operating Control Cards on the chassis, one in active mode and one in standby mode. In this case, both the standby and active cards are upgraded to the TNCS-2 or TNCS-2O cards.

Procedure

Step 1 Verify that the node you are upgrading has R 11.0 installed. The software version is displayed in the upper left corner of the window.

Step 2 Back up the database before beginning the upgrade. https://www.cisco.com/c/en/us/td/docs/optical/15000r10_0/ncs/network_config/guide/b_ncs_network_configuration/b_ncs_network_configuration_chapter_010000.html#ID17_backupdatabase

Step 3 Physically replace the standby TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with the TNCS-2/TNCS-2O card

Note
It takes approximately 10 minutes for the active TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card to copy the system software and database to the TNCS-2 or TNCS-2O card. During this operation, the LEDs on the TNCS-2 or TNCS-2O card flash Fail and then the active/standby LED flashes. When the transfer completes, the new control card reboots and goes into standby mode after approximately three minutes. Do not remove the card from the shelf during a database transfer.

a) Check the LED on the faceplate. The ACT/STBY LED on the faceplate of the control card indicates whether the card is in active or standby mode. A green ACT/STBY LED indicates an active card and an amber light indicates a standby card.
b) Open the ejectors on the standby old control card.
c) Slide the card out of the slot. This raises the IMPROPRMVL alarm, which clears when the upgrade is complete.
d) Right-click the slot from which the old control card was ejected out.
e) Click **Delete Card** to delete the old control card from CTC.

Note
If the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card is not deleted from the CTC shelf view before inserting the TNCS-2/TNCS-2O card, the PROV-MISMATCH/MEA (card mismatch) alarm appears on that slot.

The following table shows the services that must be deleted on the old control card before replacement.

Table 8: Deletion of Services on the Old Control Card

Old Control Card	Services	New Control Card
TNC, TNC-E, TNCS	OC3 payload	TNCS-2
TNCSO	OTDR port provisioning	TNCS-2
TSC and TSC-E	Provisioning	TNCS-2

Old Control Card	Services	New Control Card
TSC, TSCE, TNC, TNC-E, TNCS, TNCSO	All services	TNCS-2O

f) Open the ejectors on the TNCS-2/TNCS-2O card to be installed.
g) Slide the card into the slot along the guide rails.
h) Close the ejectors.
i) In CTC node view, Ldg (loading) appears on the newly installed TNCS-2/TNCS-2O card.

Caution
If your active TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card resets during the upgrade before the TNCS-2/TNCS-2O control card is in full standby mode, remove the TNCS-2 or TNCS-2O card immediately.

Step 4 When the newly installed TNCS-2/TNCS-2O card is in standby, right-click the active TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card in CTC.

Step 5 From the pull-down menu, click **Reset Card**.

Wait for the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card to reboot. The new standby TNCS-2/TNCS-2O card is switched to active mode. The TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card verifies that it has the same database as the TNCS-2 or TNCS-2O card and then switches to standby.

Step 6 Verify that the remaining TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card is now in standby mode (the ACT/STBY LED changes to amber).

Step 7 Physically replace the remaining TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with the second TNCS-2/TNCS-2O card.

a) Open the ejectors on the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card.
b) Slide the card out of the slot. This raises the IMPROPRMVL alarm, which clears when the upgrade is complete.
c) Right-click the slot from which the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card was ejected out.
d) Click **Delete Card** to delete the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card from CTC.

   If the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card is not deleted from the CTC shelf view before inserting the TNCS-2 or TNCS-2O card, the IMPROV-MISMATCH/MEA (card mismatch) alarm appears on that slot. The MEA alarm can be cleared by resetting the configuration to factory defaults.

e) Open the ejectors on the TNCS-2/TNCS-2O card.
f) Slide the TNCS-2/TNCS-2O card into the slot along the guide rails.
g) Close the ejectors.

The TNCS-2/TNCS-2O card boots up. The TNCS-2/TNCS-2O card must also copy the database. Do not remove the card from the shelf during a database transfer.

Step 8 If power-related alarms occur after the second TNCS-2 or TNCS-2O card is installed, refer to the troubleshooting guide for information on clearing the alarms.

Stop. You have completed this procedure.

Dual Shelf Control - Upgrade Control Card to TNCS-2 or TNCS-2O Card

A dual shelf control scenario is when a Cisco NCS 2006 or Cisco NCS 2015 has two operating Control Cards on the chassis. In this case, only the standby control card is upgraded to the TNCS-2 or TNCS-2O card.

Procedure

Step 1 Verify that the node you are upgrading has R 11.0 installed. The software version is displayed in the upper left corner of the window.

Step 2 Back up the database before beginning the upgrade. https://www.cisco.com/c/en/us/td/docs/optical/15000r10_0/ncs/network_config/guide/b_ncs_network_configuration/b_ncs_network_configuration_chapter_010000.html#ID17_backupdatabase

Step 3 Perform steps 3 to 6 from Dual Shelf Control - Upgrade the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O Card to the TNCS-2 or TNCS-2O Cards, on page 40 to upgrade the standby TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with the TNCS-2/TNCS-2O card.

Note
On a dual shelf controller, the TNCS-2 and TNCS-2O cards are only compatible to function with the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O control cards.

Stop. You have completed this procedure.

Single Shelf Control - Upgrade Control Card to TNCS-2 or TNCS-2O Card

A single shelf control scenario is where a control card is inserted in slot 1 or 8 of the NCS 2006 and slot 1 or 17 of the NCS 2015, the other slot is installed with a filler card.

Procedure

Step 1 Verify that the node you are upgrading has R 11.x.x installed. The software version is displayed in the upper left corner of the window.

Step 2 Back up the database before beginning the upgrade. https://www.cisco.com/c/en/us/td/docs/optical/15000r10_0/ncs/network_config/guide/b_ncs_network_configuration/b_ncs_network_configuration_chapter_010000.html#ID17_backupdatabase

Step 3 Physically replace the active TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with the TNCS-2/TNCS-2O card.

a) Check the LED on the faceplate. The ACT/STBY LED on the faceplate of the control card indicates whether the card is in active or standby mode. A green ACT/STBY LED indicates an active card and an amber light indicates a standby card.
b) Open the ejectors on the active TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card.
c) Slide the card out of the slot. This raises the IMPROPRMVL alarm, which clears when the upgrade is complete.
d) Right-click the slot from which the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card was ejected out.
e) Click **Delete Card** to delete the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card from CTC.

Note
If the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card is not deleted from the CTC shelf view before inserting the TNCS-2/TNCS-2O card, the PROV-MISMATCH/MEA (card mismatch) alarm appears on that slot. The complete provisioning database will be lost on clearing the MEA alarm. The backed up database has to be restored after the MEA alarm clears.

Specific services must be deleted on the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O cards before upgrading to TNCS2 and TNCS2O cards. For more information, see Table 8: Deletion of Services on the Old Control Card, on page 40.

Caution
Replacing the Active Control Card on the node is service-affecting.

f) Open the ejectors on the TNCS-2/TNCS-2O card to be installed.
g) Slide the card into the slot along the guide rails.
h) Close the ejectors.
i) In CTC node view, Ldg (loading) appears on the TNCS-2 or TNCS-2O control card.

Step 4 When the installed TNCS-2/TNCS-2O card is in active mode, wait for control card to sync from the USB successfully. This indicates that the chassis is upgraded with Release 11.00 and corresponding database.

Stop. You have completed this procedure.

Single Shelf Control - Upgrade Control Card with Release 11.0

A single shelf control scenario is where a control card is inserted in slot 1 or 8 of the NCS 2006 and slot 1 or 17 of the NCS 2015, the other slot is installed with a filler card. In this case, the active control card of a release prior to Release 11.0 is upgraded with another control card with Release 11.0 and the other slot is installed with a filler card.

Procedure

Step 1 Verify that the node you are upgrading has a Release prior to R 11.0 installed. The software version is displayed in the upper left corner of the window.

Step 2 Back up the database before beginning the downgrade. https://www.cisco.com/c/en/us/td/docs/optical/15000r10_0/ncs/network_config/guide/b_ncs_network_configuration/b_ncs_network_configuration_chapter_010000.html#ID17_backupdatabase

Step 3 Physically remove the active TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version prior to Release 11.0 and replace the card with the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version Release 11.0.

Note
When the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with a software version prior to Release 11.0 is to be replaced with another TNC, TSC, TSC-E, TNC-E, TNCS, TNCS-2, TNCS-2O, or TNCS-O card with a software version Release 11.0, upgrade the existing node with the TNC, TSC, TSC-E, TNC-E, TNCS, TNCS-2, TNCS-2O, or TNCS-O card with a software version Release 11.0.

Note

In NCS 2002 node with one control card, NCS 2006 and NCS 2015 nodes with one control card and filler card, replace the existing simplex control card running prior to R11.0 with another control card running prior to R11.0. If the existing simplex control card running prior to R11.0 is replaced with a R11.0 or higher control card, the node database and traffic becomes affected. This issue does not arise when replacing a standby control card with a spare card.

Note
Replacing the Active Control Card on the node has an impact on traffic.

Step 4 Sync the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version prior to Release 11.0 to USB. The USBSYNC alarm clears.

a) Open the ejectors on the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version prior to Release 11.0.
b) Slide the card out of the slot. This raises the IMPROPRMVL alarm, which clears when the upgrade is complete.
c) Right-click the slot from which the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version prior to Release 11.0 was ejected out.
d) Click **Delete Card** to delete the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version prior to Release 11.0 from CTC.

   If the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version prior to Release 11.0 is not deleted from the CTC shelf view before inserting the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version Release 11.0, the IMPROV-MISMATCH/MEA (card mismatch) alarm appears on that slot.

   Specific services must be deleted on the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O cards before upgrading to TNCS2 and TNCS2O cards. For more information, see Table 8: Deletion of Services on the Old Control Card, on page 40.

e) Open the ejectors on the TNC, TSC, TSC-E, TNC-E, TNCS, TNCS-2, TNCS-2O, or TNCS-O card with software version Release 11.0.
f) Slide the TNC, TSC, TSC-E, TNC-E, TNCS, TNCS-2, TNCS-2O, or TNCS-O card with software version Release 11.0 into the slot along the guide rails.
g) Close the ejectors.

Step 5 The sync of the TNC, TSC, TSC-E, TNC-E, TNCS, TNCS-2, TNCS-2O, or TNCS-O card with software version Release 11.0 to USB begins automatically. The USBSYNC alarm clears.

The node is active with the database that is available in the new control card.

Stop. You have completed this procedure.

Downgrade the TNCS-2 and TNCS-2O Cards to TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O Cards

Purpose	This procedure downgrades a TNCS-2 or TNCS-2O card to the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card.

Tools/Equipment	Two TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O cards.
Prerequisite Procedures	"DLP-G46 Log into CTC" in the "Connect the PC and Log into the GUI" document. "NTP-U491 Restore the Previous Software Load and Database" "NTP-U488 Back Up the Cisco NCS Software Database" Access the above procedures in the Cisco NCS 2000 Series Upgrade Guide document.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Caution Please make sure the LCD/ECU are all plugged-in and then proceed. The USB is located in the LCD module in NCS 2006 and ECU module in NCS 2015. Do not pull-out any of the mentioned devices while performing revert procedure. If the USB is inserted after the revert procedure, then it needs to be formatted manually. It is not recommended to initiate any card replacement procedure without the LCD/ECU.

Downgrade as needed:

Procedure

Dual Shelf Control - Downgrade Control Cards to TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O Card

Procedure

Step 1 Verify that the node you are downgrading has Release 11.0 installed. The software version is displayed in the upper left corner of the window.

Step 2 Back up the database before beginning the downgrade. https://www.cisco.com/c/en/us/td/docs/optical/15000r10_0/ncs/network_config/guide/b_ncs_network_configuration/b_ncs_network_configuration_chapter_010000.html#ID17_backupdatabase

Step 3 Physically replace the standby TNCS-2/TNCS-2O control card with the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with Release prior to 11.0.

Note
It takes approximately 10 minutes for the active TNCS-2/TNCS-2O card to copy the system software and database to the newly installed controller card. During this operation, the LEDs on the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card flash Fail and then the active/standby LED flashes. When the transfer completes, the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card reboots and goes into standby mode after approximately three minutes. Do not remove the card from the shelf during a database transfer.

a) Check the LED on the faceplate. The ACT/STBY LED on the faceplate of the controller card indicates whether the card is in active or standby mode. A green ACT/STBY LED indicates an active card and an amber light indicates a standby card.
b) Open the ejectors on the standby old control card.
c) Slide the card out of the slot. This raises the IMPROPRMVL alarm, which clears when the upgrade is complete.
d) Right-click the slot from which the old control card was ejected out.
e) Click **Delete Card** to delete the old control card from CTC.

Note
If the TNCS-2/TNCS-2O card is not deleted from the CTC shelf view before inserting the TNC-E/TNCS/TNCS-O card, the PROV-MISMATCH/MEA (card mismatch) alarm appears on that slot.

Specific Services must be deleted on the TNC, TSC, TSC-E, TNC-E, TNCS or TNCS-O cards before upgrading to TNCS2 and TNCS2O cards.

Table 9: Deletion of Services on the New Control Card

New Control Card	Services	Old Control Card
TNCS-2	OC3 payload	TNC, TNC-E, TNCS
TNCS-2	OTDR port provisioning	TNCSO
TNCS-2	Provisioning	TSC and TSC-E
TNCS-2O	All services	TNC, TSC, TSCE, TNC, TNC-E, TNCS, TNCSO

f) Open the ejectors on the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card to be installed.
g) Slide the card into the slot along the guide rails.
h) Close the ejectors.
i) In CTC node view, Ldg (loading) appears on the newly installed controller card.

Caution
If your active TNCS-2/TNCS-2O card resets during the upgrade before the new controller card is in full standby mode, remove the new controller card immediately.

Step 4 When the newly installed TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card is in standby, right-click the active TNCS-2/TNCS-2O card in CTC.

Step 5 From the pull-down menu, click **Reset Card**.

Wait for the TNCS-2/TNCS-2O card to reboot. The new standby TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card is switched to active mode. The old TNCS-2/TNCS-2O card verifies that it has the same database as the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card and then switches to standby.

Step 6 Verify that the remaining TNCS-2/TNCS-2O card is now in standby mode (the ACT/STBY LED changes to amber).

Step 7 Physically replace the remaining TNCS-2/TNCS-2O card with the second TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card.

a) Open the ejectors on the TNCS-2/TNCS-2O card.
b) Slide the card out of the slot. This raises the IMPROPRMVL alarm, which clears when the upgrade is complete.
c) Right-click the slot from which the TNCS-2/TNCS-2O card was ejected out.
d) Click **Delete Card** to delete the TNCS-2/TNCS-2O card from CTC.

   If the TNCS-2/TNCS-2O card is not deleted from the CTC shelf view before inserting the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card, the IMPROV-MISMATCH/MEA (card mismatch) alarm appears on that slot. The MEA alarm can be cleared by resetting the configuration to factory defaults.

e) Open the ejectors on the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card.
f) Slide the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card into the slot along the guide rails.
g) Close the ejectors.

The second TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card boots up. The TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card must also copy the database. Do not remove the card from the shelf during a database transfer.

Step 8 If power-related alarms occur after the second TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card is installed, refer to the troubleshooting guide for information on clearing the alarms.

Stop. You have completed this procedure.

Dual Shelf Control - Downgrade A Single TNCS-2 or TNCS-2O Card to the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O Card

A dual shelf control scenario is when a Cisco NCS 2006 or Cisco NCS 2015 has two operating Control Cards on the chassis. In this case, only the standby control card is downgraded from the TNCS-2 or TNCS-2O card to the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card.

Procedure

Step 1 Verify that the node you are downgrading has Release 11.0 installed. The software version is displayed in the upper left corner of the window.

Step 2 Back up the database before beginning the downgrade. https://www.cisco.com/c/en/us/td/docs/optical/15000r10_0/ncs/network_config/guide/b_ncs_network_configuration/b_ncs_network_configuration_chapter_010000.html#ID17_backupdatabase

Step 3 Perform step 3 from Dual Shelf Control - Downgrade Control Cards to TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O Card, on page 45 to downgrade the standby TNCS-2/TNCS-2O card to the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card.

Note

On a dual shelf controller, the TNCS-2 and TNCS-2O cards are only compatible to function with the TNC-E, TNCS, and TNCS-O control cards.

Specific services must be deleted on the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O cards before upgrading to TNCS2 and TNCS2O cards. For more information, see Table 8: Deletion of Services on the Old Control Card, on page 40.

Single Shelf Control - Downgrade Control Card with Software prior to Release 11.0



Caution When a control card with Software Release 11.0 is replaced by another control card with a Software Release prior to 11.0, the downgrade will not happen successfully. The node will not be in a usable condition. Hence, this is not recommended.

Before you begin

- These steps are common for NCS 2002, NCS 2006, and NCS 2015 chassis in slots 1 or 8 in NCS 2006 and slots 1 or 17 in NCS 2015.

Procedure

Step 1 Verify that the node you are downgrading has a Release 11.0 installed. The software version is displayed in the upper left corner of the window.

Step 2 Back up the database before beginning the downgrade. https://www.cisco.com/c/en/us/td/docs/optical/15000r10_0/ncs/network_config/guide/b_ncs_network_configuration/b_ncs_network_configuration_chapter_010000.html#ID17_backupdatabase

Step 3 Revert to Release prior to 11.0.

Note
Revert to a Release prior to 11.0 is not possible on the TNCS-2/TNCS-2O cards as they do not support releases prior to Release 11.0. Hence, install a TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card in the node with Release 11.0 and then revert to Release prior to 11.0

Step 4 The sync of the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version prior to Release 11.0 to USB begins automatically. The USBSYNC alarm is raised after reverting the software from Release 11.0 to a Release prior to 11.0.

Step 5 Physically remove the active TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software Release 11.0. and replace the card with the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with a software release prior to Release 11.0.

Note
When the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with a software version of Release 11.0 is to be replaced with another TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with a software version prior

to Release 11.0, revert the existing node with the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card of a software version prior to Release 11.0.

In NCS 2002 node with one control card, NCS 2006 and NCS 2015 nodes with one control card and filler card, replace the existing simplex control card running R11.0 with another control card running R11.0. If the existing simplex control card running R11.0 is replaced with another control card running prior to R11.0, the node database and traffic becomes affected. This issue does not arise when replacing a standby control card with a spare card.

Replacing the Active Control Card on the node is service-affecting.

a) Open the ejectors on the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version Release 11.0.
b) Slide the card out of the slot. This raises the IMPROPRMVL alarm, which clears when the upgrade is complete.
c) Right-click the slot from which the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version Release 11.0 was ejected out.
d) Click **Delete Card** to delete the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version Release 11.0 from CTC.

   If the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version Release 11.0 is not deleted from the CTC shelf view before inserting the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version prior to Release 11.0, the IMPROV-MISMATCH/MEA (card mismatch) alarm appears on that slot.

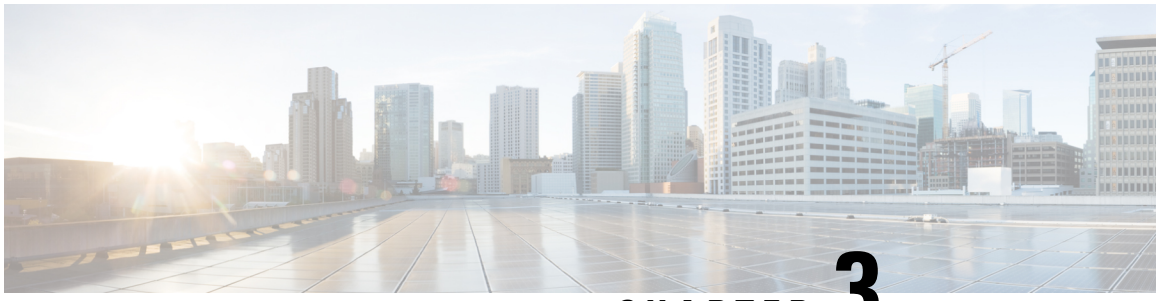
   Specific services must be deleted on the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O cards before upgrading to TNCS2 and TNCS2O cards. For more information, see Table 8: Deletion of Services on the Old Control Card, on page 40.

e) Open the ejectors on the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version prior to Release 11.0.
f) Slide the TNC, TSC, TSC-E, TNC-E, TNCS, or TNCS-O card with software version prior to Release 11.0 into the slot along the guide rails.
g) Close the ejectors.

Step 6 The sync of the TNC, TSC, TSC-E, TNC-E, TNCS or TNCS-O card with software version prior to Release 11.0 to USB begins automatically. Wait for the USBSYNC alarm to clear that is raised after replacing the card in step-5. The USBSYNC alarm clears.

The node is active with the database that is available in the new control card.

Stop. You have completed this procedure.



CHAPTER 3

Connecting the PC and Logging into the GUI

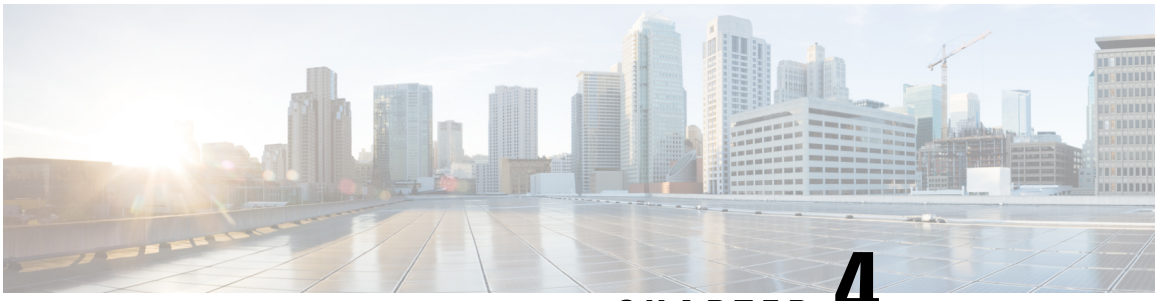
This chapter provides information on how to connect Windows PCs and Solaris workstations to the chassis and how to log into Cisco Transport Controller (CTC) software, the Operation, Administration, Maintenance and Provisioning (OAM&P) user interface.

- Connecting the PC and Logging into the GUI, on page 51

Connecting the PC and Logging into the GUI

The information in this chapter is in a new location. See Connect the PC and Log into the GUI document for information on how to connect Windows PCs and Solaris workstations to the chassis and how to log into Cisco Transport Controller (CTC) software, the Operation, Administration, Maintenance and Provisioning (OAM&P) user interface.

Connecting the PC and Logging into the GUI



CHAPTER 4

Managing the Shelf

Note Starting with Release 11.1.4, ONS 15454 M12 chassis and TCC3 card are not supported on the ONS 15454 DWDM and WSON software packages. You must not attempt to upgrade ONS 15454 M12 nodes from a previous release to Release 11.1.4.

This chapter explains how to provision a single Cisco NCS node and turn it up for service, including assigning the node name, date, and time; provisioning timing references; provisioning network attributes such as IP address and default router; setting up users and user security; and creating DWDM connections.

The procedures and tasks described in this chapter for the Cisco NCS platform is applicable to the Cisco NCS 2000 series, unless noted otherwise.

Procedures in this chapter require that you have a network plan calculated for your DWDM network with Cisco Transport Planner. Cisco Transport Planner is a DWDM planning tool that is available from your Cisco account representative. Cisco Transport Planner prepares a shelf plan for each network node and calculates the power and attenuation levels for the DWDM cards installed in the node. For information about Cisco Transport Planner, contact your Cisco account representative. For instructions on using Cisco Transport Planner, refer to the *Cisco Transport Planner DWDM Operations Guide*.

Note During the conversion of single shelf to multishelf node controller shelf, it is recommended to delete all the existing circuits on the shelf once and then proceed with re-creating them to avoid any unnecessary results. For example, the TL1 retrievals will not return the right values if the circuits are not deleted before converting to multishelf node.

Note Due to memory limitations, TCC2/TCC2P cards are not supported from Release 10.5.2 onwards. As a result, in a multishelf configuration, the TCC2/TCC2P cards cannot be a node controller or a shelf controller. Upgrade the TCC2/TCC2P card to a TCC3 card.

Note Cisco Transport Controller (CTC) views referenced in these procedures depend on the mode. In single-shelf mode, the views are network, node, and card. In multishelf mode, the views are network, multishelf, shelf, and card. For more information about CTC views, refer to CTC Enhancements, Operations, and Shortcuts.

- NTP-G139 Verifying Cisco Transport Planner Reports and Files, on page 54
- NTP-G22 Verifying Common Card Installation, on page 56
- NTP-G250 Verifying Digital Image Signing (DIS) Information, on page 57
- NTP-G144 Provisioning a Multishelf Node, on page 59
- Duplicate Node Controller, on page 61
- NTP-G23 Create Users and Assign Privileges, on page 62
- Setting Maximum Password Length Using CTC, on page 65
- NTP-G24 Setting Up Node Identification Information, on page 66
- NTP-G25 Setting Battery Power Monitor Thresholds, on page 68
- NTP-G26 Setting Up CTC Network Access, on page 69
- NTP-G194 Setting Up EMS Secure Access to the Node, on page 84
- NTP-G27 Setting Up the Node for Firewall Access, on page 85
- NTP-G28 Creating FTP Host, on page 87
- NTP-G132 Provisioning OSI, on page 89
- NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 100
- NTP-G320 Configuring the Node as a Non-DWDM Network, on page 105
- NTP-G31 Installing the DWDM Dispersion Compensating Units, on page 107
- NTP-G239 Managing Passive Units and Passive Shelves, on page 108
- NTP-G152 Creating and Verifying Internal Patchcords, on page 114
- NTP-G242 Creating an Internal Patchcord Manually, on page 116
- NTP-G354 Creating an Internal Patchcord Manually Using the Trunk to Trunk (L2) Option, on page 117
- NTP-G209 Creating, Editing, and Deleting Optical Sides, on page 127
- NTP-G38 Provisioning OSC Terminations, on page 130
- NTP-G37 Running Automatic Node Setup, on page 132
- NTP-G163 Upgrading Nodes in Single-Shelf Mode to Multishelf Mode, on page 134
- DLP-G730 Editing the Shelf ID of the Subtending Shelf in a Multishelf Configuration Using the LCD, on page 136

NTP-G139 Verifying Cisco Transport Planner Reports and Files

Purpose	This procedure verifies that you have the Cisco Transport Planner reports and files needed to turn up the node.
Tools/Equipment	None
Prerequisite Procedures	*Cisco NCS 2000 Series Hardware Installation Guide*
Required/As Needed	Required
Onsite/Remote	Onsite

Security Level	Retrieve or higher

Procedure

Step 1 Verify that you have the Cisco Transport Planner reports and files shown in the following table for the node that you will provision. The reports and files can be provided in one of the following ways:

- If you have Cisco Transport Planner, verify that you have the electronic network design plan from which you can generate the reports in Cisco Transport Planner. For information about generating the reports, refer to the *Cisco Transport Planner DWDM Operations Guide*.
- If you do not have Cisco Transport Planner, you must have printouts of all reports listed in the following table except the Assisted Configuration Setup file. Assisted Configuration Setup is an electronic file that will be imported into CTC. You must be able to access it from the CTC computer used to provision the node
- If you not do not have all the reports and files listed in the following table, do not continue. See your site planner or network planner for the required information and files.

Step 2 Print the following table for reference. You will need information from the reports during node turn-up.

Stop. You have completed this procedure.

Cisco Transport Planner Node Setup Information and Files

Table 10: Cisco Transport Planner Node Setup Information and Files

Source	Format	Description
Shelf layout	JPG file	Cisco Transport Planner provides a shelf layout showing the cards that should be installed in each slot. Cisco Transport Planner can export each of these cards as a JPG file with a user-defined name.
Installation Parameters	Table	Provides the target reference values for the variable optical attenuators (VOAs), output power, optical thresholds, and amplifier configuration parameters.
Internal Connections	Table	Identifies the patchcords that must be installed within the shelf.
NE Update Configuration file	XML file	The Cisco Transport Planner NE Update configuration file is an electronic file with an XML extension and a name assigned by the network designer for the network you are provisioning. The file is imported into CTC where it preprovisions internal patchcords, optical sides and card parameters for optical cards, transponders, and passive units (DCUs and patch panels). It configures the ANS parameters based on the network calculated by Cisco Transport Planner.

Source	Format	Description
Traffic Matrix	Table	Shows the traffic flow within the node. During node turn-up, this report is used to identify the location of Y-cable protection groups.
Cable list	Table or list	A list of cables needed to provision the node. The list can be derived from the Internal Connections Report or from the Bill of Materials report prepared by Cisco Transport Planner.

NTP-G22 Verifying Common Card Installation

Purpose	This procedure verifies the following: • • Cisco NCS 2006 and the Cisco NCS 2002 shelves have TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O cards installed. • and the NCS 2015 shelves have TNCS/TNCO cards installed.
Tools/Equipment	None
Prerequisite Procedures	Install the Shelf in the *Cisco 15454 Hardware Installation Guide*
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Procedure

Step 1 Verify the following:

- Two TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O/TNCS/TNCS-O cards are installed in Slots 1 and 8 on the NCS 2006 shelf.
- A stand-alone TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O card is installed in Slot 1 on the NCS 2002 shelf.
- Two TNCS/TNCS-O cards are installed in Slots 1and 17 on the NCS 2015 shelf.

Step 2 Verify that the FAIL LED is off on both the control cards.

Step 3 Verify that the green ACT (active) LED is illuminated on one control card and that the amber STBY (standby) LED is illuminated on the other control card.

Note
If the control cards are not installed, or if their LEDs are not operating as described, do not continue. Complete the " Installing and Configuring the TNC, TNCE, TSC, TSCE, TNCS-2, TNCS-2O or TNCS/TNCS-O Card" task in the *Cisco NCS 2000 Series Hardware Installation Guide*.

Step 4 Verify that the software release shown on the LCD matches the software release required for your network. On the LCD, the software release is shown under the platform (SONET or SDH) and date/temperature. If the release does not match, perform one of the following procedures:

- Perform a software upgrade using the software CD. Refer to the release-specific software upgrade document.
- On NCS 2006, replace the LCD and TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O/TNCS/TNCS-O cards with cards containing the correct release.
- On NCS 2002, replace the power module and TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O cards with cards containing the correct release.
- On NCS 2015, replace the LCD and TNCS/TNCS-O cards with cards containing the correct release.

Stop. You have completed this procedure.

NTP-G250 Verifying Digital Image Signing (DIS) Information

Purpose	This procedure retrieves the following information for the TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O/TNCS/TNCS-O cards: • Software signature information • Version of the digitally signed software • Public keys installed
Tools/Equipment	None
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 56 • DLP-G46 Log into CTC
Required/As Needed	As Needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve user

Procedure

Step 1 Do the following as applicable at the node where you want to verify the DIS information:

a) To retrieve the digitally signed software version, go to Step 2.
b) To retrieve the software signature information, go to Step 3.
c) To retrieve the public keys installed on the node, go to Step 4.

Step 2 In node view (single-shelf mode) or multishelf view (multishelf mode), click **Maintenance** > **Software** tab to retrieve the digitally signed software version. The following columns appear in the pane:

- Node—Displays the node name or IP address.
- Type—Displays the node type.
- **Node Status**—Displays the node status, which is based on the highest alarm level at the node.
- **Working Version**—Displays the working node software version (the general software release number [n.n.n] followed by the specific software release identification number). For example, 9.2.0 (09.20-X10E-02.06).
- **Protect Version**—Displays the protect node software version (the general software release number [n.n.n] followed by the specific software release identification number). For example, 9.2.0 (09.20-X10E-02.06).
- **Download Status**—Displays the status of any in-progress network software downloads.

Step 3 In node view (single-shelf mode) or shelf view (multishelf view), click **Maintenance** > **DIS** > **Info** > **Retrieve Signature Information** tabs to retrieve signature information. The following information is displayed in the pane:

- Attribute**—**The following information is displayed:
  - Organization Name—Displays the owner of the software image.
  - Organization Unit—Displays the business unit within Cisco.
  - Serial Number—Displays the serial number of the certificate with the digital signature.
  - Common Name—Displays the name of the platform.
  - Hash Algorithm—Displays the hashing algorithm used.
  - Image Type—Shows the type of the image-Development or Production.
  - Key Version—Indicates the key version used to digitally sign the image. A key version is identified with an alphabetical character that ranges from A to Z.
  - Sign Algorithm—Refers to the RSA algorithm.
  - Working Software Information—Displays the signature information of the working software.
  - Protect Software Information—Displays the signature information of the protect software.

Note
To refresh the signature information, click **Refresh Signature Information.**

Step 4 In node view (single-shelf mode) or shelf view (multishelf mode), click **Maintenance** > **DIS** > **Available Keys** > **Retrieve All Keys** tabs to retrieve public key information. The following information is displayed in the pane:

- **Key Type—**Displays the public key available on the system for verification:
  - **Release Key—**Verifies release images.
  - **Development Key—**Verifies the development images.

- **Public Key Algorithm—**Displays the name of the algorithm used for public key cryptography.
- **Exponent—**Displays the exponent of the public key algorithm—release or development keys.
- **Key Version—**Displays the key version used for verification.
- **Modulus**—Displays the modulus of the public key algorithm with a size of 2048 bits.

Note
To refresh the public key information, click **Refresh All Keys.**

Stop. You have completed this procedure.

NTP-G144 Provisioning a Multishelf Node

Purpose	This procedure provisions a multishelf node from CTC. A multishelf node consists of a control node and subtending shelves that are configured to operate as a single node.
Tools/Equipment	None

Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 56
	• *Cisco NCS 2000 Series Hardware Installation Guide*
	  • NTP-L15 Connecting the NCS 2006 Multishelf Node and the NCS 2006 Subtending Shelves
	  • NTP-L16 Connecting the NCS 2006 and the NCS in a Mixed Multishelf Configuration
	  • NTP-L17 Upgrading the NCS Multishelf Configuration Using the NCS 2006
	  • NTP-Connecting the NCS 2006 Multishelf Node and the NCS 2006 Subtending Shelves with Simplex Controllers
	  • NTP-G318 Connecting the NCS 2006 Multishelf Node and the NCS 2006 Subtending Shelves in a Ring Topology
	• DLP-G46 Log into CTC

Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note If a standalone node has unsupported cards, the node cannot be converted to a node controller or a subtended shelf controller.

Note When a subtending shelf controller (SSC) having active and standby control cards is initially connected to the node controller, the Software Download In-progress alarm is not raised on the standby control card of SSC.

Procedure

Step 1 If you want to set up the login node as the node controller, complete the following steps. If not, continue with Step 2.

a) In node view (single-node mode) or multishelf view (multishelf mode), click the **Provisioning** > **General** > **Multishelf Config** tabs.

b) Click **Enable as Node Controller**.

c) From the LAN Config drop-down list, complete one of the following:

- In case of NCS 2006, the public VLAN ID and private VLAN ID are static (1 and 2 respectively).

Note
Before a SSC is connected to a multishelf node controller shelf, ensure **Ethernet Switch** is selected from the LAN Config drop-down list.

Note
Public VLAN ID is used by the node controller to communicate with the external network. Private VLAN ID is used by the node controller to communicate with the subtending shelves.

Note
If the NCS 2006 shelf is used as the node controller, then you can connect the subtending shelves directly to the MSM ports on the ECU. However, a Catalyst 3560 switch can also be used along with the NCS 2006 node controller to extend the number of subtending shelves.

d) Click **Apply**.

e) In the confirmation dialog box, click **Yes** to allow the node to reboot. The CTC view changes to network view and the node icon changes to gray. Wait for the reboot to finish. (This might take several minutes.)

f) After the node reboots, double-click the node. The multishelf view appears.

Note
The shelf ID of the node controller is automatically assigned as 1.

Step 2 If you want to add a node as a subtending shelf in the multishelf configuration, complete the following steps. If not, you have completed this procedure.

a. In multishelf view, right-click the white space in the rack and choose **Add Shelf** from the shortcut menu.

b. Select the type of subtending shelf.

c. In the Shelf ID Selection dialog box, choose a shelf ID (from 2 to 50) from the drop-down list.

d. Click **OK**. The shelf appears in multishelf view.

e. Disconnect the cross-over (CAT-5) LAN cable from the EMS RJ-45 LAN (TCP/IP) on the NCS 2006 subtending shelf that correspond to the TNC/TNCE/TSC/TSCE card.

f. Connect your Windows PC or Solaris workstation network interface card (NIC) to the EMS RJ-45 LAN (TCP/IP) on the NCS 2006 subtending shelf that correspond to the TNC/TNCE/TSC/TSCE card.

g. Complete the DLP-G46 Log into CTC task at the subtending shelf.

h. Click the **Provisioning** > **General** > **Multishelf Config** tabs.

i. Click **Enable as Subtended Shelf**.

j. From the Shelf ID drop-down list, choose the shelf ID that you created in Step c.

k. Click **Apply**.

l. In the confirmation dialog box, click **Yes** to reboot the shelf. The CTC view changes to network view and the node icon changes to gray. Wait for the reboot to finish. (This might take several minutes.)

m. Disconnect your Windows PC or Solaris workstation NIC from the EMS RJ-45 LAN (TCP/IP) on the NCS 2006 subtending shelf that correspond to the TNC/TNCE/TSC/TSCE card.

n. Reconnect the cross-over (CAT-5) LAN cable (disconnected in Step e) to the EMS RJ-45 LAN (TCP/IP) on the NCS 2006 subtending shelf that correspond to the TNC/TNCE/TSC/TSCE card.

o. Repeat Steps a through n to set up additional subtending shelves.

Note
To connect the subtending shelves to the node controller, refer to the applicable procedures in the *Cisco NCS 2000 Series Hardware Installation Guide*.

Note
Non-LAN connected Multishelf nodes are not manageable from CTC unless SOCKS Proxy is enabled on the node.

Stop. You have completed this procedure.

Duplicate Node Controller

(Only on NCS 2006 and NCS 2015) When a TNC/TNC-E/TSC/TSC-E/TNCS/TNCS-2/TNCS-2O/TNCS-O node controller connects to the same switch where an NCS 2006 or NCS 2015 node controller exists, both the node controllers raise the critical Duplicate Node Controller (DUP-NC) alarm. The subtending shelves of both the node controllers raise the Shelf Communication Failure (SHELF-COMM-FAIL) alarm. Both the node controllers and their subtending shelves shut down their ports on ASIC towards the MSM ports in ECU. However, the traffic is not affected. This feature enables the original node to operate seamlessly in case of such misconfigurations, without the risk of its subtending shelves treating the new node controller as its primary.

The duplicate node controller can be any one of the following combinations.

- A node controller without any subtending shelf.
- A node controller with one or more subtending shelves connected through switch or daisy chain.

Recovering the Duplicate Node Controller

Note It is recommended to recover the nodes from the DUP-NC critical alarm in less than ten minutes.

Perform the following steps to recover the duplicate node controller.

- Disconnect the duplicate node controller's cable from switch.
- Perform soft reset of the active control card on both the node controllers. The DUP-NC alarm clears.
- Perform hard reset of the active control card on the subtending shelves to restore the multi-shelf.

NTP-G23 Create Users and Assign Privileges

Purpose	This procedure creates users and assigns their privilege levels.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G22 Verify Common Card Installation • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 Log into the node where you need to create users.

Note
You must log in as a Superuser to create additional users. The root user can be used to set up other users.

Step 2 Complete the "DLP-G54 Create a New User on a Single Node" task or the "DLP-G55 Create a New User on Multiple Nodes" task as needed.

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

Step 3 Complete the DLP-G282 Viewing and Terminating Active Logins as needed.

Step 4 If you want to modify the security policy settings, including password aging and idle user timeout policies, complete the NTP-G88 Modify Users and Change Security procedure.

Stop. You have completed this procedure.

DLP-G54 Create a Local User on a Single Node Using CTC

Purpose	This task creates a local user on a single node.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view or network view, click the **Provisioning** > **Security** > **Users** tabs.

Step 2 In the Users window, click **Create**.

Step 3 In the Create User dialog box, enter the following:

- Name—Type the user name. The user name must be a minimum of six and a maximum of 40 characters (only up to 39 characters for the TACACS and RADIUS authentication). It includes alphanumeric (a-z, A-Z, 0-9) characters and the allowed special characters are @, " - " (hyphen), and " . " (dot). For TL1 compatibility, the user name must be of 6 to 10 characters.
- Password—Type the user password.

  Note
  The password change of root user is not supported from CTC.

  The minimum password length for CTC is six and maximum of 127 characters. To set the maximum length of a password, refer to . The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters, where at least two characters are not alphabetic and at least one character is a special character; or the password can contain any 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**.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-G55 Creating a New User on Multiple Nodes

Purpose	This task adds a new user to multiple NCS 2000 nodes managed by CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
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.

Procedure

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning** > **Security** > **Users** tabs.

Step 3 In the Users window, click **Create**.

Step 4 In the Create User dialog box, enter the following:

- Name—Type the user name. The user name must be a minimum of six and a maximum of 40 characters (only up to 39 characters for the TACACS and RADIUS authentication). It includes alphanumeric (a-z, A-Z, 0-9) characters and the allowed special characters are @, " - " (hyphen), and " . " (dot). For TL1 compatibility, the user name must be of 6 to 10 characters.
- Password—Type the user password.

  The password length, by default, is set to a minimum of six and a maximum of 127 characters. To set the maximum length of a password, refer to Setting Maximum Password Length Using CTC, on page 65. The minimum length can be set to two, four, eight, ten or twelve characters, and the maximum length to 127 characters. The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters, where at least two characters are not alphabetic and at least one character is a special character; or the password can contain any 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**.

  Note
  Each security level has a different idle time. The idle time is the length of time that CTC can remain idle before it locks up and the password must be reentered. The defaults are: Retrieve user = unlimited,

Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes. To change the idle times, refer to the NTP-G88 Modify Users and Change Security procedure.

TACACS idle timeout considerations:

- From release 11.1.2.3 onwards, the TACACS server sends the idle timeout value in the minute unit. Previously, the idle timeout value was measured in the second unit. After you upgrade to release 11.1.2.3, the idle timeout unit gets adjusted to minute unit from the second unit.

  Example: On the TACACS server, the idle timeout value of 900 seconds gets changed to 15 minutes after you upgrade to release 11.1.2.3.

- The default idle timeout value on the TACACS server is 60 minutes. If you set an idle timeout value on the ISE/ACS TACACS server, the TACACS authenticated sessions expire once the idle timeout value is reached. However, the CTC sessions remain open if the CTC client is active after the idle timeout is expired.

Step 5 In the Select Applicable Nodes area, deselect any nodes where you do not want to add the user (all network nodes are selected by default).

Step 6 Click **OK**.

Step 7 In the User Creation Results dialog box, verify that the user was added to all the nodes chosen in Step 5. If not, click **OK** and repeat Steps 2 through 6. If the user was added to all nodes, click **OK** and continue with the next step.

Step 8 Return to your originating procedure (NTP).

Setting Maximum Password Length Using CTC

Purpose	This task sets the maximum password length for a local user.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view, click the **Provisioning** > **Security** > **Policy** tabs.

Step 2 In the **Password Complexity** area, click **Maximum Length** drop-down list and choose the desired maximum length for password.

Note

The maximum password length for CTC is of 20, 80, or 127 characters.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

NTP-G24 Setting Up Node Identification Information

Purpose	This procedure provisions node identification information, including the node name, node alias, a contact name with phone number, the location of the node, and the date, time, and time zone.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 56 • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Log into the node that is to be turned up. If you are already logged in, go to Step 2.

Step 2 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **General** > **General** tabs.

Step 3 In the Node Name/TID field, type 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.

Note
To avoid errors when you import the Cisco Transport Planner configuration file using the NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 100, the CTC node name and the Cisco Transport Planner site name must either be the same or at least easy to identify.

Step 4 (Optional) In the Contact field, type the name of the node contact person and the phone number, using up to 255 characters.

Step 5 (Optional) In the Node Alias field, type the alias of the node, up to 128 characters. For TL1 compliance, the alias must not contain any commas, colons, or semi-colons. It does not support any international characters set.

Note
Node alias is displayed when the node is in the discovered state. It shows as a tool tip in the Network Map and Explorer Tree of the CTC. It also shows as a separate column in the Tab View pane of the Network view.

Step 6 (Optional) In the Latitude field, enter the node latitude: N (north) or S (south), degrees, and minutes.

Step 7 (Optional) In the Longitude field, enter the node longitude: E (east) or W (west), degrees, and minutes.

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

Step 8 (Optional) In the Description field, type a description of the node. The description can be a maximum of 255 characters.

Step 9 (Optional) Check the Use NTP/SNTP Server check box if you want CTC to use a Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) server to set the date and time of the node. Using an NTP or SNTP server ensures that all the network nodes use the same date and time reference. The server synchronizes the node's time after power outages or software upgrades.

a) If you check the Use NTP/SNTP Server check box, complete the following fields:

- Use NTP/SNTP Server—Type the IP address of the primary NTP/SNTP server connected to the chassis.
- Backup NTP/SNTP Server—Type the IP address of the secondary NTP/SNTP server connected to the chassis

When the primary NTP/SNTP server fails or is not reachable, the node uses the secondary NTP/SNTP server to synchronize its date and time. If both the primary and secondary NTP/SNTP servers fail or are not reachable, an SNTP-FAIL alarm is raised. The node checks for the availability of the primary or secondary NTP/SNTP server at regular intervals until it can get the time from any one of the NTP/SNTP servers. After the node gets the time from any one server, it synchronizes its date and time with the server's date and time and the SNTP-FAIL alarm is cleared. For each retry and resynchronization, the node checks the availability of the primary NTP/SNTP server first, followed by the secondary NTP/SNTP server. The node synchronizes its date and time every hour.

Note
You will not be able to identify which NTP/SNTP server is being used for synchronization.

Note
If you plan to check gateway network element (GNE) for the SOCKS proxy server (see DLP-G56 Provisioning IP Settings, on page 70), external nodes must reference the gateway for NTP/SNTP timing. For more information about the gateway settings, refer to "Manage Network Connectivity" chapter.

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

b) If you do not check Use SNTP/NTP Server, complete the Date and Time fields. The node 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-G118 Display Alarms and Conditions Using Time Zone task.

- Date—Type the current date in the format m/d/yyyy, for example, September 24, 2002 is 9/24/2002.
- Time—Type the current time in the format hh:mm:ss, for example, 11:24:58. The node uses a 24-hour clock, so 10:00 PM is entered as 22:00:00.

Step 10 Click the Time Zone field and choose a city within your time zone from the drop-down list. The list 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 11 Check the Use Daylight Savings Time check box if the time zone that you chose uses Daylight Savings Time.

Note
The Insert AIS-V on STS-1 SD-P and SD-P BER field are not used in DWDM networks.

Step 12 Click **Apply**.

Step 13 In the confirmation dialog box, click **Yes**.

Step 14 Review the node information. If you need to make corrections, repeat Steps 3 through 12 to enter corrections. If the information is correct, continue with the NTP-G25 Setting Battery Power Monitor Thresholds, on page 68.

Stop. You have completed this procedure.

NTP-G25 Setting Battery Power Monitor Thresholds

Purpose	This procedure provisions extreme high, low, and extreme low input battery power thresholds within a –48 VDC environment.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 56 • DLP-G46 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution The default battery voltage thresholds are normally not changed. Threshold changes should only be performed at the direction of your site administrator.

Note When you change the battery voltage thresholds, alarms are raised twice with incorrect severity.

Note In Release 11.12, you can set the ECU voltage threshold for an ECU-48V to a maximum of 60V. However, it is recommended not to exceed 57.5V.

The voltage threshold range for each battery is -40.5 to -72.0.

Note When the thresholds are crossed, the control card generates warning alarms in CTC. For power specifications, see the Hardware Specifications.

Procedure

Step 1 Login to the node that you will set up. If you are already logged in, continue with Step 2.

Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning** > **General** > **Power Monitor** tabs.

Note
In multishelf mode, power monitor thresholds must be provisioned separately for each shelf within the multishelf including the node controller and all subtending shelves.

Step 3 To change the extreme low battery voltage threshold in 0.5 VDC increments, choose a voltage from the ELWBATVGVdc drop-down list. The default value is -40.5.

Step 4 To change the low battery voltage threshold in 0.5 VDC increments, choose a voltage from the LWBATVGVdc drop-down list. The default value is -44.

Step 5 To change the high battery voltage threshold in 0.5 VDC increments, choose a voltage from the HIBATVGVdc drop-down list. The default value is -54.

Step 6 To change the extreme high battery voltage threshold in 0.5 VDC increments, choose a voltage from the EHIBATVGVdc drop-down list. The default value is -56.5.

Step 7 Click **Apply**.

Stop. You have completed this procedure.

NTP-G26 Setting 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, gateway settings, static routes, Open Shortest Path First (OSPF) protocol, Routing Information Protocol (RIP), and designated SOCKS servers.
Tools/Equipment	None
Prerequisite Procedures	NTP-G22 Verifying Common Card Installation, on page 56
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 Complete the DLP-G46 Log into CTC task. If you are already logged in, continue with Step 2.

Step 2 Complete the DLP-G56 Provisioning IP Settings, on page 70 to provision the NCS IP address, subnet mask, default router, DHCP server, IIOP listener port, and SOCKS proxy server settings.

If you cannot log into the node, you can change its IP address, default router, and network mask by using the LCD on the NCS fan-tray assembly (unless LCD provisioning is suppressed). See the DLP-G57 Setting the IP Address, Default Router, and Network Mask Using the LCD, on page 75 for instructions. However, you cannot use the LCD to provision any other network settings. In an NCS 2002 shelf assembly, the LCD is on the fan-tray assembly. In a NCS 2006 shelf assembly, the LCD is a separate unit installed above the external connection unit (ECU). In a NCS 2015 shelf assembly, the LCD unit is integrated with the fan tray assembly

Note
When accessing CTC from a machine running Windows XP operating system, CTC may sometimes fail to reconnect to a GNE when the GNE proxies for several ENE nodes (approximately 15 ENE nodes). This can happen when there is a side switch or when the LAN is enabled/disabled. This is due to the Windows XP operating system limiting the number of simultaneous TCP/IP connection attempts. As a workaround, close the existing CTC session and relaunch CTC on the GNE node. You can configure a designated socks server list on the CTC to mitigate the problem.

Step 3 If the control cards are installed and you want to turn on the secure mode, which allows two IP addresses to be provisioned for the node, complete the DLP-G264 Enabling Node Security Mode, on page 78.

Step 4 If static routes are needed, complete the DLP-G58 Creating a Static Route, on page 80. For more information about static routes, see Managing Network Connectivity.

Step 5 If the NCS is connected to a LAN or WAN that uses OSPF and you want to share routing information between the LAN or WAN and the ONS network, complete the DLP-G59 Setting Up or Changing Open Shortest Path First Protocol, on page 81.

Step 6 If the NCS is connected to a LAN or WAN that uses RIP, complete the DLP-G60 Setting Up or Changing Routing Information Protocol, on page 83.

Step 7 Complete the DLP-G439 Provisioning the Designated SOCKS Servers, on page 74 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.

DLP-G56 Provisioning IP Settings

Purpose	This task provisions IP settings, which includes the IP address, IP address version, default router, DHCP access, firewall access, and SOCKS proxy server settings for NCS node.

Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution All network changes should be approved by your network (or LAN) administrator.

Caution Verify that the IPv4 or IPv6 addresses assigned to the node are unique in the network. Duplicate IP addresses in the same network cause loss of visibility.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Network** > **General** tabs.

Step 2 Complete the following information in the fields listed:

- IP Address—Type the IP address assigned to the NCS node.

  Note If the control cards are installed, dual IP addressing is available using the secure mode. When secure mode is off (sometimes called repeater mode), the IP address entered in the IP Address field applies to the EMS RJ-45 port or Craft port on the ECU (NCS 2006), EMS RJ-45 port on the power module (NCS 2002), and the control card (LAN) port. When secure mode is on, the IP Address field shows the address assigned to the control card (LAN) port and the Superuser can enable or disable display of the backplane IP address. See the DLP-G264 Enabling Node Security Mode, on page 78 as needed. See Managing Network Connectivity chapter for more information about secure mode.

- Net/Subnet Mask Length—Type the subnet mask length (decimal number representing the subnet mask length in bits) or click the arrows to adjust the subnet mask length.

- MAC Address—(Display only) Displays the IEEE 802 MAC address.

  Note In secure mode, the front and back TCP/IP (LAN) ports are assigned different MAC addresses, and the backplane information can be hidden or revealed by a Superuser.

- Default Router—If the node is connected to a LAN, enter the IP address of the default router. The default router forwards packets to network devices that the node cannot directly access. This field is ignored if any of the following are true:
  - The node is not connected to a LAN.
  - The SOCKS proxy server is enabled and the node is provisioned as an end network element (ENE).

- OSPF is enabled on both the node and the LAN where the node is connected. (OSPF is provisioned in the DLP-G59 Setting Up or Changing Open Shortest Path First Protocol, on page 81.)

- LCD IP Setting—Choose one of the following:
  - **Allow Configuration**—Displays the node IP address on the LCD and allows users to change the IP settings using the LCD. This option enables the DLP-G57 Setting the IP Address, Default Router, and Network Mask Using the LCD, on page 75.
  - **Display Only**—Displays the node IP address on the LCD but does not allow users to change the IP settings using the LCD.
  - **Suppress Display**—Suppresses the node IP address display on the LCD.

- Suppress CTC IP Display—Check this check box if you want to prevent the node IP address from appearing in CTC to users with Provisioning, Maintenance, or Retrieve security levels. (The IP address suppression is not applied to users with Superuser security level.)

  Note
  IP address suppression is not applied to users with Superuser security level. However, in secure mode the backplane IP address visibility can be restricted to only a locally connected Superuser viewing the routing table. In this case, the backplane IP address is not revealed to any user at any other NE, either on the routing table or in autonomous messages (such as the TL1 REPT DBCHG message, alarms, and performance monitoring [PM] reporting).

- 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
    Enable SOCKS Proxy on Port check box is enabled when you enable IPv6 and can be disabled only when IPv6 is disabled.

    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-G317 Change Node Access and PM Clearing Privilege.

  - 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.
  - IPv6 Default Router—Enter the IPv6 address of the default router of the IPv6 NE. This is optional. This field is disabled if the Enable IPv6 check box is not selected.

    Note
    The DWDM node uses NAT-PT internally to support native IPv6. NAT-PT uses the IPv4 address range 128.0.0.0 to 128.0.1.254 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 DLP-G264 Enabling Node Security Mode, on page 78.

- 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 SOCKS proxy server features, do not check this check box.

  Note
  If you enable DHCP, computers connected to the node can obtain temporary IP addresses from an external DHCP server. The node only forwards DHCP requests; it does not act as a DHCP server.

- Gateway Settings—Provisions the SOCKS proxy server features. (SOCKS is a standard proxy protocol for IP-based applications.) Do not change these options until you review Scenario 7 “Provisioning the ONS 15454 Proxy Server” in "Manage Network Connectivity" chapter. In SOCKS proxy server networks, the node is either an ENE, a GNE, or a proxy-only server. Provisioning must be consistent for each NE type.

- Enable SOCKS proxy server on port—If checked, the node serves as a proxy for connections between CTC clients and nodes that are connected by data communications channels (DCCs) to the proxy node. 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; it only requires IP connectivity to the proxy node. If the Enable SOCKS proxy server on port check box is unchecked, the node does not proxy for any CTC clients. When this box is checked, you can provision one of the following options:

  - **External Network Element (ENE)**—Choose this option when the node is not connected to a LAN but has DCC connections to other nodes. A CTC computer connected to the ENE through the control card TCP/IP (craft) port can manage nodes that have DCC connections to the ENE. However, the CTC computer does not have direct IP connectivity to these nodes or to any LAN or WAN that those nodes might be connected to.

  - **Gateway Network Element (GNE)**—Choose this option when the node is connected to a LAN and has DCC connections to other nodes. A CTC computer connected to the LAN can manage all nodes that have DCC connections to the GNE, but the CTC computer does not have direct IP connectivity to them. The GNE option isolates the LAN from the DCC network so that IP traffic originating from the DCC-connected nodes and any CTC computers connected to them is prevented from reaching the LAN.

  - **SOCKS proxy only**—Choose this option when the node is connected to a LAN and the LAN is separated from the node by a firewall. The SOCKS proxy only option is the same as the GNE option, except that the SOCKS proxy only option does not isolate the DCC network from the LAN.

    Note
    If a node is provisioned in secure mode, it is automatically provisioned as a GNE with SOCKS proxy enabled. However, this provisioning can be overridden, and the secure node can be changed to an ENE. In secure mode, SOCKS cannot be disabled. For information about provisioning, including GNE and ENE status, see the DLP-G264 Enabling Node Security Mode, on page 78.

Step 3 Click **Apply**.

Step 4 Click **Yes** in the confirmation dialog box.

The control cards reboot one at a time if changes were made to the IP address, subnet mask, or gateway settings. During this time (approximately 5 to 6 minutes), the active and standby control card LEDs will blink, turn on, and turn off at different intervals. Eventually, a “Lost node connection, switching to network view” message appears.

Step 5 Click **OK**. The network view appears. The node icon appears in gray, during which time you cannot access the node.

Step 6 Double-click the node icon when it becomes green.

Step 7 Return to your originating procedure (NTP).

DLP-G439 Provisioning the Designated SOCKS Servers

Purpose	This task identifies the SOCKS servers in SOCKS-proxy-enabled networks. Identifying the SOCKS servers reduces the amount of time required to log into a node and have all NEs appear in network view (NE discovery time). The task is recommended when the combined CTC login and NE discovery time is greater than five minutes in networks with SOCKS proxy enabled. Long (or failed) login and NE discovery times can occur in networks that have a high ENE-to-GNE ratio and a low number of ENEs with LAN connectivity.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
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 the nodes in the network with LAN access that have SOCKS proxy enabled.

Note SOCKS proxy servers can be any accessible ONS network nodes that have LAN access, including the NCS 2002 and NCS 2006 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-G46 Log into CTC task choosing the Disable Network Discovery option. Complete this task, then login again with network discovery enabled.

Procedure

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 SOCKS server. The server 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 nodes within the network. Add all the nodes that have SOCKS proxy enabled and are connected to the LAN.

Step 6 Click **Check All Servers**. CTC verifies that all nodes can perform as SOCKS servers. Once verified, 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 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-G57 Setting the IP Address, Default Router, and Network Mask Using the LCD

Purpose	This task changes the NCS IP address, default router, and network mask using the LCD on the fan-tray assembly. Use this task if you cannot log into CTC. In a NCS 2002 shelf assembly, the LCD is on the fan-tray assembly. In a NCS 2006 shelf assembly, the LCD is a separate unit installed above the external connection unit (ECU). In a NCS 2015 shelf assembly, the LCD unit is integrated with the fan tray assembly.
Tools/Equipment	None
Prerequisite Procedures	DLP-G604 Installing the TNC, TNCE, TSC, TSCE, TNCS-2, TNCS-2O, TNCS-O, or TNCS Card, on page 24

Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note You cannot perform this task if the LCD IP Display field on the node view Provisioning > Network tab is set to Display Only or Suppress Display. See the DLP-G56 Provisioning IP Settings, on page 70 to view or change the LCD IP Display field. If the node is locked in secure mode with the LCD display disabled, you will not be able to change this provisioning unless the lock is disabled by Cisco Technical Support. See Managing Network Connectivity chapter for more information about secure mode.

Note The LCD reverts to normal display mode after 5 seconds of button inactivity.

Procedure

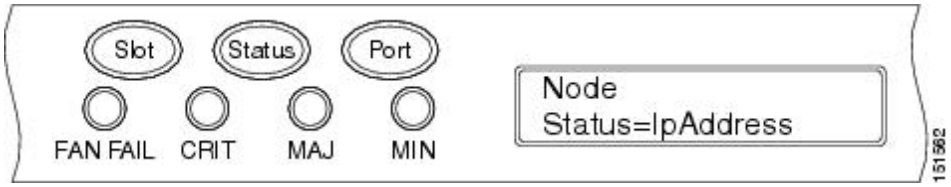
Step 1 On the NCS front panel, repeatedly press the **Slot** button until SHELF appears on the first line of the LCD. You are in the Shelf menu.

Note
In a NCS 2002 shelf assembly, the LCD panel and the **Slot**, **Port**, and **Status** buttons are present on the fan-tray assembly. In a NCS 2006 shelf assembly, the LCD is a separate unit installed above the external connection unit (ECU); the **Slot**, **Port**, and **Status** buttons are present on the LCD unit. In a NCS 2015 shelf assembly, the **Slot**, **Port**, and **Status** buttons are present on the LCD unit that is integrated with the fan tray assembly.

Step 2 Repeatedly press the **Port** button until the following information appears:

- To change the node IP address, Node Status=IpAddress
- To change the node network mask, Node Status=Net Mask
- To change the default router IP address, Node Status=Default Rtr

Figure 8: Selecting the IP Address Option

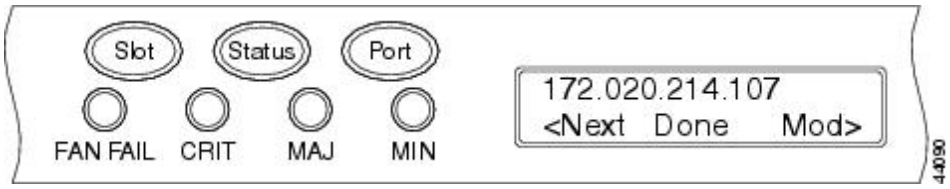


Step 3 Press the **Status** button to display the node IP address, the node subnet mask length, or the default router IP address.

The following IP addresses are displayed in the LCD one after the other:

- Regular IP—Node IP address that is used to access the node when the controller card is in nonsecure mode.
- Secure IP (15454 secure mode IP)—IP address that is assigned to the backplane LAN port. This port connects the node to an operations support system (OSS) through a central office LAN or private enterprise network. This IP address becomes a private address in the secure mode and prevents the front-access craft port user from accessing the LAN through the backplane port.

Figure 9: Changing the IP Address



Step 4 Push the **Slot** button to move to the digit of the IP address, subnet mask, or default router that you want to change. The selected digit flashes.

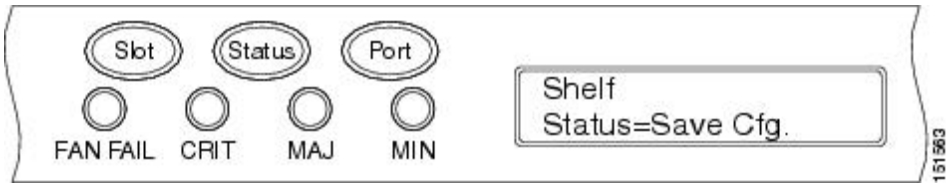
Tip The Slot, Status, and Port button positions correspond to the positions of the commands shown on the LCD. For example, you press the Slot button to invoke the Next command and the Status button to invoke the Done command.

Step 5 Press the **Port** button to cycle the IP address, subnet mask, or default router to the correct digit.

Step 6 When the change is complete, press the **Status** button to return to the relevant Node Status menu.

Step 7 Repeatedly press the **Port** button until the Shelf Save Configuration option appears.

Figure 10: Selecting the Save Configuration Option



Step 8 Press the **Status** button to choose the Save Configuration option.

A Save and REBOOT message appears.

Figure 11: Saving and Rebooting the Control Card



Step 9 Press the **Slot** button to apply the new IP address, subnet mask, or default router configuration or press **Port** to cancel the configuration.

Note
The IP address and default router must be on the same subnet. If not, you cannot apply the configuration.

Step 10 Saving the new configuration causes the control cards to reboot. During the reboot, a message appears on the LCD. The LCD returns to the normal alternating display after both the control cards finish rebooting.

Step 11 Return to your originating procedure (NTP).

DLP-G264 Enabling Node Security Mode

Purpose	This task enables the security mode. When security mode is enabled, two IP addresses are assigned to the node. One address is assigned to the EMS port (NCS 2002 and NCS 2006). The other address is assigned to the RJ-45 TCP/IP (LAN) port of the control cards.
Tools/Equipment	The control cards must be installed.
Prerequisite Procedures	• NTP-G103 Backing Up the Database • DLP-G46 Log into CTC `
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution The IP address assigned to the control card TCP/IP (LAN) port must reside on a different subnet from the EMS port (NCS 2002 and NCS 2006). Verify that the new control card IP address meets this requirement.

Note The node will reboot after you complete this task, causing a temporary disconnection between the CTC computer and the node.

Note If an OTS-to-OTS PPC is created between nodes, it will no longer function if the node Security Mode is enabled. The reason for this is that if the Secure mode is enabled, it is no longer possible for the DCN extension feature to use the LAN interface to extend the internal network (due to the network isolation in this configuration mode). The result is that the topology discovery on the OTS-to-OTS PPC no longer operates.

Procedure

Step 1 Click the **Provisioning** > **Security** > **Data Comm** tabs.

Step 2 Click **Change Mode**.

Step 3 Review the information on the Change Secure Mode page, then click **Next**.

Step 4 On the Ethernet Port page, enter the IP address and subnet mask for the the control card LAN port.

Step 5 Click **Next**.

Step 6 If needed, on the Backplane Ethernet Port page, modify the backplane IP address, subnet mask, and default router. You normally do not modify these fields if no network changes have occurred.

Step 7 Click **Next**.

Step 8 On the SOCKS Proxy Server Settings page, choose one of the following options:

- **External Network Element (ENE)**—If selected, the CTC computer is only visible to the NCS where the CTC computer is connected. The CTC computer is not visible to the nodes connected to the DCC. In addition, firewall is enabled, which means that the node prevents IP traffic from being routed between the DCC and the LAN port.
- **Gateway Network Element (GNE)**—If selected, the CTC computer is visible to other DCC-connected nodes. The node prevents IP traffic from being routed between the DCC and the LAN port.

Note
The SOCKS proxy server is automatically enabled when you enable secure mode.

Step 9 Click **Finish**.

Within the next 30 to 40 seconds, the control cards reboot. CTC switches to network view, and the CTC Alerts dialog box appears. In network view, the node changes to gray and a DISCONNECTED condition appears in the Alarms tab.

Step 10 In the CTC Alerts dialog box, click **Close**. Wait for the reboot to finish. (This might take several minutes.)

Step 11 After the DISCONNECTED condition clears, complete the following steps to suppress the backplane IP address from appearing in CTC and the LCD. If you do not want to suppress the backplane IP address display, continue with Step 12.

a) Display the node in node view (single-shelf mode) or multishelf view (multishelf mode).
b) Click the **Provisioning** > **Security** > **Data Comm** tabs.
c) In the LCD IP Setting field, choose **Suppress Display**. The IP address will not appear on the LCD.
d) Check the **Suppress CTC IP Address** check box. The IP address will not appear in the CTC information area or the Provisioning > Security > Data Comm tabs.
e) Click **Apply**.

Note
After you turn on secure mode, the control card IP address becomes the node IP address.

Step 12 Return to your originating procedure (NTP).

DLP-G58 Creating a Static Route

Purpose	This task creates a static route to establish CTC connectivity to a computer on another network. This task is performed when one of the following conditions exists: • CTC computers on one subnet need to connect to NCS nodes that are connected by a router to NCS nodes residing on another subnet. • OSPF is not enabled (the OSPF Active on LAN check box is not checked on the Provisioning > Network > OSPF tab) and the External Network Element (ENE) gateway setting is not checked. • You need to enable multiple CTC sessions among NCS nodes residing on the same subnet and the External Network Element (ENE) gateway setting is not checked.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Network** tabs.

Step 2 Click the **Static Routing** tab. Click **Create**.

Step 3 In the Create Static Route dialog box, enter the following:

- Destination—Enter the IP address of the computer running CTC. To limit access to one computer, enter the full IP address and a subnet mask of 255.255.255.255. To allow access to all computers on the 192.168.1.0 subnet, enter 192.168.1.0 and a subnet mask of 255.255.255.0. You can enter a destination of 0.0.0.0 to allow access to all CTC computers that connect to the router.
- Mask—Enter a subnet mask. If the destination is a host route (that is, one CTC computer), enter a 32-bit subnet mask (255.255.255.255). If the destination is a subnet, adjust the subnet mask accordingly, for example, 255.255.255.0. If the destination is 0.0.0.0, CTC automatically enters a subnet mask of 0.0.0.0 to provide access to all CTC computers. You cannot change this value.
- Next Hop—Enter the IP address of the router port or the node IP address if the CTC computer is connected to the node directly.
- Cost—Enter the number of hops between the node and the computer.

Step 4 Click **OK**. Verify that the static route appears in the Static Route window.

Note

Static route networking examples are provided in the Managing Network Connectivity chapter.

Step 5 Return to your originating procedure (NTP).

DLP-G59 Setting Up or Changing Open Shortest Path First Protocol

Purpose	This task enables the OSPF routing protocol on the NCS. Perform this task if you want to include the NCS in OSPF-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC You will need the OSPF Area ID, Hello and Dead intervals, and authentication key (if OSPF authentication is enabled) provisioned on the router to which the NCS is connected.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Network** > **OSPF** tabs.

Step 2 On the top left side of the OSPF area, complete the following:

- DCC/GCC OSPF Area ID Table—In dotted decimal format, enter the number that identifies the NCS nodes 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.

  ANSI Nodes

- SDCC Metric—This value is normally unchanged. It sets a cost for sending packets across the Section DCC, which is used by OSPF routers to calculate the shortest path. This value should always be higher than the LAN metric. The default SDCC metric is 100.

- LDCC Metric—Sets a cost for sending packets across the Line DCC. This value should always be lower than the SDCC metric. The default LDCC metric is 33. It is usually not changed.

  ETSI Nodes

- 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 multiplex section DCC (MS-DCC). This value should always be lower than the SDCC 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 the NCS OSPF topology to be advertised to OSPF routers on the LAN. Enable this field on NCS nodes that directly connect to OSPF routers.
- LAN Port Area ID—Enter the OSPF area ID (dotted decimal format) for the router port where the NCS 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 interval defaults are the defaults most commonly used by OSPF routers. Verify that these defaults match the ones used by the OSPF router where the NCS is connected.

- Router Priority—Provision the router priority, which determines the designated router for a subnet.
- Hello Interval (sec)—Provision the number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
- Dead Interval—Provision 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)—Provision the service speed. One second is the default.
- Retransmit Interval (sec)—Provision the number of seconds that will elapse before a packet is resent. Five seconds is the default.
- LAN Metric—Provision the cost for sending packets across the LAN. This value should always be lower than the SDCC or RS-DCC metric. Ten is the default.

Step 6 Under OSPF Area Range Table, create an area range table if one is needed:

Note
Area range tables consolidate the information that is outside an OSPF area border. One node in the NCS 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 NCS OSPF area.

a) Click **Create**.

b) In the Create Area Range dialog box, enter the following:

- Range Address—Enter the area IP address for the NCS nodes that reside within the OSPF area. For example, if the NCS 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 NCS nodes. This is either the ID in the DCC OSPF Area ID field or the ID in the Area ID for LAN Port field.
- Mask Length—Enter the subnet mask length. In the Range Address example, this is 16.
- 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 NCS 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 the 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 NCS OSPF area:

- Neighbor—Enter the router ID of the Area 0 router.
- Transit Delay (sec)—Enter the service speed. One second is the default.
- Hello Int (sec)—Provision 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 15454 is connected uses authentication, choose **Simple Password**. Otherwise, choose **No Authentication**.
- Retransmit Int (sec)—Provision the time that will elapse, in seconds, before a packet is resent. Five seconds is the default.
- Dead Int (sec)—Provision 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 the NCS OSPF area data, click **Apply**.

If you changed the Area ID, the control cards reset, one at a time. The reset takes approximately 10 to 15 minutes.

Step 9 Return to your originating procedure (NTP).

DLP-G60 Setting Up or Changing Routing Information Protocol

Purpose	This task enables RIP on the NCS. Perform this task if you want to include the NCS in RIP-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC You need to create a static route to the router adjacent to the NCS for the NCS to communicate its routing information to non-DCC-connected nodes.
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Network** > **RIP** tabs.

Step 2 Check the **RIP Active** check box if you are activating RIP.

Step 3 Choose either RIP Version 1 or RIP Version 2 from the drop-down list, depending on which version is supported in your network.

Step 4 Set the RIP metric. The RIP metric can be set to a number between 1 and 15 and represents the number of hops.

Step 5 By default, RIP is set to No Authentication. If the router that the NCS is connected to requires authentication, complete the following steps. If not, continue with Step 6.

a) Click the **No Authentication** button.

b) In the Edit Authentication Key dialog box, complete the following:

- Type—Choose **Simple Password**.
- Enter Authentication Key—Enter the password.
- Confirm Authentication Key—Enter the same password to confirm it.

c) Click **OK**.

The authentication button label changes to Simple Password.

Step 6 If you want to complete an address summary, complete the following steps. If not, continue with Step 7. Complete the address summary only if the NCS is a gateway NE with multiple external NCS NEs attached with IP addresses in different subnets.

a) In the RIP Address Summary area, click **Create**.

b) In the Create Address Summary dialog box, complete the following:

- Summary Address—Enter the summary IP address.
- Mask Length—Enter the subnet mask length using the up and down arrows.
- Hops—Enter the number of hops. The smaller the number of hops, the higher the priority.

c) Click **OK**.

Step 7 Return to your originating procedure (NTP).

NTP-G194 Setting Up EMS Secure Access to the Node

Purpose	This procedure provisions nodes and CTC computers for secure access.

Tools/Equipment	None
Prerequisite Procedures	NTP-G26 Setting Up CTC Network Access, on page 69
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Procedure

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-G27 Setting Up the Node for Firewall Access

Purpose	This procedure provisions NCS nodes and CTC computers for access through firewalls.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 56 • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

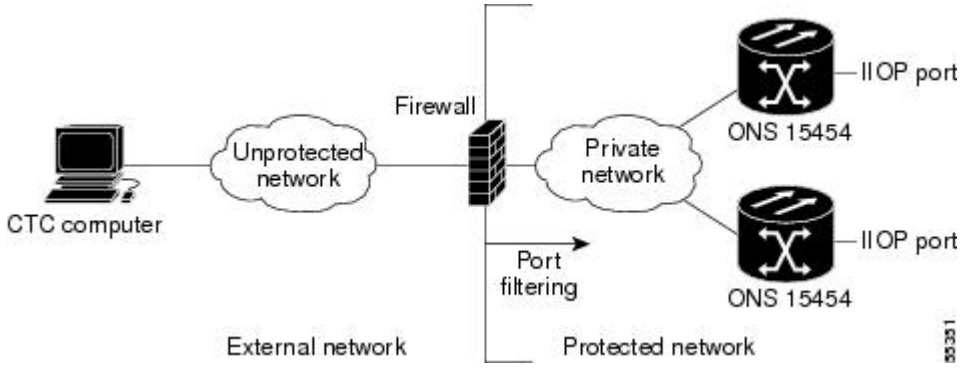
Procedure

Step 1 Log into a node that is behind the firewall. If you are already logged in, continue with Step 2.

Step 2 If the node is in a protected network and the CTC computer is in an external network, complete the DLP-G61 Provisioning the IIOP Listener Port on the NCS, on page 88.

The following figure shows nodes in a protected network and the CTC computer in an external network. For the computer to access the nodes, you must provision the IIOP listener port specified by your firewall administrator on the node.

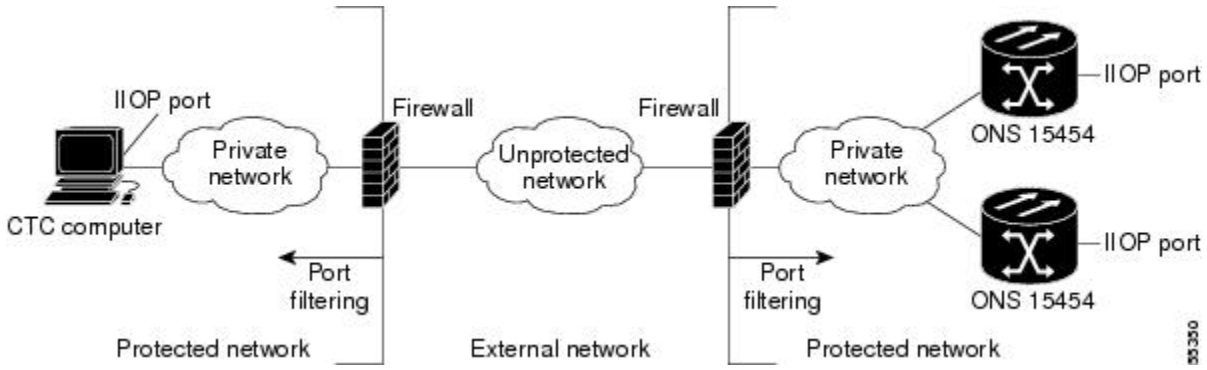
Figure 12: Nodes Behind a Firewall



Step 3 If the CTC computer resides behind a firewall, complete the DLP-G62 Provisioning the IIOP Listener Port on the CTC Computer, on page 88.

The following figure shows a CTC computer and node behind firewalls. For the computer to access the node, you must provision the IIOP port on the CTC computer and on the node.

Figure 13: CTC Computer and Nodes Residing Behind Firewalls



Stop. You have completed this procedure.

NTP-G28 Creating 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-G26 Setting Up CTC Network Access, on page 69 • NTP-G27 Setting Up the Node for Firewall Access, on page 85 • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Procedure

Step 1 If you want to turn on the NCS secure mode, which allows two IPv4 addresses to be provisioned for the node if the control cards are installed, complete the DLP-G264 Enabling Node Security Mode, on page 78. Refer to the Managing Network Connectivity chapter for information about secure mode.

Step 2 In Node view, click the **Provisioning** > **Network** > **FTP Hosts** tabs.

Step 3 Click **Create**.

Step 4 Enter a valid IP address in the FTP Host Address field. A maximum of 12 host can be entered.

Note
You can configure an IPv6 address for an FTP server, in addition to an IPv4 address.

Step 5 The Mask is automatically set according to the Net/Subnet Mask length specified in DLP-G56 Provisioning IP Settings, on page 70. To change the Mask, click the Up/Down arrows on the Length menu.

Step 6 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 8. 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 7 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 8 Click **OK**.

Step 9 Repeat Step 3 through Step 8 to provision additional FTP Hosts.

Stop. You have completed this procedure.

DLP-G61 Provisioning the IIOP Listener Port on the NCS

Purpose	This task sets the IIOP listener port on the NCSshelf which enables you to access nodes that reside behind a firewall.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If the Enable SOCKS proxy on port 1080 check box is checked, CTC will use Port 1080 and ignore the configured IIOP port setting. If the check box is later unchecked, the configured IIOP listener port will be used.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Security** > **Access** tabs.

Step 2 In the TCC CORBA (IIOP) Listener Port area, choose a listener port option:

- **Default - TCC Fixed**—Uses Port 57790 to connect to the nodes 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 available.
- **Standard Constant**—Uses Port 683, the Common Object Request Broker Architecture (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**.

The control cards reboot, one at a time. The reboot takes approximately 15 minutes.

Step 5 Return to your originating procedure (NTP).

DLP-G62 Provisioning the IIOP Listener Port on the CTC Computer

Purpose	This task selects the IIOP listener port for CTC and must be completed if the computer running CTC resides behind a firewall.

Tools/Equipment	IIOP listener port number from LAN or firewall administrator
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 56 • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

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**—Use to connect to NCS nodes from within a firewall or if no firewall is used (default).
- **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 NCS 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).

NTP-G132 Provisioning OSI

Purpose	This procedure provisions the ONS 15454 so it can be installed in networks with other vendor NEs that use the OSI protocol stack for data communications network (DCN) communications. This procedure provisions the Target Identifier Address Resolution Protocol (TARP), OSI routers, manual area addresses, subnetwork points of attachment, and IP-over-Connectionless Network Service (CLNS) tunnels.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G604 Installing the TNC, TNCE, TSC, TSCE, TNCS-2, TNCS-2O, TNCS-O, or TNCS Card, on page 24 • DLP-G46 Log into CTC

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 Managing Network Connectivity chapter and ensure that you know the role of the NCS 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.

Procedure

As needed, complete the following tasks:

- DLP-G283 Provisioning OSI Routing Mode, on page 90—Complete this task first.
- DLP-G284 Provisioning the TARP Operating Parameters, on page 92—Complete this task second.
- DLP-G285 Adding a Static TID-to-NSAP Entry to the TARP Data Cache, on page 94—Complete this task as needed.
- DLP-G287 Adding a TARP Manual Adjacency Table Entry, on page 95—Complete this task as needed.
- DLP-G288 Provisioning OSI Routers, on page 96—Complete this task as needed.
- DLP-G289 Provisioning Additional Manual Area Addresses, on page 97—Complete this task as needed.
- DLP-G290 Enabling the OSI Subnet on the LAN Interface, on page 98—Complete this task as needed.
- DLP-G291 Creating an IP-Over-CLNS Tunnel, on page 99—Complete this task as needed.

Stop. You have completed this procedure.

DLP-G283 Provisioning OSI Routing Mode

Purpose	This task provisions the OSI routing mode. Complete this task when the NCS is connected to networks with third party NEs that use the OSI protocol stack for DCN communication.
Tools/Equipment	None

Prerequisite Procedures	• DLP-G604 Installing the TNC, TNCE, TSC, TSCE, TNCS-2, TNCS-2O, TNCS-O, or TNCS Card, on page 24 • DLP-G46 Log into CTC
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 End System, Intermediate System Level 1, or IS Level 1/Level 2. This decision must be carefully considered. For additional information about OSI provisioning, refer to Managing Network Connectivity chapter.

Caution Link State Protocol (LSP) buffers must be the same at all NEs within the network, or loss of visibility might occur. Do not modify the LSP buffers unless you confirm that all NEs within the OSI have the same buffer size.

Caution LSP buffer sizes cannot be greater than the LAP-D maximum transmission unit (MTU) size within the OSI area.

Note For NCS nodes, three 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.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **OSI** tabs.

Step 2 Choose a routing mode:

- **End System**—The NCS performs OSI end system (ES) functions and relies upon an intermediate system (IS) for communication with nodes that reside within its OSI area.

  Note
  The End System routing mode is not available if more than one virtual router is enabled.

- I**ntermediate System Level 1**—The NCS 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 NCS 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 3 If needed, change the LSP data buffers:

- L1 LSP Buffer Size—Adjusts the Level 1 link state protocol data unit (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 4 Return to your originating procedure (NTP).

DLP-G284 Provisioning the TARP Operating Parameters

Purpose	This task provisions the TARP operating parameters including TARP PDU propagation, timers, and loop detection buffer (LDB).
Tools/Equipment	None
Prerequisite procedures	DLP-G46 Log into CTC
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), 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
  The TARP PDUs L1 Propagation parameter is not used when the Node Routing Area (on the Provisioning > OSI > Main Setup tab) is set to End System.

- TARP PDUs L2 Propagation—If checked (default), TARP Type 2 PDUs that are received by the node and 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
  The TARP PDUs L2 Propagation 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 are 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
  TARP Data Cache 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
  The L2 TARP Data Cache 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 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 loop detection 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
The T1, T2, and T4 timers are not used if the TARP PDUs Origination check box is not checked.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-G285 Adding 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-G46 Log into CTC
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioner or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), 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 or multishelf 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-G287 Adding 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 15454 must communicate across routers or NEs that lack TARP capability.
Tools/Equipment	None
Prerequisite procedures	DLP-G46 Log into CTC
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), 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-G288 Provisioning OSI Routers

Purpose	This task enables an OSI router and edits its primary manual area address.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 56 • DLP-G46 Log into CTC
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 and 3.



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 NSAP address.



Note The System ID for Router 1 is the node MAC address. The System IDs for Routers 2 and 3 are created by adding 1 and 2 respectively to the Router 1 System ID. You cannot edit the System IDs.

Procedure

Step 1 Click the **Provisioning** > **OSI** > **Routers** > **Setup** tabs.

Step 2 Chose the router you want provision 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 **Edit**.

c) In the Edit Manual Area Address dialog box, edit the primary area address in the Area Address field. If you prefer, click **Use Mask** and enter the edits in the Masked NSAP Entry dialog box. The address (hexadecimal format) can be 8 to 24 alphanumeric characters (0–9, a–f) in length.

d) Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Edit Manual Area Address, and OSI Router Editor.

Step 4 Return to your originating procedure (NTP).

DLP-G289 Provisioning Additional Manual Area Addresses

Purpose	This task provisions the OSI manual area addresses. One primary area and two additional manual areas can be created for each virtual router.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 56 • DLP-G288 Provisioning OSI Routers, on page 96 • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Click the **Provisioning** > **OSI** > **Routers** > **Setup** tabs.

Step 2 Chose the router where you want provision an additional manual area address and click **Edit**. The OSI Router Editor dialog box appears.

Step 3 In the OSI Router Editor dialog box:

a) Check **Enable Router** to enable the router and make its primary area address available for editing.

b) Click the manual area address, then click **Add**.

c) In the Add Manual Area Address dialog box, enter the primary area address in the Area Address field. If you prefer, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box. The address (hexadecimal format) can be 2 to 24 alphanumeric characters (0–9, a–f) in length.

d) Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Add Manual Area Address, and OSI Router Editor.

Step 4 Return to your originating procedure (NTP).

DLP-G290 Enabling 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-G22 Verifying Common Card Installation, on page 56 • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note When you create communication channels (optical service channel [OSC] or generic communications channel [GCC]), OSI subnetwork points of attachment are enabled on the communication channels. See the NTP-G38 Provisioning OSC Terminations, on page 130 and the DLP-G76 Provisioning DCC/GCC Terminations task.

Note The OSI subnetwork point of attachment cannot be enabled for the LAN interface if the OSI routing mode is set to ES.

Note If secure mode is on, the OSI subnet is enabled on the backplane LAN port, not the front control card TCP/IP (LAN) port.

Procedure

Step 1 Click the **Provisioning** > **OSI** > **Routers** > **Subnet** tabs.

Step 2 Click **Enable LAN Subnet**.

Step 3 In the Enable LAN Subnet dialog box, complete the following fields:

- ESH—Sets the End System Hello (ESH) propagation frequency. An ES NE transmits ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- ISH—Sets the Intermediate System Hello (ISH) PDU propagation frequency. An intermediate system NE sends ISHs to other ESs and ISs to inform them about the IS NEs 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.

- 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 LAN subnet, the default DIS priority is 63. It normally should not be changed.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-G291 Creating an IP-Over-CLNS Tunnel

Purpose	This task creates an IP-over-CLNS tunnel to allow NCSnodes to communicate across equipment and networks that use the OSI protocol stack.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 56 • DLP-G46 Log into CTC
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 a NCS. The other endpoint is generally provisioned on non-NCS equipment including routers and other vendor NEs. Before you begin, verify that you have the capability to create an OSI-over-CLNS tunnel on the other equipment location.

Note 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 the node.

Procedure

Step 1 Click the **Provisioning** > **OSI** > **Tunnels** tabs.

Step 2 Click **Create**.

Step 3 In the Create IP Over CLNS Tunnel dialog box, complete the following fields:

- Tunnel Type—Choose a tunnel type:
  - **Cisco**—Creates the proprietary Cisco IP tunnel. Cisco IP tunnels add the CLNS header to the IP packets.
  - **GRE**—Creates a generic routing encapsulation (GRE) tunnel. GRE tunnels add the CLNS header and a GRE header to the IP packets.

    Caution
    Always verify that the IP-over-CLNS tunnel type that you choose is supported by the equipment at the other end of the tunnel.

- IP Address—Enter the IP address of the IP-over-CLNS tunnel destination.
- IP Mask—Enter the IP address subnet mask of the IP-over-CLNS destination.
- OSPF Metric—Enter the OSPF metric for sending packets across the IP-over-CLNS tunnel. The OSPF metric, or cost, is used by OSPF routers to calculate the shortest path. The default is 110. Normally, it is not be changed unless you are creating multiple tunnel routes and want to prioritize routing by assigning different metrics.
- NSAP Address—Enter the destination NE or OSI router NSAP address.

Step 4 Click **OK**.

Step 5 Provision the other tunnel endpoint using the documentation provided by the manufacturer of the third party vendor NE.

Step 6 Return to your originating procedure (NTP).

NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File

Purpose	This procedure imports the Cisco Transport Planner NE Update configuration file and creates a log file.
Tools/Equipment	A Cisco Transport Planner NE Update file for the network where the node is installed must be accessible to the CTC computer.
Prerequisite Procedures	• NTP-G139 Verifying Cisco Transport Planner Reports and Files, on page 54 • DLP-G46 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution Verify that you have the correct Cisco Transport Planner network file before you begin this procedure. The file will have an XML extension and a name assigned by your network planner. Check with your network planner or administrator if you have any questions.

Note The import operation of Cisco Transport Planner NE Update configuration file is based on the number of configurations. The import operation takes more time for a very large configuration that includes several pluggable modules and ports. When the configuration file is imported in non-interactive mode, CTC can be used for other operations.

Note The configuration file, which is provided in XML format, provisions internal patchcords, optical sides and card parameters for optical units, transponders, and passive units (DCUs and patch panels). Finally, the NE Update file installs the ANS parameters calculated by Cisco Transport Planner. The log file, which is a text document records the results of the NE update.

Note The Cisco Transport Planner configuration file contains parameters for the node, shelf, card type, port (including the card's wavelength), pluggable port module (PPM), as well as OTN and FEC parameters. Only the values present in XML format appear in the configuration file parameters; if the values are not in XML format, a column appears blank. The XML file values are independently reported and do not affect any configuration changes that you apply.

Note Common control cards are not provisioned by Cisco Transport Planner.

Procedure

Step 1 If you choose the Provision Node Layout option to preprovision the cards in the shelf, complete the following steps. If not, continue with Step 2.

a) Display the node in node view (single-shelf mode) or multishelf view (multishelf mode).
b) Verify that the common control cards are the only cards installed. If in single or multishelf mode, verify that each shelf in the multishelf has two control cards.
   - If common control cards are the only cards installed, continue with Step 2.
   - If other cards appear, continue with Step c.
c) If a physical card other than the common control cards is installed, remove it from the shelf.
d) If preprovisioned DWDM cards are present, delete them using the DLP-G351 Deleting a Card in CTC, then repeat Steps a and b.

Step 2 If you have not created a log file to record the results of the NE update, complete the following steps. If a log file has been created, continue with Step 3.

a) Open a text editor or word processing application.

b) Create a new text (TXT) document with a file name of your choosing.

c) Save the text document in a directory that is easy to navigate to from CTC.

Step 3 In CTC node view (single-shelf mode) or multishelf view, click the **Provisioning** > **WDM-ANS** > **Node Setup** tabs.

Step 4 Choose **Load latest installation file from node** to reload the latest XML file that was applied and stored in the node. Continue with Step 7.

Step 5 Choose **Load installation file from network repository** and navigate to the Cisco Transport Planner node setup file containing the parameters for the network where the node resides. This option downloads the XML file from the remote server. Continue with Step 7.

Step 6 In the field under Select XML file, type the path to the Cisco Transport Planner node setup file containing the parameters for the network where your node resides, or click **Browse** and navigate to the file on your computer. Click the file, then click **Open**. The file will have an XML extension. Continue with Step 7.

Step 7 In the field under Select Log file, type the path to the text file that you created in Step 2, or click **Browse** and navigate to the file on your computer or a network server where you want the node setup results recorded.

Note
The log file records the parameters that were updated successfully and provides an explanation of why an update could not be completed. Each node setup session overwrites the log file contents. If you want to save the results from a previous NE update, save the log file with new name.

Step 8 Click **Apply**.

Step 9 When **Load installation file from network repository** option is chosen, the FTP Remote Installation File *Node-Name* page appears.

a) When the node is configured as a Gateway Network Element (GNE) node, enter the parameters (host name, port, user name, password, remote directory, and XML file name of the remote server) and click **Next**.

b) When the node is configured as a Elementary Network Element (ENE) node, an additional parameter called GNE Selector appear. From the **GNE Selector** drop-down list, select the appropriate GNE in the network. The FTP relay must be configured on the selected GNE to the remote server where the XML file is stored. See NTP-G28 Creating FTP Host, on page 87 to configure the FTP relay on the selected GNE.

Step 10 When the Node Setup Selection for *Node-Name* page appears, complete the following steps. If not, continue with Step 11.

a) Choose the node profile that you want to apply to the node. The Cisco Transport Planner XML file contains profiles for all nodes in the network. Choose the profile that applies to the node you are provisioning.

b) Click **Next**.

Step 11 On the Node Setup for *node name* page, choose one or more of the following:

- Node Layout—Preprovisions the slots in each shelf in CTC for the cards defined in the network plan. Choose this option when no DWDM cards are installed. (Errors will occur if cards are installed or the slots are preprovisioned.) Preprovisioning the slots before the physical cards are installed ensures that card installers place the cards in the correct slots. Preprovisioning the slots is also useful if you want to set up the network prior to card installation. The node layout also preprovisions the chassis and passive units.

- Card Parameters—If checked, provisions the following parameters, if the cards are installed.
  - TXP, MXP, GE_XP, 10GE_XP, GE_XPE, 10GE_XPE, ADM-10G, and OTU2_XP cards—Provisions the OTN and FEC parameters.
  - OPT-AMP-17-C, OPT-AMP-C, OPT-EDFA-17, OPT-EDFA-24, OPT-EDFA-35, GE_XP, 10GE_XP, GE_XPE, and 10GE_XPE cards—Provisions the card mode.
- Pluggable Port Modules— If checked, allows the provisioning of PPMs on TXP, MXP, GE_XP, 10GE_XP, GE_XPE, 10GE_XPE, ADM-10G, and OTU2_XP cards, including PPM payloads.
- Internal Patchcords—If checked, allows creation of internal patchcords among cards provisioned in the node.
- Optical Sides—If checked, allows the provisioning of optical sides.
- ANS Parameters—If checked, installs the ANS parameters. ANS parameters provision the values required for the node to function within the specified network design. ANS parameters include span losses, optical power, optics thresholds, amplifier working mode, gain, tilt, and many others. Refer to Node Reference chapter for a list of ANS parameters.

  Note
  If you are importing the Cisco Transport Planner configuration file for the first time, you normally choose all the available options.

- Skip Interactive Mode—If checked, CTC provisions all the chosen setup components automatically without allowing you to view the results after each one.
- Save Installation Files (XML and log) On Node—If checked, CTC saves the XML and log files on the node.

Step 12 Click **Next.** If you chose Skip Interactive Mode, continue with Step 13. If not, the wizard page that appears depends on the options chosen in Step 11. Complete the steps shown in the following table for each option.

Table 11: NE Update Wizard Options

NE Update Function	
Node/Shelves Layout	View the cards and slots on the left side of the page and verify that they are the same as the la Cisco Transport Planner Shelf Layout (see Cisco Transport Planner Node Setup Information page 55). If the cards and slots match, click **Apply**. If not, click **Cancel**. and contact your ne support to verify that you have the correct node setup file. If the site has a multishelf configu **Next** and repeat this step for each shelf at the site. CTC preprovisions the slots. This might take a few seconds. The results appear in the Log wi that are successfully provisioned display an "Applied" status. A "Slot not empty" status appe cannot be provisioned because a card is physically installed or the slot is already provisioned. complete the following steps. Otherwise, continue with the next NE Update function. **a.** Click **Cancel**, then click **Yes** in the confirmation dialog box. The slot preprovisioning do when you click Cancel. **b.** If a physical card is installed, remove it from the shelf. **c.** Perform one of the following steps: • Delete all the preprovisioned slots using the DLP-G351 Deleting a Card in CTC tas Steps 1 through Step 12 . • Delete the slot where the Slot Not Empty error occurred using the DLP-G351 Deleti CTC task. Complete the DLP-G353 Preprovisioning a Slot task to provision the slot n repeat Steps 1 through 12 making sure to uncheck the Provision Node Layout optio **Note** When you preprovision a slot, the card is purple in the CTC shelf graphic and "NP" appears on the card. After the physical card is installed, the card changes to white ar removed from the CTC shelf graphic.
Passive Units Layout	**a.** Review the passive unit settings. **b.** Click **Apply**. **c.** Click **Next.**
Pluggable Port Modules	**a.** Review the PPM settings for each TXP, MXP, GE_XP, 10GE_XP, GE_XPE, 10GE_XPE, a card. **b.** Click **Apply**. **c.** Click **Next.**
Card Parameters	**a.** Review the OTN, FEC, and card mode settings for each TXP, MXP, GE_XP, 10GE_XP, 10GE_XPE, and OTU2_XP card. **b.** Click **Apply**. **c.** Click **Next.**

NE Update Function	
Internal Patchcords	**a.** Review the internal patchcords. **b.** Click **Apply**. **c.** Click **Next.**
Optical Sides	**a.** Review the optical side assignments. **b.** Click **Apply**. **c.** Click **Next.**
ANS Parameters	**a.** Review the ANS parameters on the left half of the page. **b.** Click **Apply**. The log file displays the results. At the end, a Done status will appear. If a not be applied, a Setting Refused status appears. If this occurs, contact your next leve
Select All	If checked, selects all the options.
Skip Interactive Mode	If checked, CTC provisions all the chosen setup components automatically without allow the results after each one.
Save Installation Files (XML and log) On Node	If checked, CTC saves the XML and log files on the node.

Step 13 Click **Finish**, then click **OK** in the Wizard Complete confirmation dialog box. The confirmation box indicates whether the xml import process was completed successfully.

Stop. You have completed this procedure.

NTP-G320 Configuring the Node as a Non-DWDM Network

Purpose	This tasks configures a node as a Non-DWDM network.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Provisioning** tabs.

Step 2 From the Selector area, select Network Type.

Step 3 Choose **Not-DWDM**, from the Value drop-down list. Click **Apply**.

Step 4 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Port Status** tabs.

Step 5 Click the **Launch ANS** button. The relevant ports in the node will be in IS state.

Step 6 Click **OK**.

Step 7 Return to your originating procedure (NTP).

DLP-G348 Using the Cisco Transport Planner Shelf Layout Report

Purpose	This task describes how to use the Cisco Transport Planner shelf layout report to install cards in a DWDM node.
Tools/Equipment	None
Prerequisite Procedures	NTP-G139 Verifying Cisco Transport Planner Reports and Files, on page 54
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 Display the Cisco Transport Planner shelf layout report for your site. The report can be viewed in Cisco Transport Planner. It can also be viewed as a JPEG graphic. Refer to the *Cisco Transport Planner DWDM Operations Guide* for information about generating shelf layout reports.

Step 2 Review the following installation information:

- Rack—Indicates the rack in the node where the cards must be installed.
- Shelf—Indicates the shelf in the rack where the cards must be installed. Shelf options include:
  - Flex Shelf—The ONS 15216 FlexLayer mechanical shelf houses Y-cable modules. Flex shelf positions are numbered 1 to 4 from left to right.
  - DCU Shelf—The Cisco ONS 15216 dispersion compensation shelf assembly houses DCUs. DCU positions are numbered 1 to 2 from left to right.

- Shelf-ANSI-*n* or Shelf-ETSI-*n*—The ONS 15454 shelf assembly houses ONS 15454 common, DWDM, and client cards. Positions in this type of shelf are numbered 1 to 17 from left to right. Multiple shelves might appear.

- Slot—Indicates the slot in the specific shelf where the cards must be installed:
  - Unit Name (Product ID)— Identifies the card by its Product ID.
  - Unit Description—Identifies the card by its name.
- Unit Side—Identifies the side of the node that the specific card is serving: A, B, C, D, E, F, G, or H.
- Unit Plug-in Modules—Identifies the type and number of PPMs that will be used with specific TXP, MXP, GE_XP, 10GE_XP, GE_XPE, 10GE_XPE, or OTU2_XP cards.

Step 3 Return to your originating procedure (NTP).

NTP-G31 Installing the DWDM Dispersion Compensating Units

Purpose	This procedure describes how to install the DCUs for DWDM shelves.
Tools/Equipment	DCUs
Prerequisite Procedures	• DLP-G604 Installing the TNC, TNCE, TSC, TSCE, TNCS-2, TNCS-2O, TNCS-O, or TNCS Card, on page 24 • NTP-G139 Verifying Cisco Transport Planner Reports and Files, on page 54
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Warning 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



Caution Always use the supplied ESD wristband when working with a powered NCS. For detailed instructions on how to wear the ESD wristband, refer to the *Electrostatic Discharge and Grounding Guide for Cisco NCS 2000 Series*.

Note For US installations, complies with the US Federal Drug Administration Code of Federal Regulations Title 21, Sections 1040.10 and 1040.11, except for deviations pursuant to Laser Notice No. 50, dated July 26, 2001.

Procedure

Step 1 Remove the DCU from its packaging, then remove the protective caps from the connectors. (Safety caps are typically yellow.)

Step 2 Use both hands to push the DCU all the way into the chassis until the connector spring lock on the right side of the module clicks into place.

Step 3 Open the cover with the laser warning on the connector adapter and then connect the cable connector.

Note
The Side A DCU is commonly installed on the left side and the Side B DCU is commonly installed on the right side.

Note
Double-check the placement of the DCU card(s) with your Cisco Transport Planner shelf layout. If you install the wrong DCU in a slot, remove the DCU and install the correct one.

Stop. You have completed this procedure.

NTP-G239 Managing Passive Units and Passive Shelves

Purpose	This procedure explains how to add or delete passive units or passive shelves.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the DLP-G46 Log into CTC task to log in to a NCS node on the network.

Step 2 As needed, complete the following tasks:

- Complete the DLP-G543 Adding Passive Units or Passive Shelves Manually, on page 109 to manually preprovision a passive unit or passive shelf.

- Complete the DLP-G544 Deleting a Passive Unit or Passive Shelf, on page 110 to delete a passive unit or passive shelf.
- Upgrade the firmware of the passive shelves.
- Complete the #unique_94 to associate a passive unit or passive shelf with the USB port, perform a Blink LED operation, or a Power Refresh on the passive units or passive shelves.

Stop. You have completed this procedure.

DLP-G543 Adding Passive Units or Passive Shelves Manually

Purpose	This task preprovisions passive units (passive shelves, patch panels, and DCUs) in CTC. Preprovisioning of the passive units is normally performed when you complete the NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 100 . Use this task if you need to manually preprovision a passive unit or passive shelf. All slot preprovisioning must be based upon the Cisco Transport Planner shelf layout prepared for your site.
Tools/Equipment	Cisco Transport Planner shelf layout table or JPG file.
Prerequisite Procedures	• DLP-G46 Log into CTC • NTP-G139 Verifying Cisco Transport Planner Reports and Files, on page 54
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Passive Cards** tabs.

Step 2 Click **Create**. The Create Passive Card dialog box appears.

Step 3 Choose the unit from the Card Type drop-down list and click **OK**.

If PASSIVE SHELF MF or PASSIVE SHELF MF10 is selected, go to the next step, otherwise go to Step 5.

Note
You can also add a passive unit in the multishelf view by right-clicking the slot inside the rack. Refer to the NTP-G146 Add a Rack, Passive Unit, or Shelf to a Multishelf Node procedure.

Note
If you need to view the details of the passive units that have been installed on a node, click the Inventory tab.

Step 4 Enter a shelf ID in the PShelf ID field.

The range is from 1 to 126. The next available ID is automatically assigned if a value is not specified.

Step 5 Choose the shelf where the passive unit is to be provisioned from the Passive Shelf drop-down list.

The drop-down list contains all provisioned passive shelves. If you want to provision a passive unit outside the passive shelf, choose the N/A option.

Step 6 Choose the slot from the Slot drop-down list if you have selected a passive shelf in Step 5.

Step 7 Choose the DCU type from the DCU Type drop-down list. The available values are SMF and ELEAF.

Step 8 Choose the DCU compensation from the DCU Compensation drop-down list.

After successfully adding the passive shelf, the shelf might not appear in the CTC. In this scenario, we recommend you to relaunch the CTC to display the newly added passive shelf.

Step 9 Return to your originating procedure (NTP).

DLP-G544 Deleting a Passive Unit or Passive Shelf

Purpose	This task deletes a passive unit or passive shelf.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Passive Cards** tabs.

Step 2 Click the passive unit or passive shelf you want to delete.

Step 3 Click **Delete**, then click **Yes**.

Note
All slots in a shelf have to be empty to delete a passive shelf.

You can also delete a passive unit or passive shelf in the multi-shelf view. Refer to NTP-G147 Delete a Passive Unit, Shelf, or Rack from a Multishelf Node procedure.

Step 4 Return to your originating procedure (NTP).

DLP-G792 Performing a Firmware Upgrade on Passive Shelves

Purpose	This task upgrades the firmware of the fiber shuffle or MPO fan out unit.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The firmware upgrade is non-service-affecting. However, there is a temporary loss of connectivity. It is recommended to upgrade only one fiber shuffle or MPO fan out unit per node at a time.

Note During the firmware upgrade, do not reset the TNCS or TNCS-O card nor remove the cable from USB 3.0 port of the fiber shuffle or the MPO fan out unit.

Note Firmware upgrade is allowed only when the ports are in OOS (out-of-service) or Maintenance service state.

Note Event notifications are triggered at every stage of the firmware upgrade process. These event notifications are reported as transient conditions in the multishelf view > Alarms tab in CTC. The notifications are also displayed in the multishelf view > History > Session tab in CTC. The following event notifications are displayed:

- FIRMWARE_DOWNLOAD —When the firmware download is in progress. The firmware upgrade is initiated after the download is complete.
- FIRMWARE_UPG — When the firmware upgrade is progress.
- FIRMWARE_UPG_FAIL— When the firmware download or the firmware upgrade fails.
- FIRMWARE_UPG_COMPLETE —When the firmware upgrade is completed successfully.

Procedure

Step 1 In the multishelf view, double-click the MF-6RU or MF10-6RU shelf to open shelf mode or right-click the passive shelf and choose **Open Shelf.**

Step 2 Click the **Maintenance** > **Firmware** tab.

The revision number of the bootrom and kernel are displayed. If the bootrom revision is lower than the current revision, continue with the next step. If the bootroom revision is current and the kernel revision is lower than the current revision, go to Step 5.

Note
The Upgrade OS KERNEL button is disabled when the bootrom revision is lower than the current revision and is enabled only after the bootrom upgrade.

Step 3 Click the **Upgrade BOOTROM** button.

The upgrade process takes about 45 minutes.

Step 4 Verify the bootrom revision in the Maintenance > Firmware tab after the upgrade is complete.

The bootrom revision is also updated in the Inventory tab.

Step 5 Click the **Upgrade OS KERNEL** button.

The upgrade process takes about 30 minutes.

Step 6 Verify the kernel version in the Maintenance > Firmware tab after the upgrade is complete.

Step 7 Return to your originating procedure (NTP).

DLP-G793 Performing Upgrade on Fiber Shuffle

Table 12: Feature History

Feature Name	Release Information	Feature Description
Fiber Shuffle Upgrade	Cisco NCS 2000 Release 11.12	This feature allows you to upgrade the Boot ROM version, OS Kernel, and Uboot version of the fiber shuffle through CTC.

Purpose	This task upgrades the firmware of the passive fiber shuffle (NCS2K-MF10-6RU, and NCS2K-MF-6RU).
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Passive Cards** tabs.

Step 2 Choose the passive card and click **Upgrade Firmware**.

The **Upgrade Passive Software** dialog box appears.

Step 3 Click **Upgrade BOOTROM** to upgrade the Boot ROM version necessary for the new software release.

Note
The upgrade process may take up to 80 minutes. Do not plug-out the device nor start other firmware upgrade operation until the Boot ROM upgrade operation is completed.

Step 4 Click **Upgrade OS KERNEL**.

Note
The upgrade process may take up to 40 minutes. Do not plug-out the device nor start other firmware upgrade operation until the kernel upgrade operation is completed.

Step 5 Click **Upgrade UBOOT** to update the Uboot version.

Note
You must upgrade the Boot ROM before proceeding with Uboot upgrade.

The upgrade process may take up to 15 minutes. Do not plug-out the device nor start other firmware upgrade operation until the Uboot upgrade operation is completed.

Step 6 Click **Yes** in the **Warning: Upgrade Firmware** dialog box.

Note
CTC confirms whether the device firmware is up to date. If the firmware is not the latest version, CTC triggers upgrade process with the help of USB commands to fiber shuffle. After successful upgrade you can see the upgraded version of Boot ROM / OS Kernel / Uboot in the **Upgrade Passive Software** dialog box.

DLP-G762 Associating Passive Units or Passive Shelves to USB Ports

Purpose	This task associates passive units (passive shelves, patch panels, and DCUs) to the USB ports in CTC. This task is also used to perform a power refresh on the passive units or passive shelves.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

Procedure

Step 1 In the node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Passive Cards** tabs.

Step 2 Select the passive unit or passive shelf to associate with the USB port.

Step 3 Click **Associate to USB Port**. The Associate USB port dialog box appears.

Step 4 Choose the shelf from the Shelf drop-down list.

Note
If the passive unit selected in Step 2 is provisioned in a passive shelf, check the Associate within Passive Shelf checkbox so that the Shelf drop-down lists the passive shelves.

Step 5 Choose the USB port from the USB port drop-down list.

The USB port drop-down list contains the USB ports that are physically connected to the equipment type selected in Step 2.

Step 6 Click **OK**.

The passive unit is associated with the selected USB port and shelf.

Step 7 To perform a LED blink function of the device connected to the selected USB port, click **Blink LED**.

The LED Blink dialog box appears indicating that the LED blink has been performed.

The LED blinks in blue color helping the operator to identify a specific passive module. Click **Blink LED** again to stop the blinking.

Step 8 To retrieve the power values on the selected passive unit or passive shelf, click **Power Refresh**.

Note
The Power Refresh and Blink LED functions can be performed only after associating the passive units or passive shelves to USB ports.

Step 9 Return to your originating procedure (NTP).

NTP-G152 Creating and Verifying Internal Patchcords

Purpose	This procedure imports the internal patchcords using the CTP XML file. Internal patchcords can also be manually provisioned.
Tools/Equipment	• Cisco Transport Planner shelf layout • Cisco Transport Planner Internal Connections Report

Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 56 • NTP-G139 Verifying Cisco Transport Planner Reports and Files, on page 54 • DLP-G46 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 Login to the node where you want to provision the DWDM cable connections. If you are already logged in, continue with Step 2.

Step 2 Complete the NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 100 to import the Cisco Transport Planner NE update file.

Step 3 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcords** tabs.

Note
The Internal Patchcords tab does not show OPT-PRE DCU connections or span connections.

Note
The number of rows in the Provisioning > WDM-ANS > Internal Patchcords tab are created dynamically, as per the number of sides present in a node.

Note
On the NCS 2002 and the NCS 2006 shelves, you can create internal patchcords between the TNC and TNCE cards and the optical amplifier cards.

Step 4 Verify that the connections in the Internal Patchcords tab match the connections in the Cisco Transport Planner Internal Connections Report for the DWDM cards (see the DLP-G349 Using the Cisco Transport Planner Internal Connections Report task). The Internal Patchcords tab will not show OPT-PRE DCU connections or span connections.

Step 5 Complete the NTP-G242 Creating an Internal Patchcord Manually, on page 116 for any connections that require manual provisioning, for example, to create patchcords between TXP and MXP trunk ports and OCH filter ports. If you need to delete a connection, complete the DLP-G355 Deleting an Internal Patchcord, on page 126.

Note
Connections related to optical bypass circuits must be manually provisioned.

Step 6 To view patchcords that are directly connected to TXP cards only, check the TXP Only checkbox.

Stop. You have completed this procedure.

NTP-G242 Creating an Internal Patchcord Manually

Purpose	This procedure creates an internal patchcord manually.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note Use only one management interface to complete the creation of internal patchcords. For example, do not begin the internal patchcord creation using the TL1 interface or CTP XML file and end the internal patchcord creation using CTC.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcord** tabs.

Step 2 Click **Create**.

Step 3 Choose one of the following link types for the internal patchcord:

- Trunk to Trunk (L2)—Creates a bidirectional patchcord between the trunk ports of GE_XP and 10GE_XP cards. If you choose this option, complete NTP-G354 Creating an Internal Patchcord Manually Using the Trunk to Trunk (L2) Option, on page 117.
- OCH-Trunk to OCH-Filter—Creates an internal patchcord between an optical channel trunk port on a TXP/MXP stage card (which includes GE_XP, 10GE_XP, GE_XPE, 10GE_XPE, ADM-10G, OTU2_XP, 100G-LC-C, 10x10G-LC, CFP-LC, 100G-CK-C, AR_MXP, AR_XP, AR_XPE or ITU-T line cards) and an optical channel filter port on an add/drop stage card (which includes 32MUX, 40-MUX-C, 32WSS, 40-WSS-C/40-WSS-CE, 32DMX, 32DMX-O, 40DMX, 40-SMR1-C, or 40-SMR2-C cards).

  You can use this option to also create an internal patchcord between an optical channel trunk port on a TXP/MXP stage card (which includes TXP, MXP, GE_XP, 10GE_XP, GE_XPE, 10GE_XPE, ADM-10G, OTU2_XP, 100G-LC-C, 10x10G-LC, CFP-LC, 100G-CK-C, AR_MXP, AR_XP, AR_XPE or ITU-T line cards) and the COM port on a PSM card in channel protection configuration (where, PSM card is equipped between one TXP/MXP stage and two add/drop stages). In this case, the Internal Patchcord Creation wizard will prompt you to create patchcords between the working and protect ports on the PSM card and the ports on the two different add/drop stage cards (which includes 32MUX, 40-MUX-C, 32WSS, 40-WSS-C/40-WSS-CE, 32DMX, 32DMX-O, 40DMX, 40-SMR1-C, 40-SMR2-C, 80-WXC-C, or 16-WXC-FS cards). If you choose this option, complete DLP-G547 Creating an Internal Patchcord Manually Using the OCH-Trunk to OCH-Filter Option, on page 118.

- OCH-Filter to OCH-Filter—Creates an unidirectional or bidirectional internal patchcord between a MUX input port and a DMX output port. If you choose this option, complete DLP-G548 Creating an Internal Patchcord Manually Using the OCH-Filter to OCH-Filter Option, on page 120.
- OTS to OTS—Creates a unidirectional or bidirectional internal patchcord between two optical transport section (OTS) ports, between two optical cards, between an optical card and a passive card, between two passive cards, or between the TNC or TNCE cards and an optical amplifier card. This option also includes OSC ports. If you choose this option, complete DLP-G549 Creating an Internal Patchcord Manually Using the OTS to OTS Option, on page 122.
- Optical Path—Creates an internal patchcord between two optical cards, or between an optical card and a passive card. If you choose this option, complete DLP-G531 Creating an Internal Patchcord Manually Using the Optical Path Option, on page 125.

Note
Manual creation of OTS/OCH to OTS/OCH internal patchcords is not required for standard DWDM nodes. However, manual creation might be required for non-standard nodes, for example, a hub node that has wavelength selective switches installed. In such cases, manual creation is recommended by Cisco Transport Planner.

Note
To successfully create an internal patchcord between WSS/DMX channel port and TXP trunk port, choose the TXP as the source endpoint and WSS/DMX as the destination endpoint.

Stop. You have completed this procedure.

NTP-G354 Creating an Internal Patchcord Manually Using the Trunk to Trunk (L2) Option

Purpose	This task creates a bidirectional internal patchcord between the trunk ports of two GE_XP or 10GE_XP cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcord** tabs.

Step 2 Click **Create**.

Step 3 On the Internal Patchcord Type Selection page, choose the patchcord type as Trunk to Trunk (L2) and click **Next**.

Step 4 On the Internal Patchcord Origination page, provision the internal patchcord origination parameters:

- Slot—Choose the slot containing the card where the internal patchcord originates.
- Tx Port—Choose the TX port where the internal patchcord originates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 5 Click **Next**.

Step 6 In the Internal Patchcord Termination page, provision the internal patchcord termination parameters:

- Slot—Choose the slot containing the card where the internal patchcord terminates.
- Port—Choose the RX port where the internal patchcord terminates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 7 Click **Next**.

Step 8 Review the display-only information on the Internal Patchcord Origination Reverse page. This page shows the slot, and port that CTC will use for the opposite internal patchcord origination route.

Step 9 Click **Next**.

Step 10 Review the information displayed on the Internal Patchcord Termination Reverse page. This display-only page shows the slot, and port that CTC will use for the reverse internal patchcord termination route.

Step 11 Click **Finish**. The new internal patchcord appears in the Internal Patchcord table.

Step 12 Return to your originating procedure (NTP).

DLP-G547 Creating an Internal Patchcord Manually Using the OCH-Trunk to OCH-Filter Option

Purpose	This task creates a bidirectional internal patchcord between a TXP, MXP, or XP trunk and a DWDM add and drop channel port.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcord** tabs.

Step 2 Click **Create**.

Step 3 On the Internal Patchcord Type Selection page, choose the patchcord type as OCH-Trunk to OCH-Filter option and click **Next**.

Step 4 On the Internal PatchcordOCH Attributes page, provision the following parameters:

- OCHNC Wavelength—Sets the OCHNC wavelength for the OCH trunk to OCH filter internal patchcord. Use the unnamed band selection box below to display C-band or L-band wavelengths in the OCHNC Wavelength field. Provision the OCHNC wavelength to the wavelength provisioned for the GE_XP, 10GE_XP, GE_XPE, or 10GE_XPE, ADM-10G, OTU2_XP, 100G-LC-C, 10x10G-LC, CFP-LC, 100G-CK-C, AR_MXP, AR_XP, AR_XPE or ITU-T line card trunk port.
- PSM Protection—Select this check box if you have provisioned a PSM card in channel protection configuration.
- Colorless—Select this check box if you want to create a colorless patchcord.

Step 5 Click **Next**.

Step 6 On the Internal Patchcord Origination page, provision the internal patchcord origination parameters:

- Slot—Choose the slot containing the card where the internal patchcord originates.
- Tx Port—Choose the TX port where the internal patchcord originates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 7 In the Internal Patchcord Termination page, provision the internal patchcord termination parameters:

- Type—Choose the type of card (optical or passive card) where the internal patchcord terminates.
- Side—Choose the side where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Slot—Choose the slot containing the card where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord terminates. This field is visible only if you have chosen the type as Passive Card.
- Rx Port—Choose the RX port where the internal patchcord terminates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 8 Click **Next**.

Step 9 In the Internal Patchcord Origination Reverse page, provision the internal patchcord parameters for the reverse internal patchcord origination route:

- Type—Choose the type of card (optical or passive card) where the internal patchcord originates.
- Side—Choose the side where the internal patchcord originates. This field is visible only if you have chosen the type as Optical Card.

- Slot—Choose the slot containing the card where the internal patchcord originates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord originates. This field is visible only if you have chosen the type as Passive Card.

  Note
  Choose the same passive card that you chose in Step 7.

- Tx Port—Choose the TX port where the internal patchcord originates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 10 Click **Next**.

Step 11 In the internal Patchcord Termination Reverse page, provision the internal patchcord parameters for the reverse internal patchcord termination route:

- Slot—Choose the slot containing the card where the internal patchcord originates.
- Rx Port—Choose the RX port where the internal patchcord originates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 12 Click **Next**.

Step 13 Click **Finish**. The new internal patchcord appears in the Internal Patchcord table.

Step 14 Return to your originating procedure (NTP).

DLP-G548 Creating an Internal Patchcord Manually Using the OCH-Filter to OCH-Filter Option

Purpose	This task creates a unidirectional or bidirectional internal patchcord between two DWDM add and drop channel ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcord** tabs.

Step 2 Click **Create**.

Step 3 On the Internal Patchcord Type Selection page, choose the patchcord type as OCH-Filter to OCH-Filter option and click **Next**.

Step 4 On the Internal Patchcord OCH Attributes page, provision the following parameters:

- OCHNC Wavelength—Sets the OCHNC wavelength for the OCH trunk to OCH filter internal patchcord. Use the unnamed band selection box below to display C-band or L-band wavelengths in the OCHNC Wavelength field. Provision the OCHNC wavelength to the wavelength provisioned for the GE_XP, 10GE_XP, GE_XPE, or 10GE_XPE, ADM-10G, OTU2_XP, 100G-LC-C, 10x10G-LC, CFP-LC, 100G-CK-C, AR_MXP, AR_XP, AR_XPE or ITU-T line card trunk port.
- Bidirectional—If checked, creates a bidirectional internal patchcord.
- PSM Protection—Select this check box if you have provisioned a PSM card in channel protection configuration.

Step 5 Click **Next**.

Step 6 On the Internal Patchcord Origination page, provision the internal patchcord origination parameters:

- Type—Choose the type of card (optical or passive card) where the internal patchcord terminates.
- Side—Choose the side where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Slot—Choose the slot containing the card where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord terminates. This field is visible only if you have chosen the type as Passive Card.
- Tx Port—Choose the TX port where the internal patchcord terminates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 7 In the Internal Patchcord Termination page, provision the internal patchcord termination parameters:

- Type—Choose the type of card (optical or passive card) where the internal patchcord terminates.
- Side—Choose the side where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Slot—Choose the slot containing the card where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord terminates. This field is visible only if you have chosen the type as Passive Card.
- Rx Port—Choose the RX port where the internal patchcord terminates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 8 If you did not choose bidirectional in Step 4, continue with Step 13. Otherwise, continue with the next step.

Step 9 Click **Next**.

Step 10 In the Internal Patchcord Origination Reverse page, provision the internal patchcord parameters for the reverse internal patchcord origination route:

- Type—Choose the type of card (optical or passive card) where the internal patchcord originates.

- Side—Choose the side where the internal patchcord originates. This field is visible only if you have chosen the type as Optical Card.
- Slot—Choose the slot containing the card where the internal patchcord originates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord originates. This field is visible only if you have chosen the type as Passive Card.

  Note
  Choose the same passive card that you chose in Step 7.

- Tx Port—Choose the TX port where the internal patchcord originates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 11 Click **Next**.

Step 12 In the internal Patchcord Termination Reverse page, provision the internal patchcord parameters for the reverse internal patchcord termination route:

- Type—Choose the type of card (optical or passive card) where the internal patchcord terminates.
- Side—Choose the side where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Slot—Choose the slot containing the card where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord terminates. This field is visible only if you have chosen the type as Passive Card.

  Note
  Choose the same passive card that you chose in Step 6.

- Rx Port—Choose the RX port where the internal patchcord terminates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 13 Click **Finish**. The new internal patchcord appears in the Internal Patchcord table.

Step 14 Return to your originating procedure (NTP).

DLP-G549 Creating an Internal Patchcord Manually Using the OTS to OTS Option

Purpose	This task creates a unidirectional or bidirectional internal patchcord between two optical transport section (OTS) ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note When the creation of patchcords between two passive cards fails after deleting the previous internal patchcords, delete the passive cards and re-provision them.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcord** tabs.

Step 2 Click **Create**.

Step 3 On the Internal Patchcord Type Selection page, choose the patchcord type as OTS to OTS and click **Next**.

Step 4 On the Internal Patchcords OTS Attributes page, provision the following parameters:

- Bidirectional—If checked, creates a bidirectional internal patchcord.
- MPO Connection—Creates all the patchcords between two MPO connectors. If this option is checked, the bidirectional option is disabled.
- Exclude Used Port—If checked, excludes the used ports for patchcord creation. If unchecked, more than one patchcord can be created starting from the same port.
- Grid Filter—Select the grid option from the drop-down list.
- Port Type—Select the port type from the drop-down list. The options are:
  - OSC only—Cards with OSC ports are available for patchcord creation. The MPO Connection and Exclude Used Ports checkboxes are disabled and the Bidirectional option is checked.
  - DC only—Cards with DC ports and passive DCUs are available for patchcord creation. The MPO Connection and Exclude Used Ports checkboxes are disabled and the Bidirectional option is checked. Allows to create an internal patchcord between an optical card and a passive card.

Step 5 Click **Next.**

Step 6 On the Internal Patchcord Origination page, provision the internal patchcord origination parameters:

- Type—Choose the type of card (optical or passive card) where the internal patchcord originates.
- Slot—Choose the slot containing the card where the internal patchcord originates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord originates. This field is visible only if you have chosen the type as Passive Card.
- Tx Port—Choose the TX port where the internal patchcord originates. CTC automatically displays the list of ports that are available depending on the link type you choose.

- MPO—Choose the port where the internal patchcord originates.CTC automatically displays the list of ports that are available depending on the link type you choose. This field is visible only if you have chosen MPO connection in Step 4.

Step 7 Click **Next.**

Step 8 In the Internal Patchcord Termination page, provision the internal patchcord termination parameters:

- Type—Choose the type of card (optical or passive card) where the internal patchcord terminates.
- Slot—Choose the slot containing the card where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord terminates. This field is visible only if you have chosen the type as Passive Card.
- Rx Port—Choose the RX port where the internal patchcord terminates. CTC automatically displays the list of ports that are available depending on the link type you choose.
- MPO—Choose the port where the internal patchcord originates.CTC automatically displays the list of ports that are available depending on the link type you choose. This field is visible only if you have chosen MPO connection in Step 4.

Step 9 If you did not choose bidirectional in Step 4, continue with Step 14. Otherwise, continue with the next step.

Step 10 Click **Next.**

Step 11 In the Internal Patchcord Origination Reverse page, provision the internal patchcord parameters for the reverse internal patchcord origination route:

- Type—Choose the type of card (optical or passive card) where the internal patchcord originates.
- Side—Choose the side where the internal patchcord originates. This field is visible only if you have chosen the type as Optical Card.
- Slot—Choose the slot containing the card where the internal patchcord originates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord originates. This field is visible only if you have chosen the type as Passive Card.

  Note
  Choose the same passive card that you chose in Step 8.

- Tx Port—Choose the TX port where the internal patchcord originates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 12 Click **Next.**

Step 13 In the Internal Patchcord Termination Reverse page, provision the internal patchcord parameters for the reverse internal patchcord termination route:

- Type—Choose the type of card (optical or passive card) where the internal patchcord terminates.
- Side—Choose the side where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Slot—Choose the slot containing the card where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.

- Unit—Choose the passive card where the internal patchcord terminates. This field is visible only if you have chosen the type as Passive Card.

  Note
  Choose the same passive card that you chose in Step 6.

- Rx Port—Choose the RX port where the internal patchcord terminates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 14 Click **Finish**. The new internal patchcord appears in the Internal Patchcord table.

Step 15 Return to your originating procedure (NTP).

DLP-G531 Creating an Internal Patchcord Manually Using the Optical Path Option

Purpose	This task creates an internal patchcord manually between two optical cards or between an optical card and a passive card.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note When the creation of patchcords between two passive cards fails after deleting the previous internal patchcords, delete the passive cards and re-provision them.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcord** tabs.

Step 2 Click **Create**.

Step 3 On the Internal Patchcord Type Selection page, choose the patchcord type as Optical Path and click **Next**.

Step 4 On the Internal Patchcord Card List page, provision the following parameters:

- Card From Selection area:
  - Type—Choose the type of card (optical or passive card) where the internal patchcord originates.
  - Shelf—(Multishelf nodes only) Choose the shelf where the internal patchcord originates.

- Slot—Choose the slot containing the card where the internal patchcord originates.

- Card To Selection area:
  - Type—Choose the type of card (optical or passive card) where the internal patchcord terminates.
  - Shelf—(Multishelf nodes only) Choose the shelf where the internal patchcord terminates.
  - Slot—Choose the slot containing the card where the internal patchcord terminates.
- Choose the required patchcord from the list that CTC generates.

Step 5 Click **Next** to continue creating internal patchcords between cards and repeat Step 4. In the Internal Patchcord Card List page that follows, CTC automatically populates the Card From Selection fields with the values you entered in the Card To Selection fields in the previous page.

Note
After an internal patchcord is created, the selected optical card appears in the **Unit** drop-down list under *Passive Card Type*. To remove the optical card from the *Passive Card Type*, you must choose *Optical Card* and then *Passive Card* in the **Type** drop-down list. You must do this for every internal patchcord creation to correct the misplacement of the optical card.

Step 6 After creating all the internal patchcords between cards, click **Finish**. The new internal patchcords appear on the Internal Patchcord table.

Step 7 Return to your originating procedure (NTP).

DLP-G355 Deleting an Internal Patchcord

Purpose	This task deletes an internal patchcord.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcord** tabs.

Step 2 Click the connection you want to delete.

Step 3 Click **Delete**, then click **Yes**.

Step 4 Return to your originating procedure (NTP).

NTP-G209 Creating, Editing, and Deleting Optical Sides

Purpose	This procedure allows you to create, edit, and delete optical sides on a DWDM node.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 100 • DLP-G46 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note For any node type including mesh nodes, the association between the shelf, line card and side is reported in the left top window of CTC (Vital Status Pane) in the mode view.

Note For mesh nodes, the association between sides and the 40-WXC-C cards can be found in the **Provisioning** > **WDM-ANS** > **Internal Patchcords** screen. For example: PP-MESH, LC (A): Shelf 1, Slot 3 (40 WXC), port EXP-TX PP-MESH, MPO (A): Shelf 1, Slot 3 (40 WXC), port EXP-RX The above rows indicate that the: WXC port located in Shelf 1, Slot 3 is connected to the LC connector A (Side A) on PP-MESH. WXC port located in Shelf 1, Slot 3 is connected to the MPO connector A (Side A) on PP-MESH.

Procedure

As needed, complete the following tasks:

- Complete the DLP-G491 Creating an Optical Side, on page 128.
- Complete the DLP-G492 Editing an Optical Side, on page 128.
- Complete the DLP-G480 Deleting an Optical Side, on page 129.

Stop. You have completed this procedure.

DLP-G491 Creating an Optical Side

Purpose	This task creates an optical side.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Optical Sides** tabs.

Step 2 Click **Create**.

Step 3 In the Create Side dialog box, enter the following:

- Side ID—Choose a side ID (A, B,C, D, E, F, G, or H) from the drop-down list.
- Line In—Choose an RX port from the drop-down list.
- Line Out—Choose a TX port from the drop-down list.

Note
For a terminal node equipped with a PSM card in line or multiplex section protection configuration, you can only choose the W-RX and W-TX ports while creating an optical side. After you create the working (w) optical side, the control card automatically creates the protected (p) optical side involving the P-RX and P-TX ports of the PSM card. CTC refreshes the Optical Sides tab with both the working and protected optical sides.

Step 4 Return to your originating procedure (NTP).

DLP-G492 Editing an Optical Side

Purpose	This task edits the side ID of an optical side.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Optical Sides** tabs.

Step 2 Click the optical side that you want to edit.

Step 3 Click **Edit**.

Step 4 In the Edit Side ID dialog box, enter the following information:

- Side ID—Choose a side ID from the drop-down list.
- Side Description—Specify a description to identify the side.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-G480 Deleting an Optical Side

Purpose	This task deletes an optical side.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Optical Sides** tabs.

Step 2 Click the optical side that you want to delete.

Step 3 Click **Delete**.

Step 4 In the confirmation dialog box, click **Yes** to continue.

Step 5 Return to your originating procedure (NTP).

NTP-G38 Provisioning OSC Terminations

Purpose	This procedure provisions the OSC terminations.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 100 • DLP-G46 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note The OSC provides a bidirectional channel that connects all nodes within a DWDM ring. The OSC carries a supervisory data channel and synchronizes clocking at network nodes. The OSC also carries a user data channel.

Note Before provisioning OSC terminations on TNC ports carrying Fast Ethernet (FE) payloads, ensure to set the ALS mode on these ports to Disabled.

Note This procedure automatically turns on any OPT-RAMP-C, OPT-RAMP-CE, or RAMAN-CTP cards installed in the DWDM ring.

Note The DCCs, GCCs, and OSCs should not be provisioned between SONET (ANSI) and SDH (ETSI) nodes using CTC or TL1 because they cannot operate between SONET and SDH nodes. These communication channels should be provisioned on similar nodes, such as SONET-to-SONET or SDH-to-SDH.

Note In a pure NCS network configuration, provision the OSC in GE or FE SFP mode. If an OC3 OSC is mandatory, then the network must be timing-synchronized as SONET. Identify the primary node and provide external timing signal to the BITS input pins of the primary node and provision line timing to the remaining nodes in the network.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Comm Channels** > **OSC** tabs.

Step 2 In the OSC Terminations area, click **Create**.

Step 3 In the Create OSC Terminations dialog box, choose the ports where you want to create the OSC termination. To select more than one port, press the **Shift** key (to select a range of ports) or the Ctrl key (to select multiple individual ports).

Note
The number of OSC terminations that you create depends on the node type defined by Cisco Transport Planner. Terminal nodes require one OSC termination. Hub, OADM, and ROADM nodes require two OSC terminations.

Step 4 In the Layer 3 area, check the OSI box if the following conditions are met:

- The OSC termination is between two nodes.
- Third party NEs that use the OSI protocol stack are on the same network.

If you checked OSI, complete the following steps. If not, continue with Step 5.

a) Click **Next**.
b) Provision the following fields:

- Router—Choose the OSI router.
- ESH—Set the ESH propagation frequency. End system NEs transmit ESHs to inform other ESs and ISs about the NSAPs they serve. The default is 10 seconds. The range is 10 to 1000 seconds.
- ISH—Sets the 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 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 5 Click **Finish**. Ports are automatically placed in service. The following alarms might appear in the node view (single-shelf mode) or multishelf view (multishelf mode) Alarms tab Description field. They will remain until all the network OSC connections between the adjacent nodes are created:

- SDCC Termination Failure (ANSI) or RS-DCC Termination Failure (ETSI) on the OSCM or OSC-CSM card
- LOS on the OC-3 port (Port 1) on the OSCM, OSC-CSMcard
- OPWR-LFAIL on the OPT-BST or OSC-CSM card

Note

After the OSC termination is created, the line ports are placed in service and span power levels are checked.

Stop. You have completed this procedure.

NTP-G37 Running Automatic Node Setup

Purpose	This procedure runs the Launch ANS function.
Tools/Equipment	The Cisco Transport Planner Installation Parameters file
Prerequisite Procedures	• NTP-G139 Verifying Cisco Transport Planner Reports and Files, on page 54 • NTP-G30 Installing the DWDM Cards • NTP-G152 Creating and Verifying Internal Patchcords, on page 114 • NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 100 • DLP-G46 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note Launch ANS applies the ANS parameters (calculated in the NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 100) to the node and to the ports for cards installed in the node. The applied ANS parameters include span loss values, threshold values, power references, and others. Launch ANS also sets the VOA references based on the calculated power references.

Note ANS provisioning parameters must be calculated by Cisco Transport Planner. ANS provisioning parameters must be manually changed only by Cisco qualified personnel. Setting wrong ANS provisioning (either as preamplifier or booster input power thresholds) may impact traffic.

Procedure

Step 1 Referring to the "Cisco Transport Planner Installation Parameters" table, identify the parameters that have a Yes in the Manually Set column. If there are no parameters that have a Yes in the Manually Set column, continue with Step 5.

Step 2 In CTC, display the card where the parameter is to be manually provisioned in card view.

Step 3 Enter the specified Calibration parameter from the Cisco Transport Planner Installation Parameters table. Click **Apply**.

Step 4 Repeat Steps 1 through 3 for each parameter in the Cisco Transport Planner Installation Parameters table that displays Yes in the Manually Set field.

Step 5 Change to node view (single-shelf mode) or multishelf view (multishelf mode).

Step 6 Click the **Provisioning** > **WDM-ANS** > **Port Status** tabs.

Step 7 Click **Launch ANS**.

Step 8 In the Apply Launch ANS dialog box, click **Yes**.

Step 9 In the Launch ANS confirmation dialog box, click **OK**.

Step 10 Verify that one of the following status appears in the Result column for all the ports:

- Success - Changed—The parameter setpoint was recalculated successfully.
- Success - Unchanged—The parameter setpoint did not need recalculation.
- Not applicable—When ports are not in use.

If one of the following statuses is shown, complete the provided instructions:

- Fail - Out of Range—The calculated setpoint is outside the expected range. If this status appears, do not continue until you have investigated and cleared the cause. This status might appear because of an error in the Cisco Transport Planner file. It could also appear because the insertion loss of the installed cards is greater than the estimated insertion loss calculated by Cisco Transport Planner. If so, the Cisco Transport Planner file will need to be recalculated. All of these possible causes should be investigated. Contact your next level of support if you are unable to clear this status.
- Fail - Missing Input Parameter—The parameter could not be calculated because the required provisioning data is unknown or unavailable. If this status appears, check if the correct Cisco Transport Planner file was imported.
- Unchanged - Port in IS—The parameter could not be calculated because the port is in service. This status should normally not appear at this point in node turn-up. If it does, display the card in card view, change the port administrative state to OOS,DSLB (ANSI) or Locked,disabled (ETSI), and repeat Steps 5 through 10.

Note
If the ports that are in service carry circuits, you must delete the circuits before you can place the ports out of service. See the Creating Optical Channel Circuits and Provisionable Patchcords chapter for information on circuit deletion.

Stop. You have completed this procedure.

NTP-G163 Upgrading Nodes in Single-Shelf Mode to Multishelf Mode

Purpose	This procedure upgrades nodes in single-shelf mode to multishelf mode.
Tools/Equipment	The node you plan to use as the node controller must be equipped with optical units and cannot have a cross-connect card installed. Any nodes that you plan to add to the multishelf configuration as subtending shelves can be equipped with transponder and muxponder units.
Prerequisite Procedures	NTP-G22 Verifying Common Card Installation, on page 56 One of the following procedures in the *Cisco NCS 2000 Series Hardware Installation Guide*: • NTP-L15 Connecting the NCS 2006 Multishelf Node and the NCS 2006 Subtending Shelves • NTP-L16 Connecting the NCS 2006 and the NCS in a Mixed Multishelf Configuration • NTP-L17 Upgrading the NCS Multishelf Configuration Using the NCS 2006 • NTP-Connecting the NCS 2006 Multishelf Node and the NCS 2006 Subtending Shelves with Simplex Controllers NTP-G318 Connecting the NCS 2006 Multishelf Node and the NCS 2006 Subtending Shelves in a Ring Topology DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser only

Note If a standalone node has unsupported cards, the node cannot be converted to a node controller or a subtended shelf controller.

Procedure

Step 1 If you want to configure a shelf as the node controller, continue with Step 2. If you want to configure a shelf as a subtending shelf, continue with Step 3.

Step 2 To set up the login node as the node controller, complete the following steps:

a) In node view (single-node mode) or multishelf view (multishelf mode), click the **Provisioning** > **General** > **Multishelf Config** tabs.
b) Click **Enable as Node Controller**.
c) Click **Apply**.
d) In the confirmation dialog box, click **Yes** to allow the node to reboot. The CTC view changes to network view and the node icon changes to gray. Wait for the reboot to finish. (This might take several minutes.)
e) After the node reboots, double-click the node. The multishelf view appears.

Note
The shelf ID of the node controller is automatically assigned as 1.

Step 3 To add a node as a subtending shelf in the multishelf configuration, complete the following:

a) In multishelf view, right-click in the white space in the rack and choose **Add Shelf**.
b) Select the type of subtending shelf.
c) In the Shelf ID Selection dialog box, choose a shelf ID (from 2 to 50 if the controller card is TNC, TNCE, TSC, TSCE) from the drop-down list.

Note
If a standalone node has unsupported cards, the node cannot be converted to a node controller or a subtended shelf controller.

d) Click **OK**. The shelf appears in the multishelf view.
e) Preprovision the new shelf so that it has the same provisioning as the actual shelf that you will add as the subtending shelf:

Caution
If the subtending shelf is not preprovisioned, traffic will be lost.

- Cards, PPMs, administrative states, client and trunk port configuration—For more information on card and port settings, see the Provisioning Transponder and Muxponder Cards chapter.
- Timing—For more information, see the NTP-G53 Set Up Timing procedure.
- GCC—For more information, see the DLP-G76 Provisioning DCC/GCC Terminations.

f) Disconnect the cross-over (CAT-5) LAN cable from the EMS port of NCS 2006 subtending shelf.
g) Connect your Windows PC or Solaris workstation NIC to the EMS port of the NCS 2006 subtending shelf.
h) Complete the DLP-G46 Log into CTC task at the subtending shelf.
i) Click the **Provisioning** > **General** > **Multishelf Config** tabs.
j) Click **Enable as Subtended Shelf**.
k) Select the appropriate subtending shelf.
l) From the Shelf ID drop-down list, choose the shelf ID that you created in Step c.
m) Click **Apply**.
n) In the confirmation dialog box, click **Yes** to reboot the shelf. The CTC view changes to network view and the node icon changes to gray. Wait for the reboot to finish. (This might take several minutes.)
o) Disconnect your Windows PC or Solaris workstation network interface card (NIC) from the EMS port of the NCS 2006 subtending shelf.
p) Reconnect the cross-over (CAT-5) LAN cable (disconnected in Step f) to the EMS port of the NCS 2006 subtending shelf.

Note

The Ethernet cable must be connected to the subtended shelf of the control card soon after the control card completes its boot phase (when it becomes active and its peer control card starts rebooting). Connecting it before the control card completes its boot phase is a risk in the conversion process. Connecting it long time after completion of the boot phase might affect traffic due to missing provisioning.

q) Repeat Steps a through p to set up additional subtending shelves.

Note
Cisco Transport Manager (CTM) users can use the CTM NE Explorer to monitor and configure single-shelf and multishelf nodes. When the upgrade is complete, the original individual subtending shelves will remain the CTM network view and must be manually deleted.

Stop. You have completed this procedure.

DLP-G730 Editing the Shelf ID of the Subtending Shelf in a Multishelf Configuration Using the LCD

Purpose	This task edits the Shelf ID of a subtending shelf using LCD on the fan try assembly. In an NCS 2006 shelf assembly, the LCD panel is a separate unit installed above the external connection unit (ECU).
Tools/Equipment	None
Prerequisite Procedures	NTP-G163 Upgrading Nodes in Single-Shelf Mode to Multishelf Mode, on page 134
Required/As Needed	As needed.
Onsite/Remote	Onsite
Security Level	Superuser only

Caution The traffic is lost when you change the Shelf ID of the subtending shelf in a multishelf configuration.

Note The LCD reverts to normal display mode after 5 seconds of button inactivity.

Procedure

Step 1 On the NCS front panel, repeatedly press the **Slot** button until SHELF appears on the first line of the LCD. You are in the Shelf menu.

Note

In a NCS 2006 shelf assembly, the LCD is a separate unit installed above the external connection unit (ECU); the **Slot**, **Port**, and **Status** buttons are present on the LCD unit.

Step 2 Repeatedly press the **Port** button until the "Controller Status = MS Configuration" appears on the LCD.

Step 3 Press the **Status** button to display the current multishelf configuration settings.

Step 4 Push the **Slot** button to move to the ID field that you want to change. The selected digit flashes.

Note
The Slot, Status, and Port button positions correspond to the positions of the commands shown on the LCD. For example, you press the Slot button to invoke the Next command and the Status button to invoke the Done command.

Step 5 Press the **Port** button to change the Shelf ID to the desired number.

Step 6 When the change is complete, press the **Status** button to return to the relevant Controller Status menu.

Step 7 Repeatedly press the **Port** button until the Shelf Save Configuration option appears.

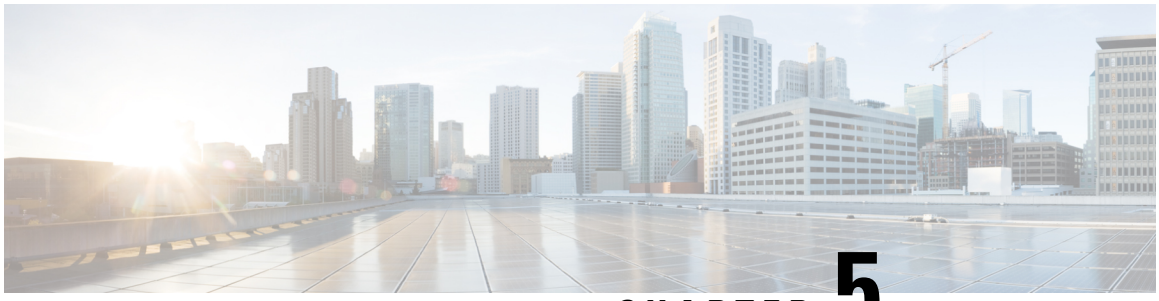
Step 8 Press the **Status** button to choose the Save Configuration option.

A Save and REBOOT message appears.

Step 9 Press the **Slot** button to apply the new Shelf ID or press **Port** to cancel the configuration.

Step 10 Saving the new configuration causes the control cards to reboot. During the reboot, a message appears on the LCD. The LCD returns to the normal alternating display after both the control cards finish rebooting.

Step 11 Return to your originating procedure (NTP).



CHAPTER 5

Synchronizing Node Timing

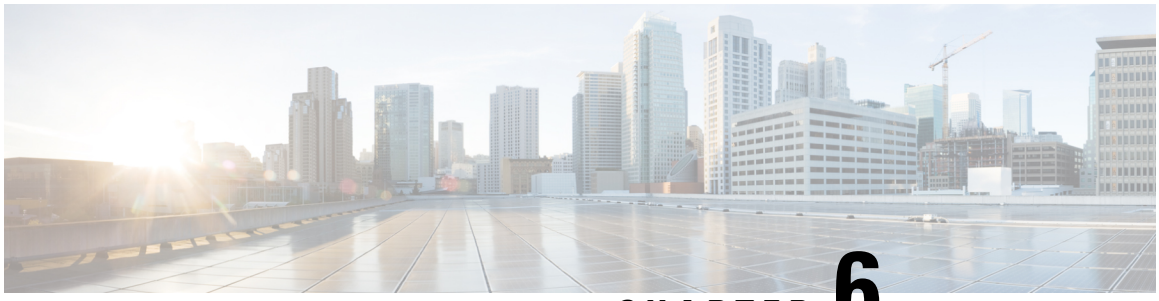
This chapter provides information about users and node timing parameters and network timing.

- Synchronizing Node Timing, on page 139

Synchronizing Node Timing

The information in this chapter is in a new location. See Timing Reference for information about users and node timing parameters, network timing, and Synchronization Status Messaging (SSM).

Synchronizing Node Timing



CHAPTER 6

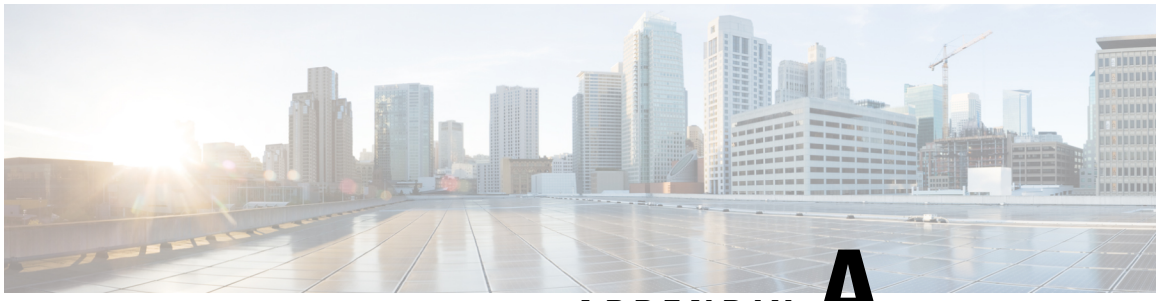
Provisioning Security

This chapter provides information related to user IDs and security levels, user privileges and policies, audit trail, and RADIUS security.

• Provisioning Security, on page 141

Provisioning Security

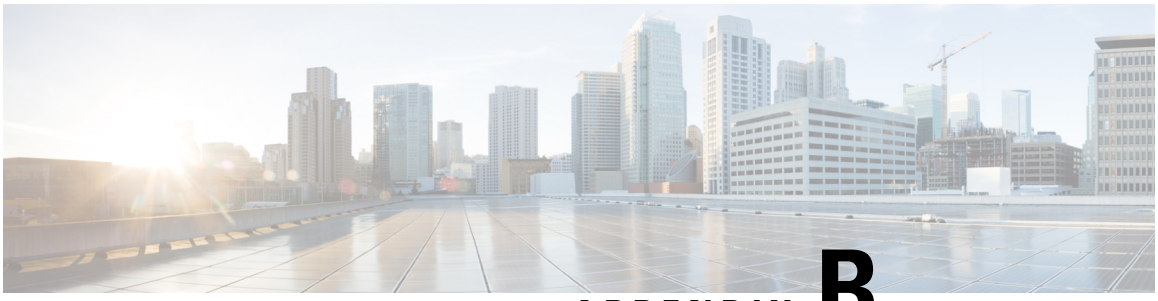
The information in this chapter is in a new location. See Security Reference for information related to user IDs and security levels, user privileges and policies, audit trail, and RADIUS security.



APPENDIX A

Card Specifications

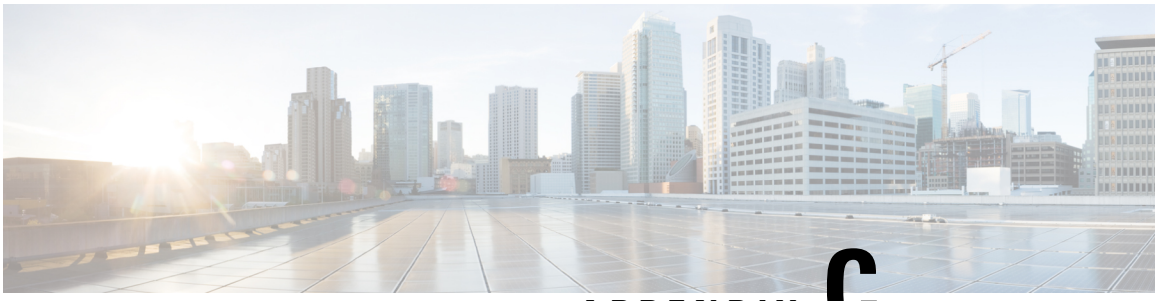
The information in this chapter is in a new location. See Hardware Specifications for information related to hardware and software specifications for the cards.



APPENDIX B

SNMP

The information in this chapter is in a new location. See SNMP for information related to Simple Network Management Protocol (SNMP).

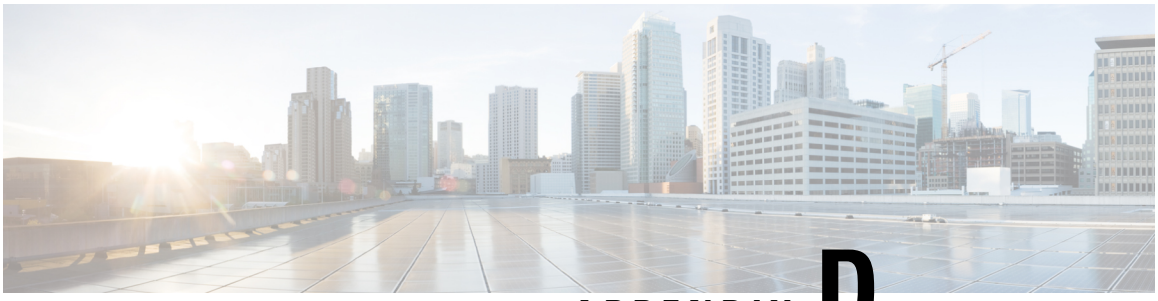


APPENDIX C

CTC Enhancements, Operations, and Shortcuts

The information in this chapter is in a new location. See CTC Enhancements, Operations, and Shortcuts for information on Cisco Transport Controller (CTC) views, menus options, tool options, shortcuts, table display options, and shelf inventory data presented in CTC.

CTC Enhancements, Operations, and Shortcuts



APPENDIX D

Network Element Defaults

The information in this chapter is in a new location. See Network Element Defaults for information related to factory-configured (default) network element (NE) settings.

Network Element Defaults



INDEX

A

adding 94–95
  static TID-to-NSAP entry to the TDC 94
  TARP MAT entry 95
administrative state, changing 133
  during ANS 133
ANS 55, 101, 133
  configuring with Cisco TransportPlanner 55, 101
  statuses 133
ANS parameters 103
  provisioning using the NE Update file 103
assigning 62, 64
  security in CTC 62
  user security level 64

B

battery power monitor thresholds 68

C

cards 103
  provisioning using the NE Update file 103
changing 75, 81, 133
  administrative state during ANS 133
  default router 75
  IP address 75
  network mask 75
  OSPF 81
Cisco Transport Controller. See<Default Para Font> CTC 3
Cisco TransportPlanner 54–55, 100–101, 106
  ANS configuration 55, 101
  importing the configuration file 100
  shelf layout report 106
  verifying reports and files 54
configuration file (Cisco TransportPlanner) 100
configuring 55, 79, 101
  ANS with Cisco TransportPlanner 55, 101
  SOCKS settings for secure mode 79
control cards 4
  card compatibility 4
cost 80–81
  when creating static routes 80
  when setting up or changing OSPF 81
creating 63–64, 80, 114, 116, 122, 125
  internal patchcord 114, 116
  internal patchcord using Card to Card 122, 125
  new user on a single node 63
  new users on multiple nodes 64
  static route 80
CTC 28, 62, 66, 69, 72, 84–85
  assigning security 62
  firewall access 85
  preventing IP address display 72
  Secure Mode 84
  setting up name, date, time, and contact information 66
  setting up network access 69
  verifying software release 28

D

database 22
  description 22
date 67
  provisioning 67
daylight savings time 68
DCN 89–90
DCU 107
  installing 107
default router 76
  changing using LCD 76
deleting 126, 128
  internal patchcords 126, 128
designated intermediate system priority. See<default para font> DIS
    priority 99

E

enabling 98
  OSI subnet on the LAN 98
End System Hello. See<default para font> ESH 98
ENEs, provisioning in secure mode 73
ES 98
external network element 73

F

firewall 85, 88
  provisioning IIOP listener port 88
  setting up 85

G

gateway network element 73
gateway settings. See<Default Para Font> proxy server 73
GNEs, provisioning in secure mode 73
GRE tunnel 100

H

hello interval 82–83
hops 80
  when creating static routes 80

I

IIH 131
IIOP listener port 88
  provisioning on the PC 88
importing 100
  Cisco TransportPlanner configuration file 100
installing 107
  DCUs 107
Intermediate System Hello. See<default para font> ISH 98
internal patchcord 103, 114, 116–117, 126, 128
  creating 114, 116
  deleting 126, 128
  provisioning OCH-Trunk to OCH-Filter option 116
  provisioning OCH/OCH to OTS/OCH option 117
  provisioning using the NE Update file 103
  verifying 114
internal patchcord using Card to Card 122, 125
  creating 122, 125
IP 70–71
  provisioning IP settings 70
  provisioning settings in secure vs. repeater mode 71
IP address 70–72, 76
  IP address using LCD 76
  preventing display in CTC 72
  provisioning dual 70
  provisioning network information 71
  restricting visibility 72
  viewing on LCD with secure mode enabled 76
IS Level 1/Level 2 91
IS-IS 98
  cost 98

L

LAN 71, 82
  OSPF activity 82
  provisioning default router during network setup 71
latitude 67
LCD 57, 70, 72, 75
  changing IP address, network mask, and default router 75
  provisioning network settings 70
  reading the software version on 57
  suppressing IP address display 72
listener port. See<Default Para Font> IIOP listener port 88
logging in 74
  when slow on large networks 74
longitude 67
LSP buffers 91–92

M

MAC address 71
  viewing 71
MTU 91
multishelf mode 59, 134
  provisioning a multishelf node 59
  upgrading from single shelf 134

N

networks 69
  setting up CTC network access 69
node 66, 85, 102
  accessing behind a firewall 85
  provisioning layout using the NE Update file 102
  setting up name, date, time, and contact information 66
NSAP 94, 96, 100
  adding a static TID-to-NSAP entry to the TDC 94
  adding NSAP address to TARP MAT 96
  provisioning NSAP address in IP-over-CLNS tunnel 100

O

optical sides, provisioning using the NE update file 103
OSC 130
  provisioning OSC terminations 130
OSI 90, 92, 96–99
  and secure mode 98
  enabling the OSI subnet on the LAN 98
  primary area address 97
  provisioning additional manual area addresses 97
  provisioning routers 96
  provisioning routing mode 90
  See also<Default Para Font> TARP [OSI 92
    zzz] 92
  tunneling. See<Default Para Font> IP-over-CLNS tunnel 99

OSPF 81
setting up or changing 81

P

passive shelves 111
firmware upgrade 111
passive units 109–110, 113
adding 109, 113
deleting 110
passwords 63–64
creating new user 63–64
PC setup 85
accessing behind a firewall 85
power 68
setting power monitor thresholds 68
PPMs 103
provisioning using the NE Update file 103
preferences, designating the SOCKS servers 74
preventing IP address display in CTC 72
protocols 67, 73
DHCP 73
NTP 67
SNTP 67
provisionable patchcord 78
functionality when Secure mode is enabled 78
provisioning 59, 67–68, 70, 80, 87, 96–97, 100, 130
multishelf nodes 59
network settings from the LCD 70
node date 67
NSAP addresses in IP-over-CLNS tunnels 100
OSC terminations 130
OSI manual area addresses 97
OSI routers 96
secure mode 87
subnet mask in a static route 80
time zone 68
Provisioning user. See<Default Para Font> security 63
proxy server 70, 73, 79
configuring SOCKS settings for secure mode 79
provisioning settings 70
provisioning SOCKS 73

R

repeater mode 71
provisioning IP settings 71
RIP 83

S

secure mode 71, 78, 87, 98
and OSI 98
provisionable patchcord functionality 78
provisioning 87
secure mode *(continued)*
provisioning IP settings 71
security 62, 64, 78
assigning in CTC 62
assigning user security level 64
PPCs when Secure mode enabled 78
setting 65, 68
battery power monitor thresholds 68
single node or multiple node 65
setting up 60, 66, 69, 81, 85, 135
CTC network access 69
firewall access 85
name, date, time, and contact information 66
OSPF 81
subtending shelf in a multishelf node 60, 135
SOCKS 74
designating the SOCKS server 74
static route 80, 83
creating 80
RIP prerequisite 83
subnet mask 71, 80, 83
OSPF area range table 83
provisioning in a static route 80
provisioning subnet mask length during network setup 71
subtending shelf 60, 134–135
setting up in multishelf nodes 60, 135
upgrading from single shelf 134
suppressing 72
LCD IP address display 72

T

TARP 94–95
adding a static TID-to-NSAP entry to the TDC 94
adding MAT entry 95
TARP data cache. See<default para font> TARP 89
TCC2 card 22
database back up 22
soft reset 22
TCC2P card 22
database back up 22
soft reset 22
TCC3 card 22
soft reset 22
time zone 68
provisioning 68
timed out. See<Default Para Font> idle time 64
timing 67
setting node clock 67
TNC card 22–23, 29–30
configuring UDC and VoIP 30
installing 23
provisioning PPM and port 29
soft reset 22
TNCS 17, 21
card workflow diagram 17

TNCS *(continued)*
related procedures 21
TNCS card 10
TSC card 22
soft reset 22

U

upgrading 134
to a multishelf configuration 134
users 63–65
creating on a single node 63
creating on multiple nodes 64
setting maximum password length 65

V

variable optical attenuator. See<Default Para Font> VOA 132
verifying 54, 114
Cisco TransportPlanner reports and files 54
internal patchcords 114
viewing 71
MAC address 71
virtual link table (OSPF) 83
VOA 132
running ANS 132

X

XML file 100