Cisco CPT Configuration Guide–CTC and Documentation Release 9.7.0.5 and Cisco IOS Release 15.2(02) SC5

First Published: 2015-06-16

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

Text Part Number: 78-21171-03

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.

Preface

Note The terms "Cisco CPT" and "CPT" are used interchangeably.

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

This section provides the following information:

Document Objectives

This guide provides information on the hardware and software features supported by Cisco Carrier Packet Transport. It also includes procedures to configure the supported features.

Audience

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

Document Organization

This document is organized into the following chapters:

Chapter	Description
Understanding the Carrier Packet Transport System, on page 3	Provides an overview of the Carrier Packet Transport (CPT) system and information about the CPT cards, CPT software features, and CPT configuration modes.
Hardware, on page 23	Describes the fabric card, line card, and CPT 50 panel. It also explains how to install the cards and the CPT 50 shelf.
Configuring Ethernet Virtual Circuit, on page 131	Describes Ethernet Virtual Circuit (EVC), EVC types, Ethernet Flow Point (EFP), and bridge domain. This chapter also describes procedures to configure EVC and EFP.
Configuring Multiprotocol Label Switching, on page 169	Describes Multiprotocol Label Switching and procedures to configure Multiprotocol Label Switching.
Configuring MPLS–Transport Profile, on page 283	Describes the Multiprotocol Label Switching–Transport Profile and procedures to configure Multiprotocol Label Switching–Transport Profile.
Configuring Pseudowire, on page 331	Describes static and dynamic pseudowires. This chapter also describes the configuration procedures of pseudowires.
Configuring Quality of Service, on page 401	Describes the Quality of Service and procedures to configure Quality of Service.
Configuring High Availability, on page 469	Describes Stateful Switchover, Cisco Nonstop Forwarding, and In-Service Software Upgrade. This chapter also describes the configuration procedures.
Configuring Resilient Ethernet Protocol, on page 495	Describes Resilient Ethernet Protocol (REP), REP configuration guidelines, VLAN load balancing, REP timers, and REP over EVC. This chapter also describes procedures to configure REP.
Configuring Link Aggregation Group and Link Aggregation Control Protocol, on page 533	Describes Link Aggregation Group and Link Aggregation Control Protocol and the configuration procedures.
Configuring MAC Learning, on page 575	Describes MAC learning and procedures to configure MAC learning.
Configuring Multicast VLAN Registration, on page 595	Describes Multicast VLAN Registration and procedures to configure Multicast VLAN Registration.
Configuring IGMP Snooping, on page 613	Describes IGMP Snooping and procedures to configure IGMP Snooping.

Chapter	Description
Configuring Performance Monitoring, RMON, OTN, and Port Provisioning, on page 741	Describes performance monitoring, Remote Monitoring, and Optical Transport Network and the configuration procedures.
Configuring Local Authentication, on page 781	Describes local authentication and procedures to configure local authentication.
Configuring Cisco Discovery Protocol, on page 793	Describes Cisco Discovery Protocol (CDP) and procedures to configure CDP.
Alarm Troubleshooting, on page 797	Describes CPT alarms.
SNMP, on page 847	Describes SNMP and the MIBs supported in CPT.
Configuring System Log, on page 861	Describes System Log and procedures to configure syslog
CPT Error Messages, on page 879	Describes the CPT error messages.
Network Element Defaults, on page 909	Describes the Network Element (NE) defaults supported on CPT 200 and CPT 600.

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.**

Warning	**IMPORTANT SAFETY INSTRUCTIONS** **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.** Statement 1071 **SAVE THESE INSTRUCTIONS**
Waarschuwing	**BELANGRIJKE VEILIGHEIDSINSTRUCTIES** **Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.** **BEWAAR DEZE INSTRUCTIES**
Varoitus	**TÄRKEITÄ TURVALLISUUSOHJEITA** **Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.** **SÄILYTÄ NÄMÄ OHJEET**
Attention	**IMPORTANTES INFORMATIONS DE SÉCURITÉ** **Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.** **CONSERVEZ CES INFORMATIONS**

Warnung	**WICHTIGE SICHERHEITSHINWEISE** **Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.** **BEWAHREN SIE DIESE HINWEISE GUT AUF.**
Avvertenza	**IMPORTANTI ISTRUZIONI SULLA SICUREZZA** **Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.** **CONSERVARE QUESTE ISTRUZIONI**
Advarsel	**VIKTIGE SIKKERHETSINSTRUKSJONER** **Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.** **TA VARE PÅ DISSE INSTRUKSJONENE**
Aviso	**INSTRUÇÕES IMPORTANTES DE SEGURANÇA** **Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.** **GUARDE ESTAS INSTRUÇÕES**
¡Advertencia!	**INSTRUCCIONES IMPORTANTES DE SEGURIDAD** **Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.** **GUARDE ESTAS INSTRUCCIONES**

Varning!	**VIKTIGA SÄKERHETSANVISNINGAR** **Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.** **SPARA DESSA ANVISNINGAR**
Figyelem	**FONTOS BIZTONSÁGI ELOÍRÁSOK** **Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.** **ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!**
Предупреждение	**ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ** **Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.** **СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ**
警告	重要的安全性说明 此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。 请保存这些安全性说明
警告	安全上の重要な注意事項 「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。 これらの注意事項を保管しておいてください。
주의	중요 안전 지침 이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오. 이 지시 사항을 보관하십시오.

Aviso	**INSTRUÇÕES IMPORTANTES DE SEGURANÇA** **Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.** **GUARDE ESTAS INSTRUÇÕES**
Advarsel	**VIGTIGE SIKKERHEDSANVISNINGER** **Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.** **GEM DISSE ANVISNINGER**
تحذير	**إرشادات الأمان الهامة** **يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز.** **قم بحفظ هذه الإرشادات**
Upozorenje	**VAŽNE SIGURNOSNE NAPOMENE** **Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.** **SAČUVAJTE OVE UPUTE**
Upozornění	**DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY** **Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.** **USCHOVEJTE TYTO POKYNY**
Προειδοποίηση	ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή. ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

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

Related Documentation

Use this guide in conjunction with the following referenced publications:

- *Cisco CPT Command Reference Guide-CTC and Documentation Release 9.3 and Cisco IOS Release 15.1(01)SA*
- *Cisco CPT Command Reference Guide-CTC and Documentation Release 9.7 and Cisco IOS Release 15.2(02)SA*
- *Upgrading the Cisco CPT to Release 9.7*
- *Cisco CPT Licensing Configuration Guide*
- *Cisco CPT Hardware Installation Guide*
- *Release Notes for Cisco CPT–CTC and Documentation Release 9.3 and Cisco IOS Release 15.1(01)SA*
- *Release Notes for Cisco CPT–CTC and Documentation Release 9.7 and Cisco IOS Release 15.2(02)SA*

Obtaining Optical Networking Information

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

Where to Find Safety and Warning Information

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

Cisco Optical Networking Product Documentation CD-ROM

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.

Cisco CPT Documentation Roadmap for Release 9.7.0.5

Technical Documentation Ideas Forum

Suggest ways Cisco technical documentation can be improved and better serve your needs. Participate in the Technical Documentation Ideas forum at http://www.cisco.com/go/techdocideas.

Download Software

Click the following link to download release specific softwares:

http://www.cisco.com/c/en/us/support/optical-networking/carrier-packet-transport-cpt-system/tsd-products-support-series-home.html

Note You must have a Cisco.com account to access the Download Software page. Go to the following link to register for a Cisco account:

Cisco.com Registration

Cisco Carrier Packet Transport (CPT)

To open a document, click the link provided:

- http://www.cisco.com/c/en/us/td/docs/optical/cpt/r_975/cpt9705_relnotes.html
- Cisco CPT Hardware Installation Guide
- http://www.cisco.com/c/en/us/td/docs/optical/cpt/r_975/cpt975_configuration.html
- Cisco CPT Command Reference Guide
- Cisco CPT Licensing Configuration Guide
- http://www.cisco.com/c/en/us/td/docs/optical/cpt/r_975/b_cpt_975upgrade.html

Other Documentation

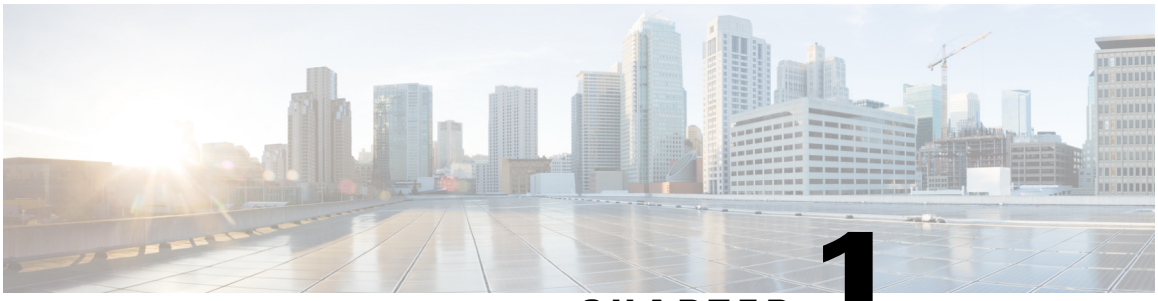
To open a document, click the link provided:

- http://www.cisco.com/en/US/docs/optical/cpt/compliance/RCSICPT.html
- Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms

Troubleshooting Tool

Click the link to open the:

- Return Material Authorization (RMA) Instructions
- RMA FAQs
- Support Tools and Resources



CHAPTER 1

New and Changed Information

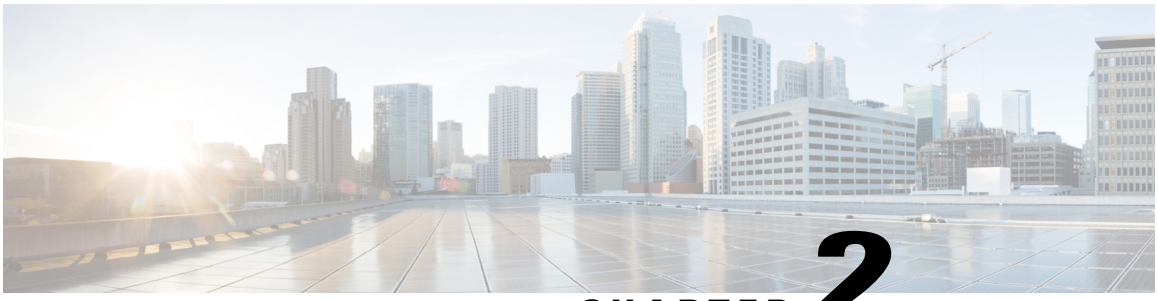
This chapter provides an overview of the significant changes made for this release.

New and Changed Information for Release 9.7.0.5

The following table provides an overview of the significant changes to this guide for Release 9.7.0.5.

Table 1: New and Changed Features for Release 9.7.0.5

Feature	Description	Where Documented
In-service VLAN edit	This feature provides the ability to support for VLAN edit operation for EVC, VPLS and VPWS features in CTC mode.	Edit EVC at DLP-J3 Edit an EVC Circuit Using CTC, on page 147 Edit VPLS at DLP-J336 Edit a VPLS Circuit Using CTC, on page 394 Edit VPWS at DLP-J223 Edit a Pseudowire Using CTC, on page 363
Inner/Outer VLAN CoS mapping	This feature provides the ability to support packet classification based on inner VLAN CoS or inner VLAN for double tagged packets for ingress QoS functions in CTC mode.	• DLP-J191 Creating or Editing a Class Map Using CTC, on page 411



CHAPTER 2

Understanding the Carrier Packet Transport System

This chapter describes the Cisco Carrier Packet Transport system. This chapter includes the following topics:

Carrier Packet Transport System

Packet-based services dominate the overall network traffic and as a result service providers are required to migrate their existing transport networks from time-division multiplexing (TDM) networks to packet transport networks. Service providers need next-generation transport networks that can enable and support new mesh, multipoint, and multidirectional services. By deploying packet transport networks, service providers can benefit from statistical multiplexing, dynamic bandwidth allocation, and quality of service (QoS).

The Carrier Packet Transport (CPT) system is designed to help service providers transition from TDM networks to packet transport networks smoothly and efficiently. The CPT System is an integrated packet transport platform that enables service providers to deploy new packet transport networks.

The CPT System is the first Packet–Optical Transport System (P–OTS) built on standards-based Multiprotocol Label Switching–Transport Profile (MPLS–TP) technology. The CPT System unifies both packet and transport technologies, giving service providers a strong foundation for next-generation transport. The CPT System is

designed to support transport applications so that service providers can continue to offer existing transport services while enabling new packet services.

The CPT System is a platform that provides architectural flexibility with support for MPLS–TP, IP/MPLS, and Carrier Ethernet transport. This provides service providers data plane and control plane flexibility in network deployments. The CPT platform enables service providers to provide mobile back-haul, Ethernet services, and TDM services for residential and business customers.

The CPT System integrates DWDM, Optical Transport Network (OTN), Ethernet, and standards-based MPLS-TP in a single system. The CPT System also integrates with other Cisco platforms such as the ONS 15454, Cisco ASR 9000 Series Router, and Carrier Routing System to deliver a combined IP/MPLS and MPLS–TP solution under a single control plane, forwarding mechanism, and Network Management System (NMS). This solution enables service providers to deploy this solution and interoperate with existing deployed IP/MPLS networks.

The CPT System works in the metro edge and access portion of the network providing an integrated packet and transport solution. The CPT System results in significant reduction in rack space and power consumption.

The CPT System offers:

- A unique architecture with remotely managed CPT 50 panels.
- High Gigabit Ethernet and 10 Gigabit Ethernet port density per rack unit.
- Integrated A-to-Z management for packet and transport.

Understanding CPT Cards

The CPT System is supported on the CPT 200 and CPT 600 chassis. The CPT 200 chassis consists of two service slots and has a 160 GB switch capacity. The CPT 600 chassis comes with six service slots and has a 480 GB switch capacity. For more information on CPT 200 and CPT 600 shelves, see the *Cisco CPT Hardware Installation Guide*.

There are two cards in the CPT System:

- Fabric card
- Line card

The CPT 50 panel is a stand-alone unit and can be connected to the CPT System. The CPT 50 panel enables you to scale the number of ports on the CPT System.

Fabric Card

The fabric card is a single slot card with two 10 Gigabit Ethernet SFP+ ports and two 10 Gigabit Ethernet XFP ports. The XFP ports on the fabric card support the OTN protocol. The fabric card provides high availability and high switching capacity. The 10GE XFPs of the fabric card removes the need to deploy additional transponders for DWDM applications. It also supports telnet connection.

Line Card

The line card has four 10 Gigabit Ethernet SFP+ ports. The line card expands the I/O capacity of CPT 200 and CPT 600 chassis by interconnecting with other line and fabric cards. It offers carrier class reliability, network flexibility, network ease of provisioning, and industrial grade Operations, Administration, and Maintenance (OAM).

CPT 50 Panel

The CPT 50 panel has four 10 Gigabit Ethernet SFP+ ports and 44 Gigabit Ethernet SFP ports. The CPT 50 panel can be deployed locally with the CPT 200 or CPT 600 or remotely up to 40 km away from the main chassis. The functionality of CPT 50 changes depending on its association with a fan-out-group (FOG) or a ring.

- CPT 50 as a FOG - The four 10 Gigabit Ethernet SFP+ ports can be used to connect with the fabric and line cards. The CPT 50 panel can be combined with CPT 200 or CPT 600 to create a platform that behaves as a single integrated system. The CPT 50 panel is managed as part of the same node, effectively as a virtual line card.
- CPT 50 in a Ring - The two 10 Gigabit Ethernet SFP+ ports (45 and 46) can be used to connect with the chassis (CPT 200 or CPT 600) or another CPT 50 in a ring. The other two 10 Gigabit Ethernet SFP+ ports (47 and 48) can be used as UNI ports. Each CPT 50 in a ring that is subtended from the chassis behaves as a system. It also supports telnet connection and FTP operations.

For more information on the CPT cards and CPT 50 panel, see the Hardware chapter.

CPT Software Features

The software features supported by the CPT System are shown in Table 2: CPT Software Features, on page 5.

Table 2: CPT Software Features

Feature	See
Ethernet Virtual Circuit (EVC)	Configuring Ethernet Virtual Circuit, on page 131
Multiprotocol Label Switching (MPLS)	Configuring Multiprotocol Label Switching, on page 169
Multiprotocol Label Switching – Transport Profile (MPLS–TP)	Configuring MPLS–Transport Profile, on page 283
Pseudowire	Configuring Pseudowire, on page 331
Quality of service (QoS)	Configuring Quality of Service, on page 401
Resilient Ethernet Protocol (REP)	Configuring Resilient Ethernet Protocol, on page 495
Link Aggregation Group (LAG)	Configuring Link Aggregation Group and Link Aggregation Control Protocol, on page 533
MAC Learning	Configuring MAC Learning, on page 575
Multicast VLAN Registration (MVR)	Configuring Multicast VLAN Registration, on page 595
IGMP Snooping	Configuring IGMP Snooping, on page 613

CPT Packet Profile Package

The CPT package is a single packet profile package that supports both SONET and SDH nodes. The terminology used in CPT package is similar to the terminology used in SONET.

The SONET and SDH nodes can be added to the CPT network through CTC. When the nodes are added to the CPT network, the respective configurations (SONET or SDH) are supported by the CTC session. The CPT nodes can be added to the CPT network even when there are non CPT nodes in the network. However, you cannot add both the SONET and SDH nodes to the same CTC session.

Configuration Rules

When both CPT and non CPT nodes are present in a shelf, the following configuration rules apply:

- Add SDH nodes of various types such as 15454SDH-DWDM LITE, 15454SDH-DWDM, 15454SDH-M6, and 15454SDH-M2 to CPT CTC. The terminology of the CPT nodes changes to the terminology of the SDH node. The change in terminology is specific only to the CTC session.
- Add SONET nodes of various types such as 15454-DWDM LITE, 15454-DWDM, 15454-M6, and 15454-M2 to CPT CTC. The terminology of the CPT nodes changes to the terminology of the SONET node. The change in terminology is specific only to the CTC session.
- The creation of Optical Channel Trail and Provisionable Patchcords is allowed between CPT and non CPT nodes.
- The non CPT nodes are not listed while creating L2+ services between CPT nodes.
- The nodes that belong to a different release and multishelf nodes are allowed in the same CTC session.
- The TL1 sessions for CPT nodes use SONET terminology.
- CPT supports FE/GE OSC provisioning; However, CPT does not support OC3 OSC provisioning.
- In the Edit -> Preferences -> Managed Network tab of CTC, the following options are listed:
  - ANSI and Packet (default option)
  - ETSI and Packet

  When you add the SDH nodes to the CPT network, the option changes automatically to ETSI and Packet. When you close the CTC session and start a new session, the option does not change back to ANSI and Packet. Hence, you need to manually change the option by editing the network preferences.

Supported Loopbacks

The following loopbacks are supported in CPT.

- Facility loopback at the interface level
- Terminal loopback at the interface level

Note The loopback can be only configured if port is in OOS-MT mode

Understanding CPT Configuration Modes

You can configure the CPT System features either through Cisco Transport Controller (CTC) or Cisco Internetwork Operating System (IOS) commands.

CTC

CTC is a Java application that is installed in two locations—it is stored on the Transport Node Controller (TNC) or Transport Shelf Controller (TSC) card and it is downloaded to your workstation the first time you log into the CPT System with a new software release.

Cisco IOS

Cisco IOS is the software used on the majority of Cisco systems routers and network switches. Cisco IOS is a package of routing, switching, internetworking, and telecommunications functions tightly integrated with a multitasking operating system.

The Cisco IOS is designed as a modal operating system. The term modal describes a system where there are different modes of operation, each having its own domain of operation. The CLI command mode structure is hierarchical, and each mode supports a set of specific commands.

The following table lists the common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 3: IOS CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	`Router>`	Issue the **logout** or **exit** command.	• Change terminal settings. • Perform basic tests. • Display device status.

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
Privileged EXEC	From user EXEC mode, issue the **enable** command.	`Router#`	Issue the **disable** command or the **exit** command to return to user EXEC mode.	• Issue **show** and **debug** commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the **configure terminal** command.	`Router(config)#`	Issue the **exit** command or the **end** command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the **interface** command.	`Router(config-if)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual interfaces.

Note Even in IOS mode, the following configurations can be performed only through CTC:

- Creating a Fan–Out–Group (FOG)
- Provisioning Pluggable Port Modules (PPM) and port
- Viewing performance monitoring parameters
- Configuring and monitoring Optical Transport Network (OTN) settings
- Modifying Ethernet settings and alarm thresholds
- Viewing Alarms
- Creating a provisionable patchcord
- Performing In-Service Software Upgrade (ISSU)
- Configure a Single-Homed or Dual-Homed ring

NTP-J20 Change the CPT System Configuration Mode Using CTC

Purpose	This procedure changes the CPT System configuration mode to CTC or Cisco IOS mode.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The fabric/line/CPT 50 card reboots when you change the configuration mode from CTC to Cisco IOS mode or vice versa.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to change the CPT System configuration mode.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Configuration Mode** tab.

Step 5 To change the CPT System configuration mode from CTC to Cisco IOS:

a) Click **IOS Mode**.

b) Click **Apply**. The Apply Provisioning Mode Change dialog box appears.

c) Click **Yes** in the dialog box to retain the configuration changes that were performed through CTC.

d) Click **No** in the dialog box to start the Cisco IOS mode with the default configuration.
The Provisioning tab, Maintenance (OAM) tab, and Service Level Alarm tab in CTC are disabled when you change the CPT System configuration mode from CTC to Cisco IOS.

Step 6 To change the CPT System configuration mode from Cisco IOS to CTC:

a) Click **CTC Mode**.

b) Click **Apply**. The Apply Provisioning Mode Change dialog box appears.

c) Click **Yes** in the dialog box to change the configuration mode to CTC.

Note The configuration changes performed through Cisco IOS are lost when you change the configuration mode from Cisco IOS to CTC.

Step 7 To open the Cisco IOS configuration mode using CTC, see DLP-J56 Open the Cisco IOS Configuration Mode and View the Feature Configuration Details Using CTC, on page 10.
Stop. You have completed this procedure.

DLP-J56 Open the Cisco IOS Configuration Mode and View the Feature Configuration Details Using CTC

Purpose	This procedure opens the Cisco IOS configuration mode and views the feature configuration details using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to open the Cisco IOS configuration mode and view the feature configuration details.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Maintenance** tab.

Step 4 From the left pane, click **IOS**.

Step 5 Click **Open IOS Connection**. The IOS Login dialog box appears.

Step 6 Enter the user name and password.

Step 7 Enter any show command.

Note You can use show commands in CTC and Cisco IOS to display the configuration status. When the **show** command with **more** option is simultaneously used in Cisco IOS and CTC, the system crashes.

Step 8 Press **Enter**. The output is displayed.

Step 9 Return to your originating procedure (NTP).

NTP-J21 Set Up the Computer for CTC

Purpose	This procedure configures your Windows PC or Solaris workstation to run CTC.
Tools/Equipment	CPT System software CD
Prerequisite Procedures	Install the CPT 200 and CPT 600 shelf.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	None

Procedure

Complete one of the following procedures:

- If your computer is a Windows PC, complete the DLP-J57 Run the CTC Installation Wizard for Windows PCs, on page 12 procedure.
- If your computer is a Solaris workstation, complete the DLP-J58 Run the CTC Installation Wizard for Solaris Workstations, on page 14 procedure.

Stop. You have completed this procedure.

DLP-J57 Run the CTC Installation Wizard for Windows PCs

Purpose	This procedure configures your Windows PC or Solaris workstation to run CTC.
Tools/Equipment	CPT System software CD
Prerequisite Procedures	None
Required/As Needed	This procedure is required if you use a Windows computer to run CTC and if any one of the following is true: • JRE 1.7 is not installed. • CTC online user manuals are not installed and are needed. • CTC JAR files are not installed and are needed.
Onsite/Remote	Onsite or remote
Security Level	None

Procedure

Step 1 Insert the CPT System software CD into your computer CD drive. The installation program begins running automatically. If it does not start, navigate to the CD directory and double-click **setup.exe**.
The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer:

- JRE 1.7
- Acrobat Reader 8.1.2
- Online User Manuals
- CTC JAR files

Step 2 Click **Next**.

Step 3 Complete one of the following:

- Click **Typical** to install the JRE, CTC JAR files, online user manuals, and Acrobat Reader. If you already have JRE 1.7 installed on your computer, choose **Custom**.
- Click **Custom** if you want to choose the components that you want to install. By default, Acrobat Reader and the online user manuals are selected. Check the CTC components that you want to install and click **Next**.

Step 4 Click **Next**.

The directory where the installation wizard will install the CTC online user manuals appears. The default is C:\Program Files\Cisco\CTC\Documentation.

Step 5 Click **Next**.

Step 6 Review the components that will be installed and click **Next**. It might take a few minutes for the JRE installation wizard to appear.

Step 7 To install the JRE, complete the following:

a) In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and accept the terms of the license agreement.

b) Click **Next**.

c) Choose one of the following:

- Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
- Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.

d) Click **Next**.

e) If you selected Typical, continue with 7.i, on page 13. If you selected Custom, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:

- Java 2 Runtime Environment—(Default) Installs JRE 1.7 with support for European languages.
- Support for Additional Languages—Adds support for non-European languages.
- Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

f) Click **Next**.

g) In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.

Note Setting the JRE as the default for these browsers might cause problems with these browsers.

h) Click **Next**.

i) Click **Finish**.

Step 8 In the Cisco Transport Controller Installation Wizard, click **Next**. The online user manuals and Adobe Acrobat Reader are installed.

Step 9 Click **Finish**.

Step 10 Return to your originating procedure (NTP).

DLP-J58 Run the CTC Installation Wizard for Solaris Workstations

Purpose	This procedure installs the CTC online user manuals, Acrobat 8.1.2, and JRE 1.7 on Solaris workstations, as necessary.
Tools/Equipment	CPT System software CD
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Procedure

Step 1 Change the directory. Enter:
cd /cdrom/cdrom0/

Step 2 From the CD directory, enter:
./setup.bat
The Cisco Transport Controller Installation Wizard displays the components that are installed on your computer:

- JRE 1.7
- Acrobat Reader 8.1.2
- Online User Manuals
- CTC JAR files

Step 3 Click **Next**.

Step 4 Complete one of the following:

- Click **Typical** to install both the JRE and the online user manuals. If you already have JRE 1.7 installed on your computer, choose **Custom**.
- Click **Custom** if you want to install either the JRE or the online user manuals.

Step 5 Click **Next**.

Step 6 Complete the following, as applicable:

a) If you selected Typical, continue with the next step.

b) If you selected Custom, check the CTC component that you want to install and click **Next**.

Step 7 The directory where the installation wizard installs the CTC online user manuals appears. The default is /usr/doc/ctc. Click **Next**.

Step 8 Review the components that will be installed and click **Next**. It might take a few minutes for the JRE installation wizard to appear.

Step 9 To install the JRE, complete the following:

a) In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and accept the terms of the license agreement.

b) Click **Next**.

c) Choose one of the following:

- Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
- Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.

d) Click **Next**.

e) If you selected Typical, continue with 9.i, on page 15. If you selected Custom, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:

- Java 2 Runtime Environment—(Default) Installs JRE 1.7 with support for European languages.
- Support for Additional Languages—Adds support for non-European languages.
- Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

f) Click **Next**.

g) In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.

Note Setting the JRE as the default for these browsers might cause problems with these browsers.

h) Click **Next**.

i) Click **Finish**.

Step 10 In the Cisco Transport Controller Installation Wizard, click **Next**. The online user manuals are installed.

Step 11 Click **Finish**.

Step 12 Return to your originating procedure (NTP).

NTP-J22 Log into CTC

Purpose	This procedure logs into the GUI of CTC.
Tools/Equipment	None

Prerequisite Procedures	NTP-J21 Set Up the Computer for CTC, on page 11
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note JRE 1.7 is required to log into nodes running CPT system.

Procedure

Step 1 From the computer connected to the CPT 200 or CPT 600 shelves, start Windows Internet Explorer (Windows PC) or Mozilla Firefox (Solaris workstation):

- If you are using a Windows PC, launch Windows Internet Explorer from the Windows Start menu or a shortcut icon.
- If you are using a Solaris workstation, determine the directory where Mozilla Firefox is installed by typing **whereis mozilla**, navigate to that directory and type:

  # mozilla -install

Step 2 In Windows Internet Explorer or Mozilla Firefox web address (URL) field, enter the CPT 200 or CPT 600 IPv4 or IPv6 address. For initial setup, this is the default IP address, 192.1.0.2.

Note The IP address appears on the LCD. You can suppress the LCD IP address display using CTC after you log in.

Step 3 Press **Enter**. The browser displays a window with a Delete CTC Cache field and information about the Cisco Transport Controller Java and System environments.

Note
- To log into CTC using an IPv6 address, you must first log into CTC using an IPv4 address and assign an IPv6 address to the node. Then, use the IPv6 address that you assigned to the node to log into CTC.
- The Delete CTC Cache field deletes the CTC JAR (Java Archive) files that are downloaded to your computer when you log into CPT 200 or CPT 600. You perform this action if connectivity problems occur or you want to delete older CTC JAR file versions from your computer.
- If you are logging into CPT 200 or CPT 600 nodes in an operation network that are running different releases of CTC software, log into the node running the most recent release. If you log into a node running an older release, you will receive an INCOMPATIBLE–SW alarm for each node in the network running a new release, and CTC will not be able to manage these nodes. To check the software version of a node, select **About CTC** from the CTC Help menu. This will display the software version for each node visible on the network view. If the node is not visible, the software version can be read from the LCD display.

Step 4 If a Java Plug-in Security Warning dialog box appears, complete the DLP-J59 Install the Public-Key Security Certificate Using CTC, on page 18 procedure to install the public-key security certificate.
After you complete the security certificate dialog box (or if the certificate is already installed), a Java Console window displays the CTC file download status. The web browser displays information about your Java and

system environments. If this is the first login, CTC caching messages appear while CTC files are downloaded to your computer. The first time you connect to CPT 200 or CPT 600, this process can take several minutes. After the download, a warning message window appears.

Step 5 Click **OK**. The CTC Login dialog box appears.

Step 6 In the CTC Login dialog box, type a user name and password (both are case sensitive).

Note
- For CPT 200 or CPT 600 shelves, the default user is CISCO15. CISCO15 has Superuser privileges, so you can create other users. You must create another Superuser before you can delete the CISCO15 user. CISCO15 is delivered with the otbu+1 password. To change the password for CISCO15, complete the DLP-J60 Change the User Password and Security Level on a Single Node Using CTC, on page 18 procedure after you log in to CTC.
- To access CPT 50 through console, the default user is CISCO15 and the default password is otbu+1. This password cannot be modified.

Step 7 Each time you log into CPT 200 or CPT 600, you can select the following login options:

- Additional Nodes — Displays a list of current login node groups.
- Disable Network Discovery — Check this box to view only the CPT 200 or CPT 600 (and additional nodes within the login node group, if any) entered in the Node Name field. Nodes linked to this node through DCCs are not discovered and will not appear in CTC network view. Using this option, you can decrease the CTC startup time in networks with many DCC–connected nodes, and can reduce memory consumption.
- Disable Circuit Management — Check this box to disable discovery of existing circuits. Using this option, you can decrease the CTC initialization time in networks with many existing circuits and reduce memory consumption. After you are logged in, you can enable circuit discovery at any time by choosing the Enable Circuit Discovery button on the Circuits tab.

Step 8 If you keep Disable Network Discovery unchecked, CTC attempts to upgrade the CTC software by downloading more recent versions of the JAR files it finds during the network discovery. Click **Yes** to allow CTC to download the newer JAR files, or **No** to prevent CTC from downloading the JAR files.

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

Step 9 Click **Login**.

If the login is successful, the CTC node view window appears. From here, you can navigate to other CTC views to provision and manage the CPT 200 or CPT 600 shelves.

Step 10 Perform the following procedures as needed:

- DLP-J60 Change the User Password and Security Level on a Single Node Using CTC, on page 18
- DLP-J59 Install the Public-Key Security Certificate Using CTC, on page 18

Stop. You have completed this procedure.

DLP-J59 Install the Public-Key Security Certificate Using CTC

Purpose	This procedure installs the ITU Recommendation X.509 public-key security certificate using CTC.
Tools/Equipment	None
Prerequisite Procedures	This procedure can be performed only during the NTP-J22 Log into CTC, on page 15 procedure.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note JRE 1.7 is required to log into nodes running CPT System.

Procedure

Step 1 If the Java Plug-in Security Warning dialog box appears, choose one of the following options:

- Yes—Installs the public-key certificate to your PC only for the current session. After the session is ended, the certificate is deleted. This dialog box will appear the next time you log into CPT 200 or CPT 600.
- No—Denies permission to install the certificate. If you choose this option, you cannot log into CPT 200.
- Always—Installs the public-key certificate and does not delete it after the session is over. It is recommended to use this option.
- More Details—Allows you to view the public-key security certificate.

Step 2 Return to your originating procedure (NTP).

DLP-J60 Change the User Password and Security Level on a Single Node Using CTC

Purpose	This procedure changes the settings for an existing user at one node using CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-J22 Log into CTC, on page 15

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

Note Each CPT 200 or CPT 600 must have only one user with a Superuser security level. The default CISCO15 user name and security level cannot be changed unless you create another user with Superuser security.

Procedure

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

Step 2 Click the user whose settings you want to modify, then click **Edit**.

Step 3 In the Change User dialog box:

- Change a user password.
- Modify the user security level.
- Lock out the user.
- Disable the user.
- Force the user to change password on next login.

Step 4 Click **OK**.

Step 5 Click **OK** in the confirmation dialog box.

Note The user settings that you changed during this procedure do not appear until that user logs out and logs back in.

Step 6 Return to your originating procedure (NTP).

DLP-J380 Create User Using CTC

Purpose	This procedure allows you to create a new user using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

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

Step 2 Enter the name of the user in the Name field.

Step 3 Enter the password in the Password field.

Step 4 Reenter the password in the Confirm Password field.

Step 5 From the Security-Level drop down list, choose security level.
Each user can be assigned one of the following security levels:

Type of User	Privileges
Retrieve-Users	Retrieve and view CTC information but cannot set or modify parameters.
Maintenance-Users	Access only the maintenance options.
Provisioning-Users	Access provisioning and maintenance options.
Superusers-Users	Perform all of the functions of the other security levels as well as set names, passwords, and security levels.

Step 6 Click **OK** to save the user.

Step 7 Return to your originating procedure (NTP).

DLP-J381 Delete User Using CTC

Purpose	This procedure allows you to delete an existing user using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J380 Create User Using CTC, on page 19
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

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

Step 2 Select the user to delete.

Step 3 Click **Delete**.

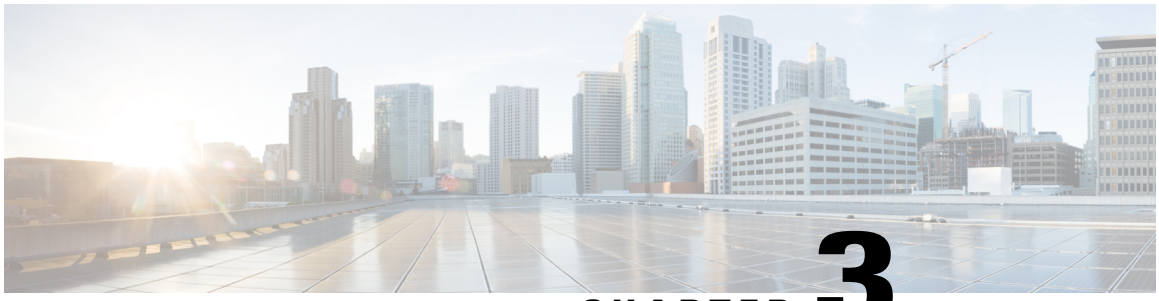
Step 4 Check Logout before Delete checkbox to end the telnet session.

Step 5 Click **OK** to delete the user.

Step 6 Return to your originating procedure (NTP).

Note When Line VTY is enabled, checking the Logout before Delete checkbox will not end the telnet session. To end the telnet session manually, run the following commands:**show users**

clear line <vty num>



CHAPTER 3

Hardware

This chapter describes fabric card, line card, and CPT 50 panel.

Introduction to Carrier Packet Transport Cards

This topic describes the Carrier Packet Transport (CPT) cards. There are two cards in the CPT system:

- Fabric Card
- Line Card

The CPT 50 panel is a standalone unit and can be connected to the CPT system. The CPT 50 panel enables the number of ports to be scaled on the CPT system.

These cards are supported on the CPT 200 and CPT 600 platforms. The CPT system complies with RoHS-6 standards.

The following system configuration is recommended on the CPT 200 shelf:

- Standalone fabric card
- Standalone TNC/TSC card
- One or more CPT 50 panels

The following system configuration is recommended on the CPT 600 shelf:

- Redundant fabric cards
- One line card

Note number of line card can be 4 in CPT600

- Redundant TNC/TSC cards
- One or more CPT 50 panels

Fabric Card

(CPT 200 and CPT 600 only)

The fabric card is a single slot card with two 10GE SFP+ ports and two 10GE XFP ports. The XFP ports on the fabric card support the Optical Transport Network (OTN) protocol. The SFP+ ports on the fabric card can serve as normal ports or InterConnect (IC) ports. When the SFP+ ports are used as IC ports, these ports are used to connect with the SFP+ ports on the CPT 50 panel.

The fabric card runs the route processor version of IOS. The fabric card manages the line card and the CPT 50 panel through the backplane GE management channel.

When fabric and line cards are installed on the shelf, a bidirectional 2 * 16G connection is set up between each fabric and line card and also between two fabric cards.

In chassis AC type, two fabric and two line cards are supported. In chassis DC type, there is no limit on the cards that are supported.

Circuit creation is possible only at XFP ports of the fabric card. Only OCHTRAIL creation is supported. Before creating the OCHTRAIL, create a provisionable patchcord (PPC) between the XFP port of the fabric card and the OCH port.

Slot Compatibility

On the CPT 600 shelf, install the redundant fabric cards in slots 4 and 5. There can be up to 2 fabric cards on the CPT 600 shelf. The two fabric cards on the CPT 600 shelf can both be in active mode with both cards carrying the traffic.

On the CPT 200 shelf, install the fabric card in slot 2 or 3.

Faceplate and Block Diagram

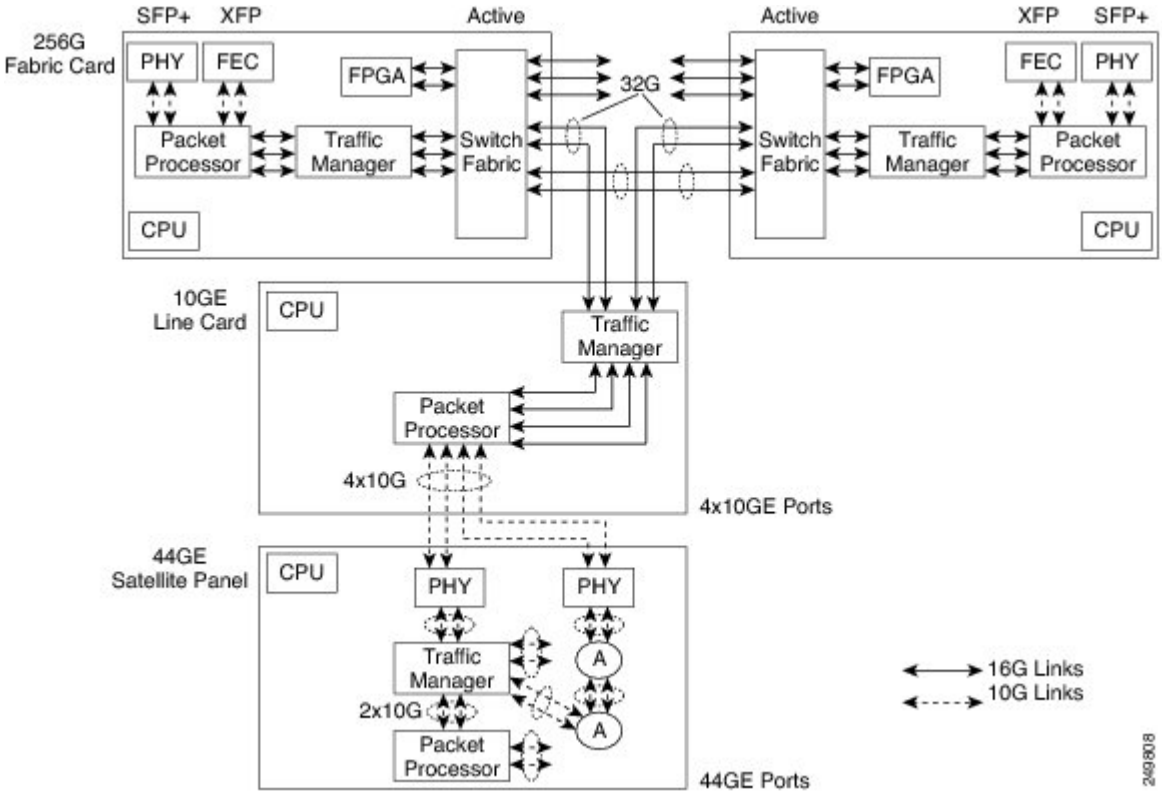
Figure 1: Fabric Card Faceplate, on page 25 illustrates the faceplate of the fabric card.

The FPGA on the fabric card processes the traffic packets. The console port on the faceplate is used for debugging.

Figure 1: Fabric Card Faceplate

Figure 2: CPT System Block Diagram, on page 26 illustrates the CPT system block diagram.

Figure 2: CPT System Block Diagram



Card-Level Indicators

Table 4: Card-Level Indicators

Card-Level LED	Description
Red FAIL LED	The red FAIL LED indicates that the processor of the card is not ready. This LED is on during the reset. The FAIL LED flashes during the boot process. Replace the card if the red FAIL LED persists.
Green ACT LED	If the ACT LED is green, the card is operational (one or more ports active) and ready to carry the traffic.
Amber SF LED	The amber SF LED indicates that a signal failure or condition such as LOS, LOF, or high BERs is present in one or more of the ports of the card. The amber SF LED is also on if the transmit and receive fibers are incorrectly connected. If the fibers are properly connected and the link is working, the light turns off.

Port-Level Indicators

A port status LED is provided for each SFP+ port and XFP port on the fabric card. The XFP ports on the fabric card have only Link LEDs and no ACT LEDs.

Table 5: Port-Level Indicators

Port-Level LED	Description
Link LED	Green—The port is either in–service and receiving a recognized signal (that is, no signal fail), or out–of–service and maintenance (OOS,MT or locked, maintenance) in which case the signal fail and alarms are ignored. Red—The port is in–service but is receiving a signal fail (LOS). Amber—The port is provisioned and is in a standby state.
ACT LED	Indicates data reception. The LED blinks on packet flow.

Line Card

(CPT 200 and CPT 600 only)

The line card has four 10GE SFP+ ports. The SFP+ ports on the line card serve as normal ports or InterConnect (IC) ports. When the SFP+ ports are used as IC ports, these ports are used to connect with the SFP+ ports on the CPT 50 panel. The line card runs the line card version of IOS.

When fabric and line cards are installed on the shelf, a bidirectional 2 * 16G connection is set up between each fabric card and each line card and also between two fabric cards.

Slot Compatibility

On the CPT 600 shelf, install the line cards in slots 2, 3, 6, and 7. There can be up to four line cards on the CPT 600 shelf. However, the line card is not required to be present on the CPT 600 shelf.

On the CPT 200 shelf, install the line card in slot 2 or 3. There can be a single line card on the CPT 200 shelf. However, the line card is not required to be present on the CPT 200 shelf.

Line Card States

The line card could be in one of the following states:

- Empty slot
- Card pre-provisioned
- Card plugged-in

- Image downloading
- Application initialization
- Ready

Faceplate

Figure 3: Line Card Faceplate, on page 28 illustrates the faceplate for the line card. The console port on the faceplate is used for debugging.

Figure 3: Line Card Faceplate

Card-Level Indicators

Table 4: Card-Level Indicators, on page 26 provides information on card–level indicators.

Port-Level Indicators

A port status LED is provided for each SFP+ port on the line card.

Table 5: Port-Level Indicators, on page 27 provides information on port–level indicators.

CPT 50 Panel

(CPT 200 and CPT 600 only)

The CPT 50 panel enables the number of ports to be scaled on the CPT system. The CPT 50 panel has 4 10GE SFP+ ports and 44 GE SFP ports. The CPT 50 panel runs the line card version of IOS.

Note The CPT 50 panel is not placed in the CPT 200 or CPT 600 shelf.

Note The CPT 50 panel should be of REV 5 hardware. To check the hardware, run the following command: **show version**.

The CPT 50 panel cannot operate independently. After connecting the CPT 50 panel to the fabric card or the line card, the CPT 50 panel is automatically discovered and registered. The discovery operation is performed using the Satellite Discovery Protocol (SDP) and the registration operation is performed using the Satellite Registration Protocol (SRP).

The four SFP+ ports on the CPT 50 panel can be connected to the SFP+ ports on the fabric card or the line card. The four SFP+ ports on the CPT 50 panel can be connected to only one card (fabric or line card) at a time.

CPT 50 shelf supports ONE-GE and FE for 1 to 44 ports. CPT 50 shelf supports TEN-GE for 45 to 48 ports. By default, the 45 to 48 ports are in IC mode and cannot be changed.

The CPT 50 panel has redundant DC feeds. The CPT 50 panel DC power supply can handle 48 V and 24 V. The 48 V power supply has both ANSI and ETSI versions.

The CPT 50 panel has a removable fan tray and a local console port for onsite access and debugging.

TDM SFP on a CPT 50 panel is supported even if the other end of the static pseudowire is connected to a Cisco ASR 9000 Series Router or a Cisco 7600 Series Router.

Faceplate

There are four variations of the CPT 50 panel faceplate:

- CPT 50 panel with AC power. See Figure 4: CPT 50 panel with AC Power Faceplate, on page 29.
- CPT 50 panel with DC ETSI 48 V. See Figure 5: CPT 50 panel with DC ETSI 48 V Faceplate, on page 29.
- CPT 50 panel with DC ANSI 48 V. See Figure 6: CPT 50 panel with DC ANSI 48 V Faceplate, on page 29.
- CPT 50 panel with DC ANSI 24 V. See Figure 7: CPT 50 panel with DC ANSI 24 V Faceplate, on page 29.

Figure 4: CPT 50 panel with AC Power Faceplate

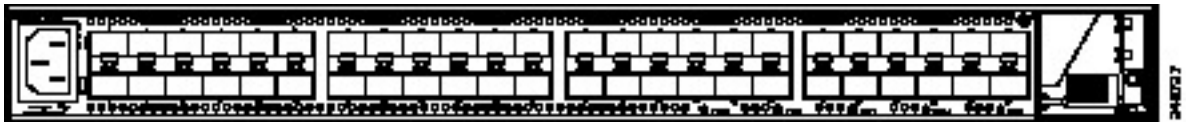


Figure 5: CPT 50 panel with DC ETSI 48 V Faceplate

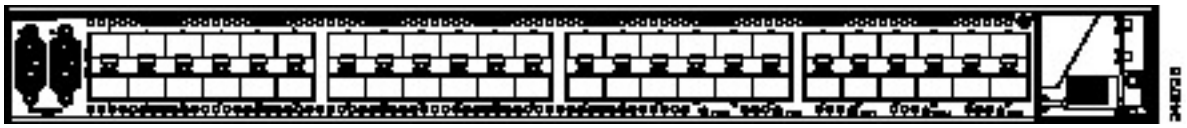


Figure 6: CPT 50 panel with DC ANSI 48 V Faceplate

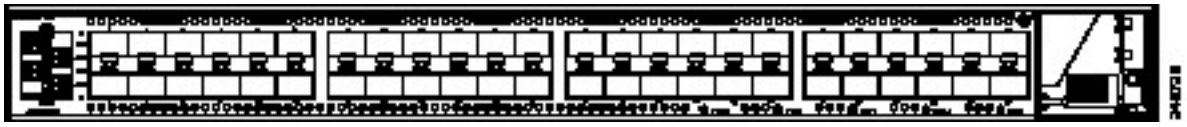
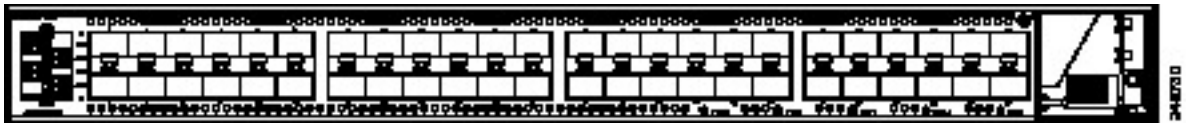


Figure 7: CPT 50 panel with DC ANSI 24 V Faceplate



Card–Level Indicators

Table 6: CPT 50 Panel Card–Level Indicators

Card-Level LED	Description
PWR	Indicates the status of the power to the card. If there is a power failure, this LED turns red.
FAN	Indicates the status of the fan to the card. If there is a fan failure, this LED turns red.
CRIT	Indicates the critical alarms in the network at the local terminal.
MAJ	Indicates the major alarms in the network at the local terminal.
MIN	Indicates the minor alarms in the network at the local terminal.

Supported CPT 50 Panels on the CPT System

- The CPT system supports up to 20 CPT 50 panels or 880 GE ports on the CPT 600 shelf.
- The CPT system supports up to 6 CPT 50 panels or 264 GE ports on the CPT 200 shelf.

The limit on the number of ports is not enforced by CTC.

CPT 50 Panel States

The following states are defined for a CPT 50 panel that is configured in the CPT system:

- Pre–provisioned—When the 10GE ports on the fabric or the line card are configured as IC ports and when these IC ports are associated with a Fan-Out-Group (FOG).
- Loading—When the CPT 50 panel has booted up with the IOS image and when the line card version of IOS is being downloaded from the fabric card.
- Active—When the CPT 50 panel boots up with the line card image and the application initialization is completed.

CPT 50 Panel Connectivity to the Fabric or Line Card

If the CPT 50 shelf loses connectivity to the fabric or line card due to interconnect (IC) link down events, the CPT 50 shelf reloads after the last IC link in the FOG (Fan-Out-Group) fails. This reload occurs after the configured carrier time delay. If there is a connection loss due to remote failures, the CPT 50 shelf reloads after detecting the failure time-out period (5 seconds) for the last link that was active. When the reload is complete, the CPT 50 shelf tries to reestablish the connection to the fabric or line card by performing the discovery operation. If the discovery operation is not successful within 5 minutes, the CPT 50 shelf reloads again. This cycle is repeated thrice with a reduction in the time-out period (30 seconds), until the discovery operation is successful. In the event of successful discovery, the CPT 50 shelf reestablishes the connection to the fabric or line card, else the CPT 50 shelf transits to the idle state and then attempts to connect to the fabric or line card.

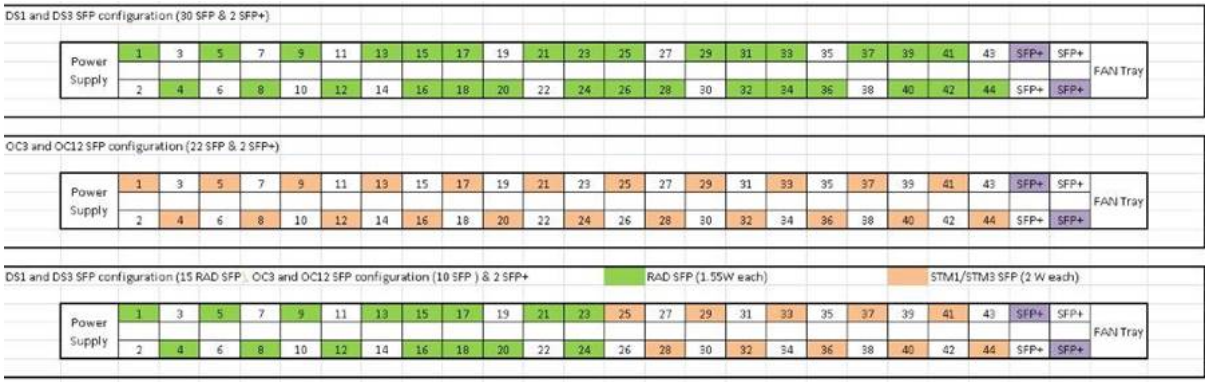
Interlink Protection

If one of the links in the FOG is down, the traffic sent on that link is switched and distributed to the remaining active links in the FOG.

Hardware Restrictions

At any given time, only 12 TDM SFP modules can be connected to a CPT 50 panel. With these modules, 15 SFP modules and 2 SFP+ modules can also be connected. For information about SFP and SFP+ modules, see the Pluggables compatible with Cisco CPT 50.These SFP and SFP+ modules can be connected to only selected ports of the CPT 50 panel. See

Figure 8: TDM SFP Configuration



Only the ports highlighted in green can be used to connect TDM SFP modules or any other SFP modules. The ports highlighted in purple can be used only to connect SFP+ modules.

Note Ensure to close the remaining ports with cage caps. The Cisco part number for a cage cap is 51-2870-01.

Note TDM interoperability is not supported in IOS mode. To support the TDM interoperability, user shall provision the TDM SFP in CTC mode.

Software Restrictions

The following software restrictions apply to the CPT 50 panel:

- The CPT system supports up to 880 GE ports on the CPT 600 shelf and these ports are distributed among 1 to 20 CPT 50 panels.
- The CPT system supports up to 264 GE ports on the CPT 200 shelf and these ports are distributed among 1 to 6 CPT 50 panels.

  The limit on the number of ports is not enforced by CTC.
- Each CPT 50 panel can be connected to only one fabric or line card at a time.
- Only one FOG can be created for each CPT 50 panel.

Pre-provisioning

The following can be pre-provisioned through CTC:

- Fabric card
- Line card
- FOG
- TEN-GE PPMs
- Port states
- OTN parameters

The ONE-GE and FE PPMs are not pre-provisioned by default.

NTP-J19 Install the Fabric and Line Cards

Purpose	(CPT 200 and CPT 600 only) This procedure installs the fabric and line cards on the CPT 200 and CPT 600 shelves. On the CPT 600 shelf, install the redundant fabric cards in slots 4 and 5. On the CPT 200 shelf, install the fabric card in slots 2 or 3. On the CPT 600 shelf, install the line cards in slots 2, 3, 6, and 7. On the CPT 200 shelf, install the line card in slots 2 or 3.
Tools/Equipment	Fabric and line cards.
Prerequisite Procedures	DLP–G604 Install the TNC or TSC Card in *Cisco ONS 15454 DWDM Configuration Guide*
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

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

Warning Class 1 laser product. Statement 1008

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

Warning Class 1 laser product. Statement 1008

Caution Always use the supplied ESD wristband when working with a CPT 200 and CPT 600 shelf. For detailed instructions on how to wear the ESD wristband, refer to the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.

Note If protective clips are installed on the backplane connectors of the cards, remove the clips before installing the cards.

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

Note It is recommended to clear the **database**before performing any configuration if you are inserting the TNC/TSC card and no other card is present on the chassis.

Procedure

Step 1 Navigate to the Cisco Transport Planner shelf layout for the node where you will install the fabric or line card.

Step 2 Remove the card from its packaging, then remove the protective clips from the backplane connectors.

Step 3 Open the card ejectors.

Step 4 Hold the card firmly and align it to the guard rails and slide it inside the slot until the card plugs into the receptacle at the back of the slot designated by the Cisco Transport Planner shelf layout.

Step 5 Verify that the card is inserted correctly and simultaneously close the ejectors on the card.

Note It is possible to close ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Note If you install the card in the wrong slot, CTC will raise a MEA (EQPT) alarm. To clear this alarm, open the ejectors, slide the card out, then insert it in the correct slot.

After you install the card, the FAIL, ACT, and SF LEDs will go through a sequence of activities. They will turn on, turn off, and blink at different points. After approximately 2 to 3 minutes, the ACT or ACT/STBY LED turns on. The SF LED might persist until all card ports connect to their far-end counterparts and a signal is present.

Note Until a card is provisioned, the card is in the standby condition and the ACT/STBY LED remains amber in color.

Step 6 If the card does not boot up properly or the LEDs do not progress through the activities described in step 5, check the following:

- When a physical card type does not match the type of card provisioned for that slot in CTC, the card might not boot and CTC will show a MEA (EQPT) alarm. If the card does not boot, open CTC and ensure that the slot is not provisioned for a different card type before assuming that the card is faulty.
- If the red FAIL LED does not turn on, check the power.
- If you insert a card into a slot provisioned for a different card, all LEDs turn off.
- If the red FAIL LED is on continuously or the LEDs behave erratically, the card is not installed properly.

If any of these conditions are present, remove the card and repeat steps 3 to 5. If the card does not boot up properly the second time, contact your next level of support.

Note Until a card is provisioned, the card is in the standby condition and the ACT/STBY LED remains amber in color.

Stop. You have completed this procedure.

NTP-J72 Create a Fan–Out–Group Using CTC

Purpose	This procedure creates a Fan–Out–Group (FOG) using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

By default, the SFP+ ports on the fabric or line cards are configured as 10GE ports. These ports need to be configured as IC ports and associated to a FOG to connect these ports to the CPT 50 panel. FOG is a logical channel that consists of a bundle of 10GE IC ports.

The CPT 50 panel can be connected to the fabric card using two IC ports. The CPT 50 panel can be connected to the line card using four IC ports.

The 4 SFP+ ports that are displayed as 1+ 2+ 3+ 4+ on the faceplate of the CPT 50 panel are displayed as 45, 46, 47, 48 in CTC. This includes the display in Alarms and Performance Monitoring.

Note You can create only one FOG for each CPT 50 panel.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to configure the SFP+ ports as IC ports.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Fan-Out Groups** tab.

Step 5 Click **Create**. The Create/Edit Fan-Out Group dialog box appears.

Step 6 From the Fan-Out Group ID drop-down list, choose a FOG ID. FOG ID is the virtual slot ID of the CPT 50 panel and takes values from FOG 36 to FOG 55.

Step 7 From the Card Slot drop-down list, choose a slot.

Step 8 From the Available Fan–Out Ports area, choose the required ports that you want to configure as IC ports and move these ports to the Available Fan–Out Group Member Ports area.

Step 9 Click **Apply** to create a FOG that consists of the selected ports.

Note The CPT 50 panel comes up only when the SFP+ port of the card from where it is connected is not in OOS,DSBLD administrative state.

Stop. You have completed this procedure.

Understanding Rings

The Carrier Packet Transport (CPT) system provides the ability to operate CPT 50 in a physical ring homed back to a single CPT 600 or CPT 200 chassis. This feature provides the flexibility of connecting CPT 50 in a closed-ended ring or an open-ended ring. As a result, the failure of a line or uplink card does not impact the traffic in a ring. CPT 50 in a ring works like a route processor and each CPT 50 interacts with Transport Node Controller (TNC) directly.

These sections describe more about the rings feature in CPT:

- Common Terms in Rings, on page 35
- Ring Types, on page 36
- Supported Traffic Patterns, on page 38
- Supported CPT 50 Rings Deployment Scenario, on page 39
- Limitations and Restrictions, on page 39

Common Terms in Rings

This section describes the common terms in rings.

- Topology discovery - This refers to the functionality that discovers nodes in a CPT 50 ring using REP and report it to the topology management functions residing on TNC.

- CPT 50 in a ring - This is an instance of CPT 50 that is loaded with the CPT 50 rings software and deployed in a ring subtended from CPT 600 or CPT 200.
- Ring Controller - For a provisioned ring, this refers to the following:
  - CPT 600 or 200 network element settings from which the provisioned ring is subtended.
  - TNC card from which the nodes are managed.
- Open-ended ring - This is a type of ring that is connected to CPT 600 or CPT 200 through only one interface and does not terminate on the headend. Hence, only one unprotected path gets available to the traffic on the ring.
- Closed-ended ring - This is a type of ring that is provisioned to connect to CPT 600 or CPT 200 through two interfaces on CPT 600 or 200. Hence, a protected path gets available to the traffic either through the east or west interface on the ring.
- Working Ring Controller (WRC) - For a provisioned dual-homed ring, this refers to other CPT 600 or CPT 200 network element from which the provisioned ring is subtended.
- Protect Ring Controller (PRC) - For a provisioned dual-homed ring, this refers to the other CPT 600 or 200 network element that provide node protection to WRC.
- Ring island - This indicates a ring of the CPT 50s that has lost the connectivity to CPT 600 or CPT 200. In open-ended ring, ring islands are caused by a single link failure from the east port of the ring controller. This can also be caused by a failure of one of the CPT 50s in the ring.

  In closed-ended ring, ring islands are caused by two link failures between the east and the west port of the ring controller.

  In dual homed ring, ring islands are caused by two link failures between the ring ports of the ring controller. This can also be caused by a failure of one of the CPT 50s in the ring.
- Golden image - This is an image stored on the CPT 50 panel that runs a software to establish control connection between the CPT 50 and CPT 600 or CPT 200 and downloads the kernel image from it.
- Kernel image - This refers to the CPT 50 application image that is downloaded by the golden image.
- Boot Up - This is a boot-up sequence for CPT 50 that comprises the following steps:
  - Download kernel image, and allow the Boot VLAN transit traffic.
  - Boot to kernel image, and allow boot VLAN and control VLAN transit traffic based on the REP convergence.
  - Discover a unique identifier (ID) for CPT 50 and IP address from TNC.
  - Discover active TNC, and establish a connectivity with TNC.
  - Download database from TNC, and restore equipment and service configurations.

Ring Types

CPT supports the following types of ring:

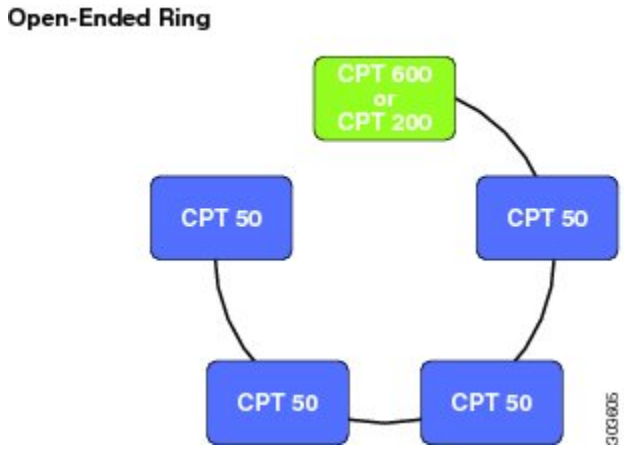
Single-Homed Ring

A Single-homed ring is the ring that is subtending from a single CPT-600 or CPT 200 in a linear or close-ended form. Following are the types of single-homed ring:

Open-Ended Ring

An Open-ended ring is the ring that is connected to a CPT 200 or CPT 600 through one port. It follows the linear topology. To create this type of ring, only the east port is required.

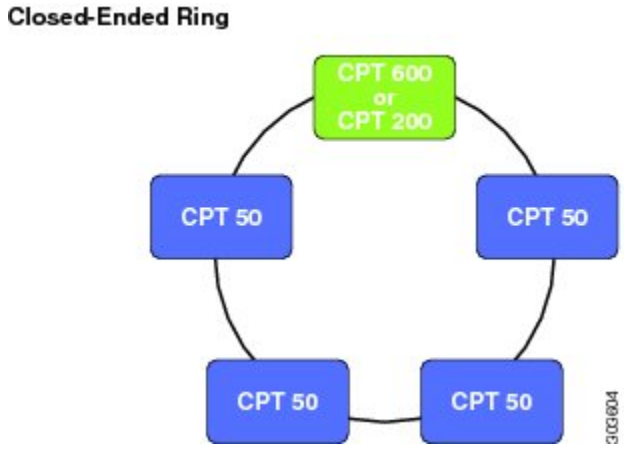
Figure 9: Open-Ended Ring



Closed-Ended Ring

A Closed-ended ring is the ring that is connected to a CPT 200 or CPT 600 through two interfaces. It follows the ring topology. To create this type of ring, both the east and west ports are required. It provides protection to the circuits and the control traffic.

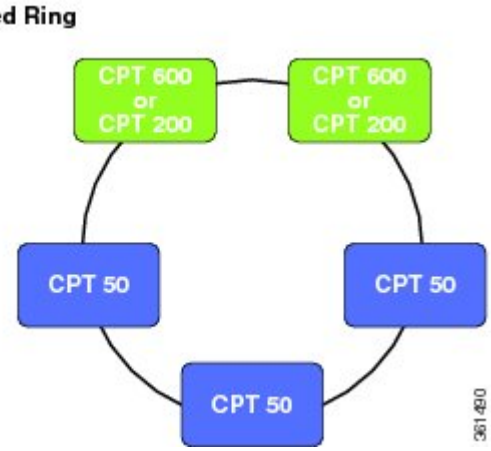
Figure 10: Closed-Ended Ring



Dual-Homed Ring

A Dual-homed ring is the ring whose east port exists on one CPT 200 or CPT 600 (WRC) and west port exists on another CPT 200 or CPT 600 (PRC). If WRC fails, this type of ring provides access to all the CPT 50s in the ring by switching the traffic to the other controller.

Figure 11: Dual-Homed Ring



Supported Traffic Patterns

The following MPLS-TP tunnel traffic is supported over a ring:

- Protected or unprotected MPLS–TP tunnel traffic from CPT 50 to the headend (CPT 600 or CPT 200).
- Protected or unprotected MPLS-TP tunnel traffic from CPT 50 to another CPT 50 in the same ring controller.
- Protected or unprotected MPLS-TP tunnel traffic from CPT 50 to another CPT 50 in another ring on the same headend.
- Protected or unprotected MPLS-TP tunnel traffic from CPT 50 to another CPT600 or CPT 200 that is reachable through the ring controller.
- Protected or unprotected MPLS-TP tunnel traffic from CPT 50 to another CPT 50 (in a ring) in another CPT 600 or CPT 200 that is reachable through the ring controller.
- Protected or unprotected MPLS-TP tunnel traffic from CPT 50 to another CPT 50 (in a fan-out group) in another CPT 600 or CPT 200 that is reachable through the ring controller.

The following services are supported over a ring:

- Ethernet services from CPT 50 UNI (front ports) realized through VPWS or VPLS over MPLS-TP tunnels on the ring.
- MPLS traffic from CPT 50 front ports stitched to VPLS or VPWS services over MPLS-TP tunnels on the ring.
- MS-PWE3 traffic from the core stitched to VPLS or VPWS services over the MPLS-TP tunnels on the ring.

• Multipoint E-LAN services with local connect .

Supported CPT 50 Rings Deployment Scenario

The CPT 50 rings architecture is raised over the CPT 50 standalone framework. CPT 50 in a ring provides a ring-based protection to the data path and the control path.

A ring can be subtended from a single CPT 600 or CPT 200 in a linear or close-ended form and are termed as single-homed rings. It can also be subtended from two interconnected CPT 600 or CPT 200 and are termed as dual-homed rings. From a CPT 600, 20 open-ended and 10 closed-ended single-homed rings can be subtended and up to 10 dual-homed rings can be subtended. From a CPT 200, six open-ended and three closed-ended single-homed rings can be subtended and up to three dual-homed rings can be subtended.

The CPT-50 support MPLS-TP based transport over the single-homed and dual-homed rings.

E-Line is realized using VPWS across the rings. E-LAN is realized using VPLS across the rings and using local switching within a CPT-50. Carrier Ethernet is not supported across the ring. Carrier Ethernet services in this case indicate E-Line and E-LAN services realized through P2P and P2MP Ethernet switching .

CPT 50 in ring mode can be provisioned through CTC only. This section describes the scenarios in which a ring can be configured using CPT 50 and the supported software features.

MPLS-TP Tunnels in a Ring

MPLS-TP tunnels in a ring can be created manually using CTC or Cisco IOS mode. BFD-based fault detection for MPLS-TP tunnels is supported at 50ms granularity using software mechanisms. It is also possible to create unprotected MPLS-TP tunnels. Only MPLS-TP data path circuit is supported over a ring. Protected MPLS-TP tunnels cannot be created in an open-ended ring as there is no alternate path available in such a configuration.

In a dual-homed ring, it is possible to create protected MPLS-TP Tunnels to WRC or PRC across the dual-homed ring and the inter-RC link spans.

VPWS in a Closed-Ended Rings

The VPWS port-based pseudowires can be created through MPLS-TP tunnels that are created within a ring or across rings. You cannot create a pseudowire in a ring if the chassis on which the corresponding attachment circuit exists, is down

VPLS in a Closed-Ended Ring

CPT 50 in a closed-ended ring can participate in the open ring or hub-and-spoke models of VPLS.

Local Switching

CPT supports local switching in a ring. Local switching allows switching of Layer 2 data between two attachment circuits on the same CPT 50 in the ring. In local switching (also known as hairpin connection), frames from one interface are switched to another interface on the same CPT 50 in a ring.

VPWS and VPLS in a Dual-Homed Ring

In a dual-homed ring, CPT 50 can participate in VPWS and VPLS by using either unprotected or protected pseudowires, terminating either at WRC or PRC.

Limitations and Restrictions

These limitations and restrictions apply to the ring in CPT:

- A maximum of 20 open-ended, 10 closed-ended and 20 dual-homed rings can be provisioned with CPT 600 and a maximum of 6 open-ended, 3 closed-ended and 6 dual-homed rings can be provisioned with CPT 200.
- A maximum of 15 CPT 50 panels can be configured in a ring.
- A maximum of 40 CPT 50 panels can be configured across all the rings (single-homed or dual-homed), on a single CPT 600 or CPT 200.
- The Resilient Ethernet Protocol (REP) configurations are internally provisioned on the ring.
- A ring cannot be configured on the XFP port.
- A CPT 600 or CPT 200 chassis can only have one role at a given time. It can be WRC, PRC or Single home.
- The ports that already have Fan-Out-Group (FOG) configured, cannot be used for creating a ring.
- The east port cannot be same as the west port while creating a single-homed ring.
- Services must be configured on the WRC of the dual-homed ring only, in the CTC mode and it should be in up state. It can be configured on the PRC when the WRC is down, but it is not recommended.
- In a dual-homed ring, in case of span failure service provisioning can be done only on the CPT 50's connected through the WRC, up to the first span failure .
- If a CPT 600 or CPT 200 chassis is used in dual-homed ring, it cannot be used in the single-homed ring.
- Both the WRC and the PRC should be in up state to perform any ring related provisioning on the dual-homed ring.
- Layer 1 and Layer 2 configurations should not be done on the dual-homed ring when the WRC is down, through the CTC and IOS mode.
- Ring segment ID and normal REP segment ID must be different.
- Alarm synching is not supported from WRC to PRC and vice versa.
- Do not remove or change the REP parameters on the ring interface as it causes data loss and separation of CPT50 from the ring.
- Normal REP must not be configured on the Interconnect (IC) link port of a dual-homed ring.

NTP-J126 Configure a Ring Using CTC

Purpose	This procedure configures a ring.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Perform any of the following procedures as needed to configure a single-homed ring:

- DLP-J371 Set the Role of a Node Using CTC, on page 54
- DLP-J363 Create a Single-Homed Ring Using CTC, on page 41
- DLP-J365 Manage the Packet Transport System View of a CPT 50 in a Ring, on page 45
- DLP-J366 View Actual Topology of a Ring, on page 53

Stop. You have completed this procedure.

Step 2 Perform the following procedures as needed to configure a dual-homed ring:

- DLP-J370 Add a Node Using CTC, on page 53
- DLP-J371 Set the Role of a Node Using CTC, on page 54
- DLP-J377 Configure a GCC Link , on page 55
- DLP-J372 Create a Dual-Homed Ring Using CTC, on page 56
- DLP-J373 Edit a Dual-Homed Ring Using CTC, on page 57
- DLP-J378 Change the Status of the PRC using CTC , on page 59
- DLP-J376 Configure Management Virtual Forwarding Interface (VFI), on page 60

Stop. You have completed this procedure.

DLP-J363 Create a Single-Homed Ring Using CTC

Purpose	This procedure allows you to do the following: • Create a single-homed ring • Add CPT 50 in the ring • Enable the service
Tools/Equipment	None
Prerequisite Procedures	DLP-J371 Set the Role of a Node Using CTC, on page 54
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to create a single-homed ring.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Rings** tab.

Step 5 Click **Create**. The Ring Creation wizard appears.

Step 6 In the Ring Attributes area, specify the ring attributes as follows:

a) From the Topology Type drop-down list, choose **Linear** or **Ring**.

b) Enter the name of the ring that you want to create in the Ring Name field.

c) In the East Post area, complete the following steps:

- From the Slot drop-down list, choose a slot.
- From the Port drop-down list, choose a port.

d) In the West Port area, complete the following steps:

Note The West Port area is displayed only if you have selected **Ring** from the Topology Type drop-down list to create a closed-ended ring.

- From the Slot drop-down list, choose a slot.
- From the Port drop-down list, choose a port.

e) Click **Save.**

Note REP is enabled on the east and west ports by default. For information about the default parameters of REP, see Understanding REP in a Ring.

f) Click **Next.**

Step 7 To add a CPT 50 in the ring, complete the following steps:

a) Right-click the link and click **Add**. The CPT 50 Attributes dialog box appears.

b) Enter the device identification number and description of CPT 50.

c) Click **Save**.

Note To save the node positions for CPT 50 in a ring, right click the Network view and choose **Open CPT50 Detailed Network View** option.

d) To add multiple CPT 50 panels, repeat the previous steps.

Step 8 From the Service drop-down list, choose **Enable**.

Note You cannot configure services such as MPLS-TP on this ring unless the service is enabled.

Step 9 Return to your originating procedure (NTP).

DLP-J364 Edit a Single-Homed Ring Using CTC

Purpose	This procedure edits a ring using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J363 Create a Single-Homed Ring Using CTC, on page 41
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to edit a ring.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Rings** tab.

Step 5 From the list of rings, select a ring to edit.

Step 6 Click **Edit**. The Ring Preview screen appears.

Step 7 Right click the CPT 50 and perform any of the following:

- Click **Open Card** to view the card details of the CPT 50.
- Click **Open PTS View** to open the Packet Transport System view of the CPT 50. For more information, see DLP-J365 Manage the Packet Transport System View of a CPT 50 in a Ring, on page 45.
- Click **Add After or Add Before** to add CPT 50 before or after already added CPT 50.

  Note **Add Before** button will appear only if the topology type is Ring and a CPT 50 is already added in the ring.
- Click **Edit** to modify the device identification number and description of the CPT 50 through CTC.

  Note After editing through CTC, run the following Cisco IOS commands on the CPT 50 console.

  1. test deviceIdentifier set <new identifier>
  2. test deviceDescription set <new description>
- Click **Delete** to delete the CPT 50.

Note To delete a CPT 50, service state should be disable.

Step 8 From the Service drop-down list, choose **Enable**.

Note If the service state of a ring is disabled and the admin state of the east port of that ring, is set as down, SINGLE-SPAN-FAILURE alarm will get raised.

Note You cannot configure services such as MPLS-TP on this ring unless the service is enabled.

Step 9 Return to your originating procedure (NTP).

DLP-J381 Replace an existing CPT 50 in a ring with another CPT 50

Purpose	This procedure allows you to replace an existing CPT 50 in a ring with another CPT 50.
Tools/Equipment	None
Prerequisite Procedures	NTP-J109 Upgrade the Cisco CPT Software
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Perform the following steps to replace an existing CPT 50 in a ring with another CPT 50.

Note If the CPT-50 is already used in 9.7.0, please follow only steps 6 to 10.

Procedure

Step 1 Physically add a new CPT 50 to the node. The port should not be a ring port

Step 2 Create FOG on the newly added CPT 50 using CTC. After creating FOG, CPT 50 will be in LC-slot with LC image.

Note Make sure that only one IC link should be connected to the CPT 50 and the node.

Step 3 Run the following command to check the golden image version: **show version**

Note If the golden image version is less than 408.0, wait for the CPT 50 to auto reboot with the latest golden image.

Note If the golden image version is less than 408.0, don't delete the FOG already created.

Step 4 Set device identifier of the new CPT50 same as the existing CPT 50 using the following commands: **test deviceidentifier set <name>**

Step 5 Set device description of the new CPT50 same as the existing CPT 50 using the following commands: **test devicedescription set <name>**

Step 6 Run the following command to check whether the device identifier and description fields are set properly: **show version**

Step 7 Run the following command to change the mode from FANOUT to ring: **test satMode ring**

Step 8 Delete the FOG from the CTC. Now the new CPT 50 will reboot with the latest golden image.

Step 9 Physically replace a new CPT 50 in the ring.

Note Perform this step only if the CPT 50 is already used in CPT version 9.7.0.

Step 10 Make east and west port connections. Now new CPT 50 automatically downloads the application image and comes up with all the services configured on the replaced CPT 50.

Step 11 Return to your originating procedure (NTP).

DLP-J365 Manage the Packet Transport System View of a CPT 50 in a Ring

Purpose	This procedure manages the Packet Transport System (PTS) view of a CPT 50 in a ring.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to manage the PTS view of a CPT 50 in a ring.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View** . The Packet Transport System View dialog box appears.

Step 3 Click the **Rings** tab.

Step 4 Choose a ring to edit and click **Edit**. The Ring Preview screen appears.

Step 5 Right-click the CPT 50 and choose **Open PTS View**. The CPT50 PTS View dialog box appears.

Step 6 The CPT50 PTS View dialog box consists following tabs:

- **Provisioning** tab
- **Maintenance** tab
- **Service Level Alarms** tab

The following table lists all the configurations that you can perform in the Provisioning tab.

Note The configuration procedures performed in the PTS view of a CPT 50 in a ring is same as those performed in the PTS view of a card. However, the navigation steps to the PTS views of a CPT 50 in a ring and a card are different. Ignore the first three steps in the following procedures and follow step 1 through step 5 mentioned in this procedure to navigate to the CPT50 PTS View dialog box.

Pane	Configuration Procedure

Port Configuration	• DLP-J224 Configure CDP Using CTC, on page 795 • DLP-J225 Configure CDP Using Cisco IOS Commands, on page 794
Control plane	• DLP-J109 Create and Edit a Loopback Interface Using CTC, on page 172 • DLP-J108 Create a Loopback Interface Using Cisco IOS Commands, on page 171 • DLP-J111 Specify the IP Address for Interfaces That Participate in an MPLS Network Using CTC, on page 174 • DLP-J110 Specify the IP Address for Interfaces That Participate in an MPLS Network Using Cisco IOS Commands, on page 173 • DLP-J118 Enable or Disable MPLS LDP Autoconfiguration Using CTC, on page 193 • DLP-J115 Enable MPLS LDP Autoconfiguration Using Cisco IOS Commands, on page 188 • DLP-J116 Disable MPLS LDP Autoconfiguration Using Cisco IOS Commands, on page 190 • DLP-J113 Enable OSPF on Specific Interfaces Using CTC, on page 177 • DLP-J112 Enable OSPF Protocol on Specific Interfaces Using Cisco IOS Commands, on page 176 • DLP-J209 Configure NSF for OSPF Using CTC, on page 178 • DLP-J221 Configure Cisco NSF for OSPF Using Cisco IOS Commands, on page 179 • DLP-J222 Configure IETF NSF for OSPF Using Cisco IOS Commands, on page 180 • DLP-J122 Enable MPLS LDP-IGP Synchronization Using CTC, on page 201 • NTP-J44 Configure MPLS LDP–IGP Synchronization, on page 195

LDP	• NTP-J46 Configure MPLS LDP Session Protection, on page 205 • DLP-J124 Configure MPLS LDP Backoff Using CTC, on page 203 • DLP-J123 Configure MPLS LDP Backoff Using Cisco IOS Commands, on page 202 • DLP-J127 Enable MPLS LDP Session Protection Using CTC, on page 209 • DLP-J130 Create Targeted LDP Sessions Using CTC, on page 211 • DLP-J131 Configure MPLS LDP Discovery Using CTC, on page 212 • DLP-J133 Enable Explicit Null Label Using CTC, on page 215 • DLP-J135 Configure MPLS LDP Graceful Restart Using CTC, on page 218
MPLS TE	• DLP-J139 Enable OSPF-TE Protocol on Specific Interfaces Using CTC, on page 183 • DLP-J137 Enable MPLS-TE on a System and on Specific Interfaces Using CTC, on page 222 • DLP-J136 Configure MPLS and RSVP to Support Traffic Engineering Using Cisco IOS Commands , on page 220 • DLP-J141 Enable RSVP Graceful Restart on an Interface Using CTC, on page 224 • DLP-J140 Enable RSVP Graceful Restart on an Interface Using Cisco IOS Commands, on page 222 • DLP-J142 Configure MPLS-TE Parameters for Each Interface Using CTC, on page 224 • DLP-J144 Change the Periodic Flooding Timer Using CTC, on page 226 • DLP-J143 Change the Periodic Flooding Timer Using Cisco IOS Commands, on page 225

MPLS TP	• NTP-J36 Configure Global Settings for Multiprotocol Label Switching Transport Profile, on page 287 • DLP-J96 Configure Global Settings for Multiprotocol Label Switching Transport Profile Using CTC, on page 289 • DLP-J98 Create and Configure BFD Templates Using CTC, on page 295 **Note** The following BFD templates are configured automatically for a ring: • fast_profile_BFD • slow_profile_BFD • DLP-J97 Create and Configure BFD Templates Using Cisco IOS Commands, on page 293 • DLP-J100 Configure an MPLS–TP Link Number Using CTC, on page 301 • DLP-J99 Configure an MPLS–TP Link Using Cisco IOS Commands, on page 298 • DLP-J102 Create a Static OAM Class Using CTC, on page 304 • DLP-J101 Create a Static OAM Class Using Cisco IOS Commands, on page 303
Pseudowire Class	• DLP-J89 Create a Pseudowire Class Using CTC, on page 348 • DLP-J88 Create a Pseudowire Class Using Cisco IOS Commands, on page 346
Label Range	• DLP-J104 Specify Static Label Range Using CTC, on page 292 • DLP-J103 Specify Static Label Range Using Cisco IOS Commands, on page 291

QoS	• DLP-J193 Creating or Editing a Policy Map Using CTC, on page 420 • DLP-J194 Setting Policy Class Actions Using CTC, on page 422 • DLP-J191 Creating or Editing a Class Map Using CTC, on page 411 • DLP-J196 Attaching or Removing a Traffic Policy from the Target Using CTC, on page 427 • DLP-J195 Attaching or Removing a Traffic Policy from the Target Using Cisco IOS Commands, on page 424 • DLP-J198 Creating or Editing a Table Map Using CTC, on page 441
CFM	• NTP-J106 Configure CFM Using Cisco IOS Commands, on page 659 • DLP-J299 Enable or Disable CFM on the CPT System Using CTC, on page 662 • DLP-J305 Enable or Disable CFM on the CPT System Using Cisco IOS Commands, on page 661 • DLP-J300 Enable or Disable CFM for Each Port or Channel Group Using CTC, on page 665 • DLP-J313 Enable Caching of CFM Data Using CTC, on page 667 • DLP-J312 Enable Caching of CFM Data Using Cisco IOS Commands, on page 666 • DLP-J301 Create and Modify a Maintenance Domain Profile Using CTC, on page 670 • DLP-J303 Create and Modify a Maintenance Association Profile Using CTC, on page 675 • DLP-J304 Delete a Maintenance Association Profile Using CTC, on page 677

Y1731	• DLP-J350 Clear AIS Alarms Using CTC, on page 707 • DLP-J349 Configure ETH-AIS Parameters Using Cisco IOS Commands, on page 705 • DLP-J352 Lock an MEP or an Interface Using CTC, on page 711 • DLP-J351 Configure ETH-LCK Parameters Using Cisco IOS Commands, on page 708 • DLP-J353 Enable Y.1731 Fault Management Parameters Using CTC, on page 713 • DLP-J355 Configure and Schedule Two-Way Delay Measurement Using CTC, on page 719
Channel Group	• DLP-J15 Create a Channel Group Using CTC, on page 551 • DLP-J12 Configure a Channel Group Without LACP Using Cisco IOS Commands, on page 546 • DLP-J16 Edit a Channel Group Using CTC, on page 552 • DLP-J18 Configure Manual Load Balancing Using CTC, on page 557 • DLP-J17 Configure Manual Load Balancing Using Cisco IOS Commands, on page 555
LACP	• DLP-J9 Set LACP System Priority Using CTC, on page 541 • DLP-J8 Set LACP System Priority Using Cisco IOS Commands, on page 540
REP	• DLP-J29 Configure REP Administrative VLAN Using Cisco IOS Commands, on page 504 • DLP-J34 Create a Segment Using CTC, on page 511 • DLP-J35 Edit a Segment Using CTC, on page 513 • DLP-J30 Configure REP Administrative VLAN Using CTC, on page 505 • DLP-J40 Activate VLAN Load Balancing Using CTC, on page 518 • DLP-J41 Deactivate VLAN Load Balancing Using CTC, on page 519

EFM	• DLP-J314 Enable or Disable Ethernet Link OAM on a Port Using CTC, on page 639 • DLP-J315 Enable or Disable Link Monitoring Support on an Interface Using CTC, on page 643 • DLP-J319 Configure the Port for Remote Link Failure Indication Using CTC, on page 652 • DLP-J318 Enable Remote Loopback on an Interface Using CTC, on page 656 • NTP-J114 Configure EFM Using Cisco IOS Commands, on page 637
Timing	• DLP-J326 Set Up Timing Parameters Using CTC, on page 731 • DLP-J327 Select Timing Reference Using CTC, on page 737DLP-J330 Enable or Disable ESMC Using CTC, on page 733 **Note** For ring port, SynE is enabled by default. • DLP-J329 View Timing Status Report Using CTC, on page 738
Span	• DLP-J357 Configure a Port or EFP Span Using CTC, on page 571 • DLP-J358 Restrict the Destination Ports for a Span Using CTC, on page 573 • NTP-J119 Configure a Span Using Cisco IOS Commands, on page 565

The following table lists all the configurations that you can perform in the Maintenance tab.

Note The configuration procedures performed in the PTS view of a CPT 50 in a ring is same as those performed in the PTS view of a card. However, the navigation steps to the PTS views of a CPT 50 in a ring and a card are different. Ignore the first three steps in the following procedures and follow step 1 through step 5 mentioned in this procedure to navigate to the CPT50 PTS View dialog box.

Pane	Configuration Procedure
IOS	• NTP-J20 Change the CPT System Configuration Mode Using CTC, on page 9 • DLP-J56 Open the Cisco IOS Configuration Mode and View the Feature Configuration Details Using CTC, on page 10

MAC Learning	• DLP-J22 Configure the MAC Address Limit on a Bridge Domain Using CTC, on page 582 • DLP-J21 Configure MAC Address Limit on a Bridge Domain Using Cisco IOS Commands, on page 581 • DLP-J20 Re-enable or Disable MAC Learning on a Bridge Domain Using CTC, on page 580 • DLP-J19 Re–enable or Disable MAC Learning on a Bridge Domain Using Cisco IOS Commands, on page 578 • DLP-J28 Display Information About the MAC Address Table Using CTC, on page 593 • DLP-J27 Display Information About the MAC Address Table Using Cisco IOS Commands, on page 591 • DLP-J24 Configure a Static MAC Address on a Service Instance Using CTC, on page 586 • DLP-J23 Configure a Static MAC Address on a Service Instance Using Cisco IOS Commands, on page 584 • DLP-J26 Remove a MAC Address Using CTC, on page 589 • DLP-J23 Configure a Static MAC Address on a Service Instance Using Cisco IOS Commands, on page 584 • DLP-J25 Remove a MAC Address Using Cisco IOS Commands, on page 588 • DLP-J1 Configure an Ethernet Service Instance Using Cisco IOS Commands, on page 141 • NTP-J108 Configure a VPLS Circuit Using Cisco IOS Commands, on page 398
OAM	NTP-J107 Perform ping and traceroute Operations on Services Using CTC, on page 322

The following table lists all the configurations that you can perform in the Service Level Alarms tab.

Note The configuration procedures performed in the PTS view of a CPT 50 in a ring is same as those performed in the PTS view of a card. However, the navigation steps to the PTS views of a CPT 50 in a ring and a card are different. Ignore the first three steps in the following procedures and follow step 1 through step 5 mentioned in this procedure to navigate to the CPT50 PTS View dialog box.

Configuration Procedure
NTP-J73 Display Alarms that Affect Services Using CTC, on page 843
NTP-J74 Display Alarms on Service Using CTC, on page 844

Step 7 Return to your originating procedure (NTP).

DLP-J366 View Actual Topology of a Ring

Purpose	This procedure provides a graphical representation of the actual ring topology in the field.
Tools/Equipment	None
Prerequisite Procedures	DLP-J363 Create a Single-Homed Ring Using CTC, on page 41
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to view the actual topology of a ring.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**.
The Packet Transport System View dialog box appears.

Step 4 Click the **Rings** tab.

Step 5 Select a ring and click **Show Actual Topology**.
The Actual Topology dialog box appears containing the graphical representation of the actual ring topology in the field. The actual ring topology contains the physically connected CPT 50s. If there is a mismatch in the actual ring topology from the provisioned ring topology, corresponding alarms are generated.

Note The Show Actual Topology button is enabled only when the service state is enabled for a ring.

When PTS-FAIL alarm is present on a node, Show Actual Topology will not display correct information.

Step 6 Return to your originating procedure (NTP).

DLP-J370 Add a Node Using CTC

Purpose	This procedure allows you to add a node.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to create a dual-homed ring.

Step 2 From the File menu, choose **Add Node** to add a new node in the network.

Step 3 In the Add Node dialog box, enter the node name and click **Ok**.

Step 4 Return to your originating procedure (NTP).

DLP-J371 Set the Role of a Node Using CTC

Purpose	This procedure sets the role of a node using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to create a ring.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Node Role** tab.

Step 5 In the Node Role Configuration pane, specify the dual-homed ring attributes as follows:

a) From the Ring Mode drop-down list, choose Single Home or Dual Home.

Note To create a dual homed ring, two nodes are required with the node role as Dual Home.

b) From the Node Role drop-down list, choose WRC or PRC.

c) Enter the IP address of the peer node in the Peer Node IP field.

Note To create a single-homed ring, Peer Node IP field is disabled.

The Status field displays status of the node. The default status for WRC and single-homed ring is Active and for PRC is Stand by.

d) Enter the slot number to create interconnect (IC) link in the IC Slot field.

e) Enter the IP address to create interconnect (IC) link in the IC port field.

Note The IC Slot and IC port fields are disabled when creating a single-homed ring.

Note Only one IC link can be created between WRC and PRC.

Note On IC link following configurations are not allowed :

- REP
- Port Based Services
- Services with encapsulation as VLAN 4088
- Facility/Terminal Loopback
- Port Channel
- Destination Span

Step 6 Click **Apply**.

Step 7 Return to your originating procedure (NTP).

DLP-J377 Configure a GCC Link

Purpose	This procedure allows you to configure a generic communication channel (GCC) link.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to configure a GCC link.

Step 2 In the node view (single-shelf mode), click the **Provisioning > Comm Channels > GCC** tabs.

Step 3 Click **Create**. The Create GCC Terminations screen appears.

Step 4 Choose the port and slot to set the GCC termination point.

Step 5 From the GCC Rate drop-down list, choose the GCC rate.

Note For a dual-homed ring, configure the GCC ink on both the nodes and make a physical connection between the PTF cards of both the nodes.

Step 6 Click **Finish**.

Note Verify the GCC link in CTC.

Step 7 Return to your originating procedure (NTP).

Note Enable the admin state of the port.DLP-J78 Change the Port and Ethernet Settings Using CTC, on page 774.

DLP-J372 Create a Dual-Homed Ring Using CTC

Purpose	This procedure allows you to create a dual-homed ring.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to create a dual-homed ring.

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

Step 3 Click the **Dual Home** tab.

Step 4 Click **Create**. The Dual Home Ring Creation wizard appears.

Step 5 In the Dual Home Attributes area, specify the dual-homed ring attributes as follows:

a) Enter the name of the ring that you want to create in the Ring Name field.

b) From the Topology Type drop-down list, choose **Dual Home**.

c) Click **Next.**

Step 6 In the Dual Home Origination screen of the wizard

- From the Node drop-down list, choose a WRC node.
- From the Slot drop-down list, choose a slot.
- From the Port drop-down list, choose a port.
- Click **Next.**

Step 7 In the Dual Home Termination screen of the wizard

- From the Node drop-down list, choose a PRC node.
- From the Slot drop-down list, choose a slot.
- From the Port drop-down list, choose a port.
- Click **Finish.**

Step 8 Click **Display Dual-Homed Ring** to view the ring and the connected CPT 50s in it.

Note You can configure different services on the dual-homed ring through CTC or Cisco IOS mode.

Always run the write memory command after configuring services on the WRC, to synchronize the changes done on the WRC with the PRC.

Step 9 Return to your originating procedure (NTP).

DLP-J373 Edit a Dual-Homed Ring Using CTC

Purpose	This procedure edits a dual-homed ring and add CPT 50's in the dual-homed ring using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J372 Create a Dual-Homed Ring Using CTC, on page 56
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to edit a dual-homed ring.

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

Step 3 Click the **Dual Home** tab.

Step 4 From the list of rings, select a ring to edit.

Step 5 Click **Edit**. The Dual Home Ring Preview screen appears.

Step 6 In the Rings Attributes area, specify the ring attributes as follows:

a) Modify the name of the ring in the **Ring Name** field.

b) From the Service Creation drop-down list, choose **Enable** or **Disable**.

Note If the service state of a ring is disabled and the admin state of a port at the WRC of that ring is set as down, no ring related alarm will get raised.

Note If the service is being configured through Cisco IOS mode then the option selected in this drop-down has no impact on the services configured for dual-homed ring.

Step 7 To delete a Dual Home Ring :

a) In the Service creation drop-down list, Choose **Disable** and click **Finish** button .

b) Click **Edit**. Right click the attached CPT 50s and choose **Delete** to delete each CPT 50 in a ring.

c) Open the **Network View** and click the **Dual home** tab.

d) Select the ring you want to delete. Click **Delete**.

Step 8 To add a CPT 50 in the ring, complete the following steps:

a) Right-click the ring and click **Add**. The CPT 50 Attribute dialog box appears.

b) Enter the device identification number and description of the CPT 50.

c) Click **Save**.

d) To add multiple CPT 50 panels, repeat the step 7 a) through step 7 c).

Note The CPT 50 will be get added between the source and the destination of the link, on which you have right clicked.

Step 9 Click **Finish**.

Step 10 Return to your originating procedure (NTP).

Note The CPT 50s must be provisioned using CTC in the same manner as they are physically connected. For example, ensure that the ports and equipment identifiers are same in the physical and provisioned configurations.

DLP-J381 Replace an existing CPT 50 in a ring with another CPT 50

Purpose	This procedure allows you to replace an existing CPT 50 in a ring with another CPT 50.
Tools/Equipment	None
Prerequisite Procedures	NTP-J109 Upgrade the Cisco CPT Software
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Perform the following steps to replace an existing CPT 50 in a ring with another CPT 50.

Note If the CPT-50 is already used in 9.7.0, please follow only steps 6 to 10.

Procedure

Step 1 Physically add a new CPT 50 to the node. The port should not be a ring port

Step 2 Create FOG on the newly added CPT 50 using CTC. After creating FOG, CPT 50 will be in LC-slot with LC image.

Note Make sure that only one IC link should be connected to the CPT 50 and the node.

Step 3 Run the following command to check the golden image version: **show version**

Note If the golden image version is less than 408.0, wait for the CPT 50 to auto reboot with the latest golden image.

Note If the golden image version is less than 408.0, don't delete the FOG already created.

Step 4 Set device identifier of the new CPT50 same as the existing CPT 50 using the following commands: **test deviceidentifier set <name>**

Step 5 Set device description of the new CPT50 same as the existing CPT 50 using the following commands: **test devicedescription set <name>**

Step 6 Run the following command to check whether the device identifier and description fields are set properly: **show version**

Step 7 Run the following command to change the mode from FANOUT to ring: **test satMode ring**

Step 8 Delete the FOG from the CTC. Now the new CPT 50 will reboot with the latest golden image.

Step 9 Physically replace a new CPT 50 in the ring.

Note Perform this step only if the CPT 50 is already used in CPT version 9.7.0.

Step 10 Make east and west port connections. Now new CPT 50 automatically downloads the application image and comes up with all the services configured on the replaced CPT 50.

Step 11 Return to your originating procedure (NTP).

DLP-J378 Change the Status of the PRC using CTC

Purpose	This procedure changes the status of the PRC using CTC.
Tools/Equipment	None
Prerequisite Procedures	None

Required/As Needed	As needed when the WRC is down.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to create a ring.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Node Role** tab.

Step 5 In the Node Role Configuration pane, choose PRC in the Node Role drop-down list.

Step 6 Click **GO ACTIVE** to make the status of the PRC as active.

Note The status of a node can be changed to active, if PROTNA alarm is not raised on that node.

Step 7 Click **Apply**.

Note Change the status of the PRC only when the WRC is down.

Step 8 Return to your originating procedure (NTP).

DLP-J376 Configure Management Virtual Forwarding Interface (VFI)

Purpose	This procedure allows you to configure Management Virtual Forwarding Interface (VFI).
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Create protected tunnels between both CPT 200 or CPT 600 and CPT 50s with pseudowire class as VPLS.NTP-J41 Configure an MPLS-TP Tunnel, on page 309

Step 2 Create Pseudowire Class. NTP-J30 Create a Pseudowire Class, on page 346

Step 3 Configure Mesh VPLS between WRC and PRC. NTP-J107 Configure a VPLS Circuit Using CTC, on page 391

Step 4 Configure Loopback. DLP-J109 Create and Edit a Loopback Interface Using CTC, on page 172

Step 5 Configure OSPF. NTP-J65 Configure OSPF and OSPF–TE, on page 175

Step 6 Configure H-VPLS from one of the 1GE ports of each CPT 50 to WRC as working and to PRC as standby hub node. NTP-J107 Configure a VPLS Circuit Using CTC, on page 391

Step 7 Assign IP address with similar network mask to another 1GE port.

Step 8 Return to your originating procedure (NTP).

DLP-J380 Change CPT 50 in Ring Mode to Fan-Out-Group (FOG) Mode

Purpose	This procedure changes a CPT 50 in RIng mode to FOG mode
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

This procedure allows you to upgrade CPT 50's in ring mode to FOG mode.

Note The CPT 600 or 200 must have CPT 9.7.0 or later version.

Procedure

Step 1 Create a new ring on the CPT 600 or CPT 200.

Step 2 Add the CPT 50s to the linear ring through CTC before physically connecting the CPT 50's in the ring.

Step 3 Connect the port 45 of the CPT 50s to the east port of the newly created ring on the CPT 600 or CPT 200 and the west port to port 46 in case of closed single-homed or dual-homed ring.

Note In case of existing ring where services are already configured over the CPT 50's, follow the below three steps before proceeding to Step 4:

1. Delete the VPWS, VPLS or EVC services configured on the CPT 50's
2. Now delete the MPLS-TP tunnels configured through the CPT 50's.
3. Disable the service state.

Step 4 Telnet the CPT 50s through CTC. **telnet <node ip> <2000 + ID of the CPT 50 in a ring>**.

Step 5 Run the following command: **test satMode fanout**

Step 6 Delete the ring and CPT 50s added to that ring using CTC.

Step 7 Create the fan-out-group (FOG) using CTC.

Step 8 Physically connect the CPT 50s in FANOUT mode.

Step 9 Hard reset the CPT 50s.

Step 10 Return to your originating procedure (NTP).

DLP-J374 Upgrade CPT 50 in Fan-Out-Group (FOG) Mode to Ring Mode

Purpose	This procedure allows you to upgrade CPT 50's in FOG mode to ring mode
Tools/Equipment	None
Prerequisite Procedures	NTP-J109 Upgrade the Cisco CPT Software
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Perform the following steps to upgrade CPT 50 in FOG mode to ring mode.

Procedure

Step 1 Physically connect a new CPT 50 to the node and create FOG on the newly added CPT 50 using CTC.

Note To open the CPT 50 console, execute the following steps:

- Connect the debug console cable to that CPT 50 and wait for the CPT 50 to be in the **router>** or **Satellite>** or **LC:LC-<slot-id>** mode.
- If the CPT 50 is in FOG mode and UP, open the active PTF card console via telnet and execute the command : **test platform telnet 192.168.191.<FOG-ID>**
- Enter the password if required.

Note Make sure that only one IC link should be connected to the CPT 50 and the node.

Step 2 Run the following command on the IOS command prompt to check the golden image version: **show version**

Note The golden version can be located in the show version output against GOLDEN VERSION field.

Note If the golden image version is less than 408.0, wait for the CPT 50 to auto reboot and to come up with the latest golden image.

Note If the golden image version is less than 408.0, don't delete the FOG already created.

Step 3 Set device identifier of the new CPT50 as per the identification need or same as the existing CPT 50 if this is the replacement of existing CPT 50 by executing the following commands on the IOS command prompt: **test deviceidentifier set <name>**

Step 4 Set device description of the new CPT50 as per the identification need or same as the existing CPT 50 f this is the replacement of existing CPT 50 by executing the following commands on the IOS command prompt: **test devicedescription set <name>**

Step 5 Run the following command: **test satMode ring**

Step 6 (Optional) Run the following command: **reload**

Step 7 Launch CTC and delete the fan-out port.

Step 8 Now create a ring.

Step 9 Run the following command: **reload**

Step 10 Return to your originating procedure (NTP).

Preparing to Install the CPT 50 Shelf

This chapter explains how to prepare for the CPT 50 shelf installation.

Important Safety Recommendations

Warning 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. To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document for the appropriate Cisco chassis. Statement 274

Warning Installation of the equipment must comply with local and national electrical codes. Statement 1074

Warning This equipment must be installed and maintained by service personnel as defined by AS/NZS 3260. Incorrectly connecting this equipment to a general-purpose outlet could be hazardous. The telecommunications lines must be disconnected 1) before unplugging the main power connector or 2) while the housing is open, or both. Statement 1043

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

Warning Ultimate disposal of this product should be handled according to all national laws and regulations. Statement 1040

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

Note In this chapter, "shelf" refers to the steel enclosure that holds cards and connects power, and "node" refers to the entire hardware and software system.

Note Unless otherwise specified, CPT 50 shelf refers to both ANSI and ETSI environments.

Note The CPT 50 shelf is suitable for installation in network telecommunication facilities where the National Electric Code (NEC) applies.

Required Tools and Equipment

The following sections describe the tools and equipment you need to install and test the CPT 50 shelf.

Cisco Supplied Materials

The following materials are required and are shipped with the CPT 50 shelf (wrapped in plastic). The number in parentheses gives the quantity of the item included in the package.

- (Only ANSI) Pair of 19-inch mounting brackets (2)
- (Only ANSI) Pair of 23-inch mounting brackets (2)
- (Only ETSI) Pair of 21-inch mounting brackets (2)
- Cable guides (2)
- Rubber bumpers (4)
- M4 screws to fix brackets (8)
- M4 screws to fix ground lug (2)
- Ground lug (1)
- Power cable (1). A DC power cable is present in the kit if the customers have ordered for it.

Attention Always use M4 screws to install a ground lug on a CPT 50 shelf. The Cisco part number for this screw is 48-0468-01. The recommended maximum length is 6 millimeters (mm). If you use a screw longer than 6 mm, it can lead to a short circuit in the CPT 50 shelf.

Note If the customers have ordered a CPT-50-44GE-48E= or CPT-50-48E-LIC= shelf, a DC power cable is present in the accessory kit. If the customers have ordered a CPT-50-44GE-AC= or CPT-50-AC-LIC shelf, an AC power cable is present in the accessory kit.

Caution Use only the power cables that are designed to be used with the CPT 50 shelf. These are sold separately.

User Supplied Materials

The following materials, tools, and equipment are required but are not supplied with the CPT 50 shelf.

- Equipment rack
- M4 Phillips screw driver
- Fuse panel
- Wire cutters
- Wire wrapper
- Voltmeter
- Ground cable #8 AWG stranded, specified for up to 90° Celsius (194° Fahrenheit)
- M3 Phillips screw driver only for CPT-50-44GE-48E= and CPT-50-48E-LIC= shelves to secure the DC power cable to the shelf.

Caution Use only the power cables that are designed to be used with the CPT 50 shelf. These are sold separately.

NTP-J53 Unpack and Inspect the CPT 50 Shelf

Purpose	This procedure explains how to unpack the CPT 50 shelf and verify its contents.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite

Security Level	None

Procedure

Step 1 Complete the DLP-J171 Unpack and Verify the CPT 50 Shelf, on page 66.

Step 2 Complete the DLP-J172 Inspect the CPT 50 Shelf, on page 66.
Stop. You have completed this procedure.

DLP-J171 Unpack and Verify the CPT 50 Shelf

Purpose	This task describes how to remove the shelf from the package and verify the items.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Procedure

Step 1 When you receive the CPT 50 shelf equipment at the installation site, open the top of the box. The Cisco Systems logo indicates the top of the box.

Step 2 Remove the foam inserts from the box. The box contains the CPT 50 shelf (wrapped in plastic) and other items needed for installation.

Step 3 To remove the shelf, grasp both rings of the shelf removal strap and slowly lift the shelf out of the box.

Step 4 Verify that you have all items listed in the Required Tools and Equipment, on page 64.

Step 5 Return to your originating procedure (NTP).

DLP-J172 Inspect the CPT 50 Shelf

Purpose	This task explains how to verify that all parts of the shelf assembly are in good condition.
Tools/Equipment	None

Prerequisite Procedures	DLP-J171 Unpack and Verify the CPT 50 Shelf, on page 66
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Procedure

Step 1 Verify the following:

- The CPT 50 shelf is not damaged.
- The cable connectors, EOBC, timing connectors, and power connectors on the front panel of CPT 50 shelf are not damaged.
- The SFP cages on the front panel of the CPT 50 shelf are not damaged.

Step 2 If there is any damage, call your Cisco sales engineer for a replacement.

Step 3 Return to your originating procedure (NTP).

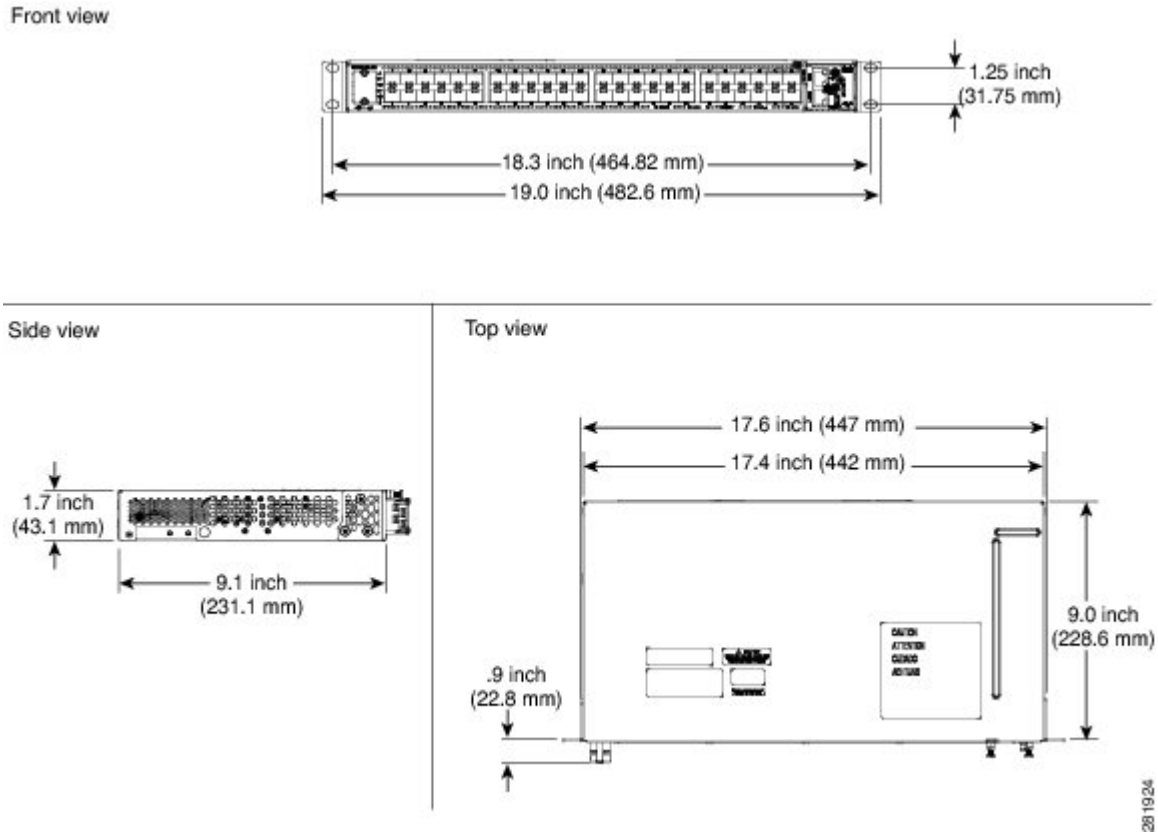
ANSI Rack Installation

The CPT 50 shelf is mounted on a 19-inch (482.6-mm) or 23-inch (584.2-mm) equipment rack. If the shelf is mounted in the front position, then it projects 0.9 inches (22.86 mm) from the front of the rack. If the shelf assembly is mounted in the middle position, then it projects 4.3 inches (109.22 mm) from the front of the rack. The shelf mounts in both Electronic Industries Alliance (EIA) standard and Telcordia-standard racks. The shelf assembly is a total of 17.4 inches (442.4 mm) wide with no mounting ears attached. Ring runs are not provided by Cisco and might hinder side-by-side installation of shelves where space is limited.

The CPT 50 shelf measures 1.7 inches (43.1 mm) high, 19 or 23 inches (482.6 or 584.2 mm) wide (depending on which way the mounting ears are attached), and 9.1 inches (231.1 mm) deep.

The following figure shows the dimensions of the CPT 50 shelf in a 19-inch ANSI rack configuration with brackets mounted in the front position.

Figure 12: CPT 50 Shelf Dimensions for a 19-inch ANSI Rack Configuration



Mounting Brackets

Caution Use only the fastening hardware provided with the CPT 50 shelf to prevent loosening, deterioration, and electromechanical corrosion of the hardware and joined material.

Caution When mounting the CPT 50 shelf in a frame with a nonconductive coating (such as paint, lacquer, or enamel) either use the thread-forming screws provided with the CPT 50 shelf shipping kit, or remove the coating from the threads to ensure electrical continuity.

The mounting brackets (19-inch or 23-inch) are used to mount the shelf on a 19-inch (482.6 mm) rack or a 23-inch (584.2 mm) rack.

Mounting a Single Node

Mounting the CPT 50 shelf on a rack requires a minimum of 1.75 inches (44.44 mm) of vertical rack space. To ensure the mounting is secure, use two #12-24 mounting screws for each side of the shelf assembly. For an ANSI rack, the brackets can be mounted in the front or middle position.

ETSI Rack Installation

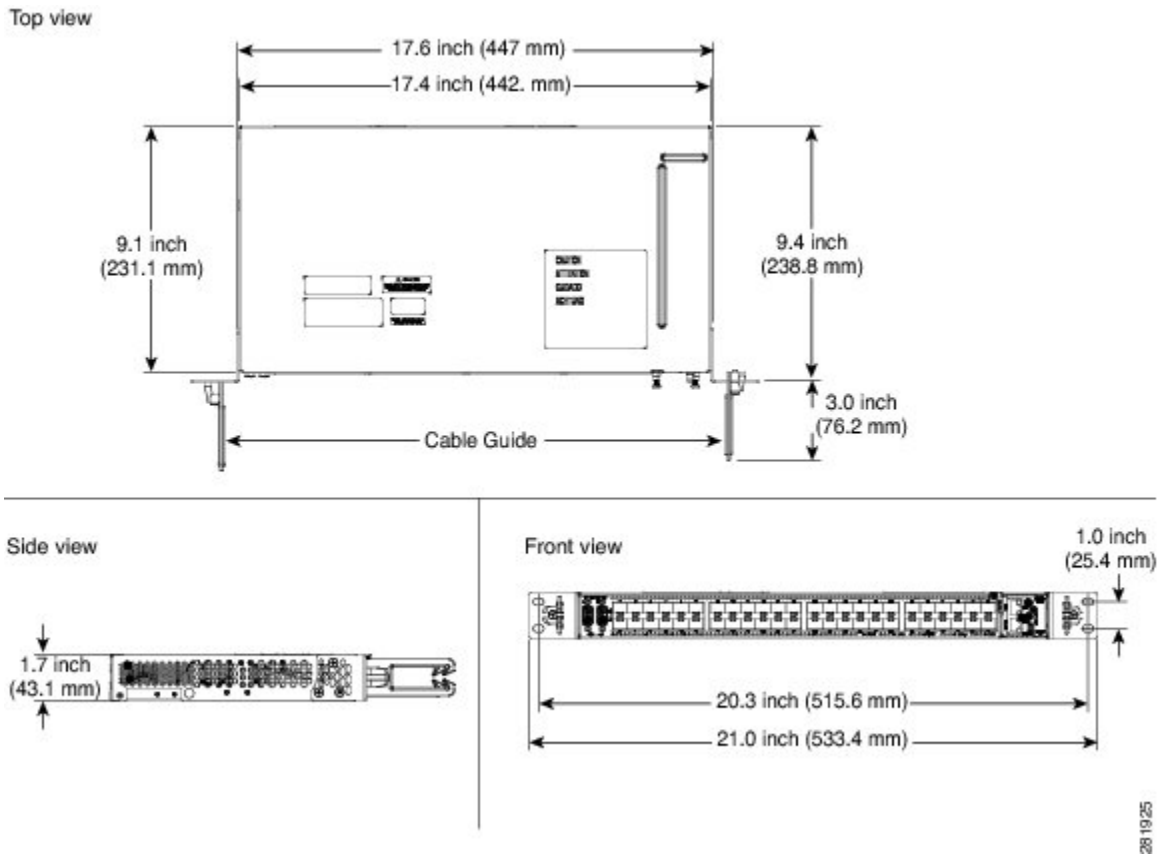
The CPT 50 shelf is mounted on a 600 x 600-mm (23.6 x 23.6-inch) or 600 x 300-mm (23.6 x 11.8-inch) ETSI standard equipment rack. The shelf assembly is a total of 442 mm (17.4 inches) wide with no mounting ears attached. Cisco does not provide ring runs, which might hinder side-by-side installation of shelves where space is limited.

The CPT 50 shelf measures 43.1 mm (1.7 inches) high, 533.4 mm (21 inches) wide, and 231.1 mm (9.1 inches) deep.

Figure 13: CPT 50 Shelf Dimensions for an ETSI Rack Configuration, on page 69 provides the dimensions of the CPT 50 shelf installed on a 600 x 600-mm (23.6 x 23.6-inch) ETSI standard equipment rack. In this figure, the cable guides are attached to the mounting brackets.

Caution When mounting a shelf in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack. If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Figure 13: CPT 50 Shelf Dimensions for an ETSI Rack Configuration



Mounting a Single Node

The CPT 50 shelf requires 1.75 inches (44.44 mm) minimum of vertical rack space. To ensure the mounting is secure, use two M6 mounting screws for each side of the shelf assembly. In an ETSI rack, the brackets can be mounted only in the front position.

Wall Mounting and Desktop Mounting the CPT 50 Shelf

This section provides information about mounting the CPT 50 shelf on the wall and the desktop.

Wall Mounting

The CPT 50 shelf can be mounted on the wall using the wall mount brackets. The type of screws used to mount the brackets on the wall depends on the wall-type; wall mount brackets are not provided by Cisco.

After the CPT 50 shelf is mounted on the wall, a fire protective tray is installed on the wall mount bracket to support the shelf assembly.

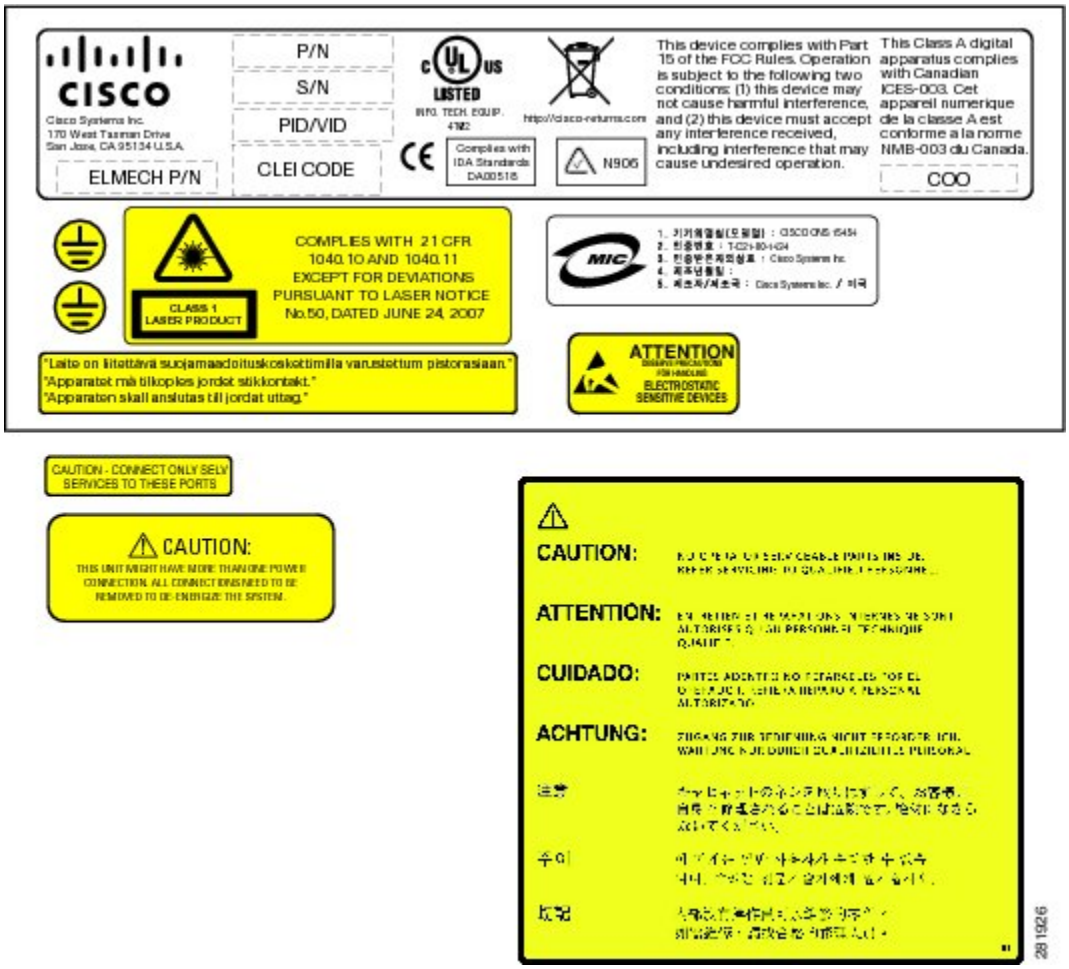
Desktop Mounting

The CPT 50 shelf can be mounted on the desktop for easy access.

Laser Warning

The laser warning label is placed on top of the chassis. The following figure shows the label placed on the CPT 50 shelf.

Figure 14: CPT 50 Shelf Label



NTP-J54 Install the CPT 50 Shelf

Purpose	This procedure describes how to install the shelf.

Tools/Equipment	• #2 Phillips Dynamometric screwdriver • Medium slot-head screwdriver • Small slot-head screwdriver • Screws
Prerequisite Procedures	NTP-J53 Unpack and Inspect the CPT 50 Shelf, on page 65
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note In a CO (Central Office) or CPE (Customer Premises Equipment) installation, if the CPT 600 and CPT 50 units are connected through copper SFP+, place the units less than 6 meters apart in the same lineup.

Warning The intra-building ports of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring. Statement 7005

Warning Stability hazard. The rack stabilizing mechanism must be in place, or the rack must be bolted to the floor before you slide the unit out for servicing. Failure to stabilize the rack can cause the rack to tip over. Statement 1048

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

Warning This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 10A for CPT 50 shelf with 48 VDC power supply; 15A for CPT 50 shelf with 24 VDC power supply. Statement 1005

Warning This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 10A-15A, 100-240VAC~. Statement 1005

Warning To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 131°F (55°C) for CPT 50 shelf with AC power module and 149°F (65°C) for CPT 50 shelf with DC power module. Statement 1047

Warning Take care when connecting units to the supply circuit so that wiring is not overloaded. Statement 1018

Warning To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack. Statement 1006

Warning To prevent airflow restriction, allow clearance around the ventilation openings to be at least: 1 inch (25.4 mm). Statement 1076

Warning To pass Electrical Fast Transient/Burst (EFT/B) for GR-1089, the Westek UL C(UL) E171740 Type CM 24AWG 75degC EIA/TIA 568-B.2 STP CAT5e dual bantam to RJ45 shielded cable or an equivalent must be used with the DS1 pluggable 30-1462-01. The cable must have a grounded wire that is connected to the RJ45 shell as well as a shield of an aluminum foil.

Note The CPT 50 installations are suitable for Network Telecommunication facilities and locations where NEC applies.

Procedure

Step 1 Complete the necessary task as applicable:

- DLP-J173 Mounting the 19-inch Brackets on the CPT 50 Shelf for the ANSI Rack Configuration, on page 74
- DLP-J174 Mounting the 23-inch Brackets on the CPT 50 Shelf for the ANSI Rack Configuration, on page 75
- DLP-J175 Mounting the Brackets on the CPT 50 Shelf for the ETSI Rack Configuration, on page 77

Step 2 Complete the necessary mounting task as applicable:

- DLP-J176 Mount the CPT 50 Shelf on a Rack (One Person), on page 79
- DLP-J178 Mount the CPT 50 Shelf on the Desktop, on page 84
- DLP-J177 Mount the CPT 50 Shelf on the Wall, on page 81

Step 3 Connect the chassis to the office ground. For detailed instructions on how to ground the chassis, see the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.
Stop. You have completed this procedure.

DLP-J173 Mounting the 19-inch Brackets on the CPT 50 Shelf for the ANSI Rack Configuration

Purpose	This task describes how to install the 19-inch mounting brackets on the CPT 50 shelf for the ANSI rack configuration.
Tools/Equipment	• #2 Phillips Dynamometric screwdriver • Medium slot-head screwdriver • Small slot-head screwdriver
Prerequisite Procedures	NTP-J53 Unpack and Inspect the CPT 50 Shelf, on page 65
Required/As Needed	As Needed
Onsite/Remote	Onsite
Security Level	None

Caution Use only the fastening hardware provided with the CPT 50 shelf to prevent loosening, deterioration, and electromechanical corrosion of the hardware and joined material.

Caution When mounting the CPT 50 shelf in a frame with a nonconductive coating (such as paint, lacquer, or enamel) either use the thread-forming screws provided with the CPT 50 ship kit, or remove the coating from the threads to ensure electrical continuity.

Note The mounting brackets can be installed in the front or the middle position of the chassis.

Procedure

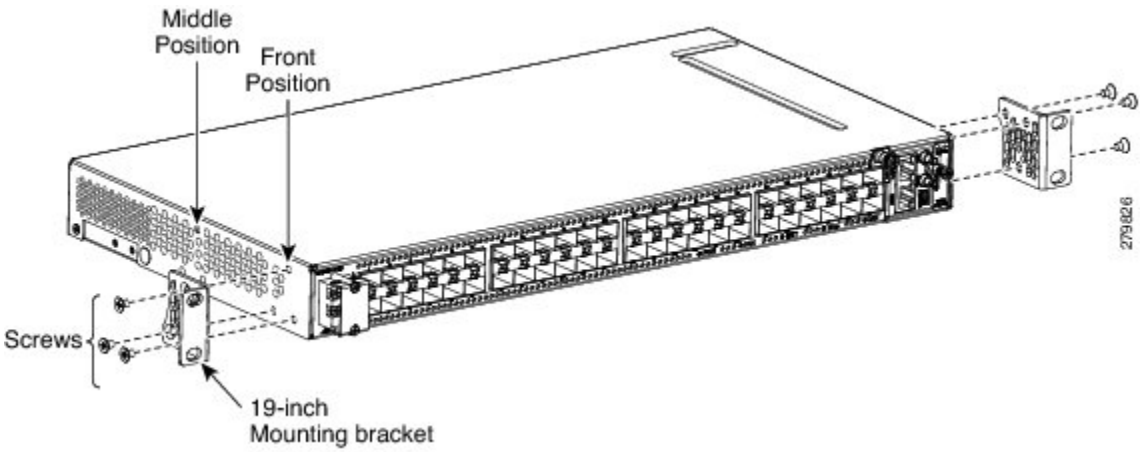
Step 1 Place the wider side of the 19-inch mounting bracket flush against the CPT 50 shelf, as shown in Figure 15: Mounting the Brackets on the CPT 50 Shelf for ANSI Rack Configuration, on page 75. The narrow side of the mounting bracket should be towards the front of the shelf.

Step 2 Align the mounting bracket screw holes against the shelf assembly screw holes.

Step 3 Insert the M4 flat screws and tighten them to a torque value of 11.5 in-lbs (1.3 N-m).

Step 4 Repeat Step 1 to Step 3 to mount the bracket on the opposite side.

Figure 15: Mounting the Brackets on the CPT 50 Shelf for ANSI Rack Configuration



Step 5 Return to your originating procedure (NTP).

DLP-J174 Mounting the 23-inch Brackets on the CPT 50 Shelf for the ANSI Rack Configuration

Purpose	This task describes how to install the 23-inch mounting brackets on the CPT 50 shelf for the ANSI rack configuration.
Tools/Equipment	• #2 Phillips Dynamometric screwdriver • Medium slot-head screwdriver • Small slot-head screwdriver
Prerequisite Procedures	NTP-J53 Unpack and Inspect the CPT 50 Shelf, on page 65

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

Caution Use only the fastening hardware provided with the CPT 50 shelf to prevent loosening, deterioration, and electromechanical corrosion of the hardware and joined material.

Caution When mounting the CPT 50 shelf in a frame with a nonconductive coating (such as paint, lacquer, or enamel) either use the thread-forming screws provided with the CPT 50 ship kit, or remove the coating from the threads to ensure electrical continuity.

Note The mounting brackets can be installed in the front or the middle position of the chassis.

Procedure

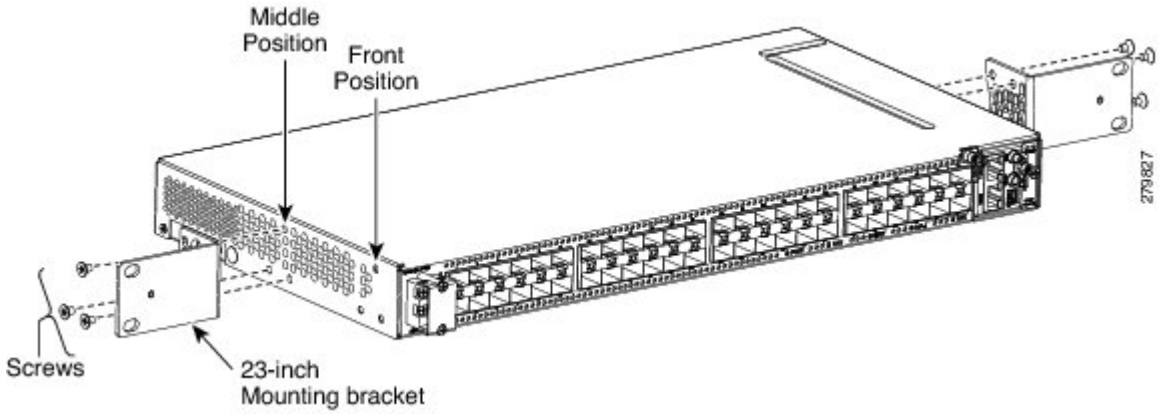
Step 1 Place the narrow side of the 23-inch mounting bracket flush against the CPT 50 shelf, as shown in Figure 16: Mounting the Brackets on the CPT 50 shelf for a 23-inch (584.2-mm) ANSI Configuration, on page 76. The wider side of the mounting bracket should be towards the front of the shelf.

Step 2 Align the mounting bracket screw holes against the shelf assembly screw holes.

Step 3 Insert the M4 flat screws and tighten them to a torque value of 11.5 in-lbs (1.3 N-m).

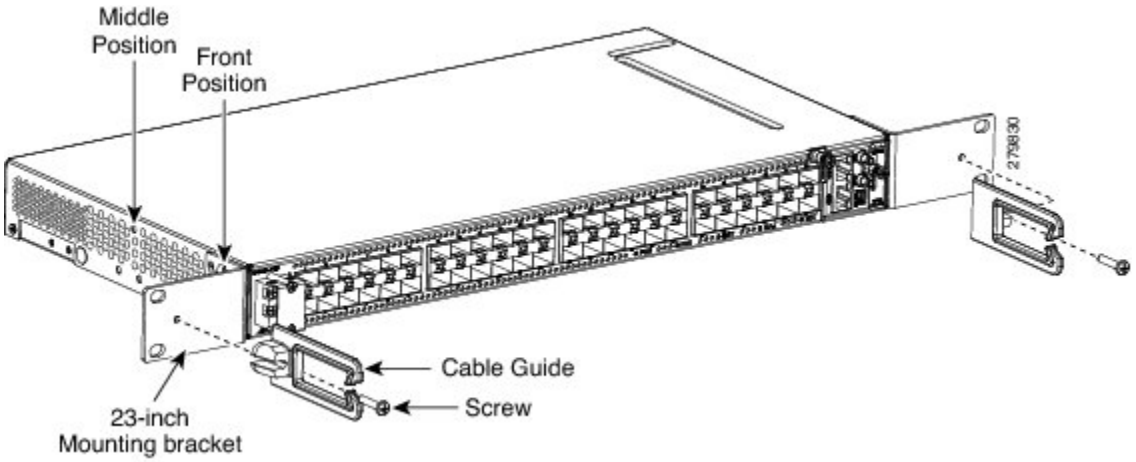
Step 4 Repeat Step 1 to Step 3 to mount the bracket on the opposite side.

Figure 16: Mounting the Brackets on the CPT 50 shelf for a 23-inch (584.2-mm) ANSI Configuration



Step 5 Align the cable guide screw hole against the mount bracket screw hole, as shown in this figure.

Figure 17: Mounting the Cable Guide on the Bracket



Step 6 Insert the M4 screw and tighten it to a torque value of 6.5 in-lbs (0.75 N-m) .

Note The cable guide is made of plastic. Therefore a lower torque value should be applied to tighten the cable guide screws to avoid breakage.

Step 7 Repeat Step 5 and Step 6 to install the cable guide on the opposite side.

Step 8 Return to your originating procedure (NTP).

DLP-J175 Mounting the Brackets on the CPT 50 Shelf for the ETSI Rack Configuration

Purpose	This task describes how to install the mounting brackets on the CPT 50 shelf for the ETSI rack configuration.
Tools/Equipment	• #2 Phillips Dynamometric screwdriver • Medium slot-head screwdriver • Small slot-head screwdriver
Prerequisite Procedures	NTP-J53 Unpack and Inspect the CPT 50 Shelf, on page 65
Required/As Needed	As Needed
Onsite/Remote	Onsite
Security Level	None

Caution Use only the fastening hardware provided with the CPT 50 shelf to prevent loosening, deterioration, and electromechanical corrosion of the hardware and joined material.

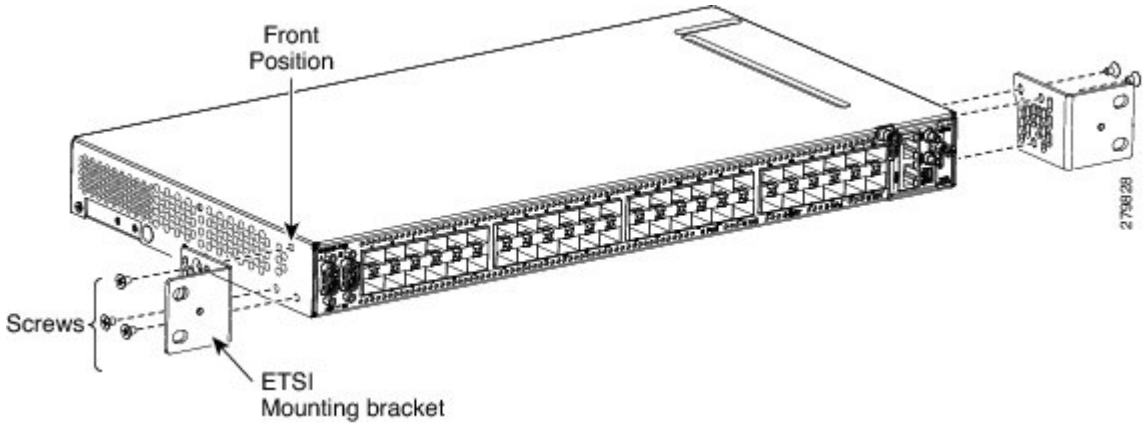
Caution When mounting the CPT 50 shelf in a frame with a nonconductive coating (such as paint, lacquer, or enamel) either use the thread-forming screws provided with the CPT-50 ship kit, or remove the coating from the threads to ensure electrical continuity.

Note The mounting brackets can be installed in the front or the middle position of the chassis.

Procedure

Step 1 Place the mounting bracket flush against the CPT 50 shelf, as shown in this figure.

Figure 18: Mounting the Brackets on the CPT 50 Shelf for the ETSI Rack Configuration



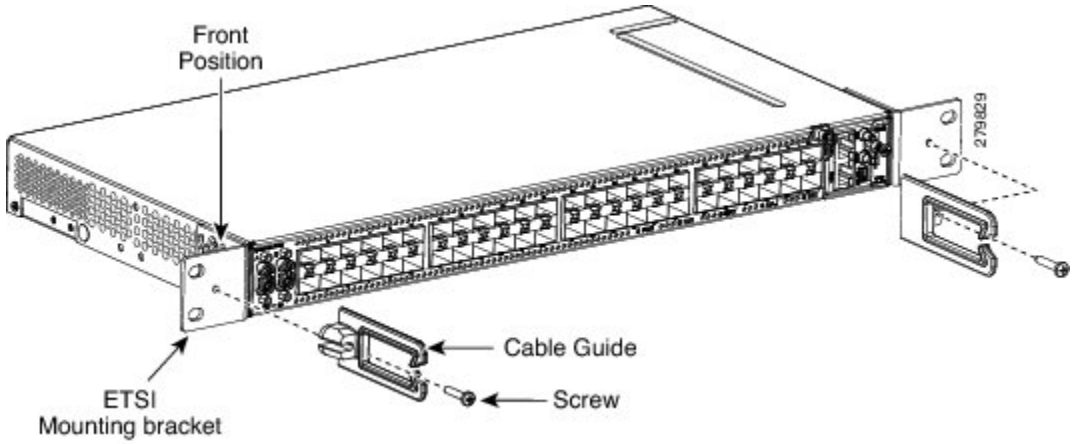
Step 2 Align the mounting bracket screw holes against the CPT 50 shelf screw holes.

Step 3 Insert the M4 flat screws and tighten them to a torque value of 11.5 in-lbs (1.3 N-m).

Step 4 Repeat Step 1 to Step 3 to mount the bracket on the opposite side.

Step 5 Align the cable guide screw hole against the mount bracket screw hole, as shown in this figure.

Figure 19: Mounting the Cable Guide on the Bracket



Step 6 Insert the M4 screw and tighten it to a torque value of 6.5 in-lbs (0.75 N-m) .

Note The cable guide is made of plastic. Therefore a lower torque value should be applied to tighten the cable guide screws to avoid breakage.

Step 7 Repeat Step 5 and Step 6 to install the cable guide on the opposite side.

Step 8 Return to your originating procedure (NTP).

DLP-J176 Mount the CPT 50 Shelf on a Rack (One Person)

Purpose	This task explains how one person can mount the shelf assembly in a rack.
Tools/Equipment	• #2 Phillips Dynamometric screwdriver • Four pan-head Phillips mounting screws
Prerequisite Procedures	NTP-J53 Unpack and Inspect the CPT 50 Shelf, on page 65
Required/As Needed	As Needed
Onsite/Remote	Onsite
Security Level	None

Note The CPT 50 shelf requires a minimum of 1.75 inches (44.44 mm) of vertical rack space. To ensure that the mounting is secure, use two M6 mounting screws on each side of the shelf for ETSI rack installation, and two 12-24 x 3/4 pan-head Phillips mounting screws on each side of the shelf for ANSI rack installation. A shelf assembly should be mounted at the bottom of the rack if it is the only unit in the rack.

Note In an ANSI rack, the chassis can be installed in the front or the middle position. In an ETSI rack, the chassis can be installed only in the front position.

Procedure

Step 1 Verify that the proper fuse panel has been installed in the top mounting space. If a fuse panel is not present, you must install one according to manufacturer instructions:

- For a 48 V DC power supply, the fuse rating must not exceed 10 A.
- For a 24 V DC power supply, the fuse rating must not exceed 15 A.
- For an AC power supply, the fuse rating must not exceed 10 A or 15 A, depending on the standards in various countries. The overcurrent and short circuit protection must be in accordance with local and national electrical codes.

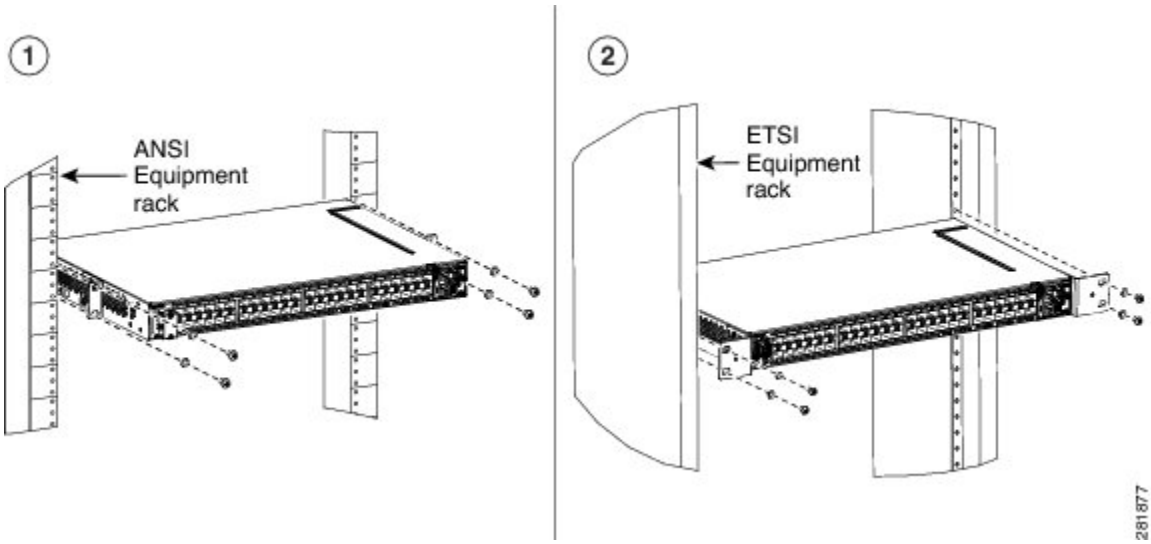
Step 2 Ensure that the shelf assembly is mounted on the appropriate rack equipment:

- 23 inches (584.2 mm) or 19 inches (482.6 mm) for ANSI racks
- 600 x 600-mm (23.6 x 23.6-inch) or 600 x 300-mm (23.6 x 11.8-inch) for ETSI racks.
- For an AC power supply, the fuse rating must not exceed 10 A or 15 A, depending on the standards in various countries. The overcurrent and short circuit protection must be in accordance with local and national electrical codes.

  Diagram 1 of Figure 20: Mounting an CPT 50 Shelf in a Rack, on page 81 shows the CPT 50 shelf mounted on an ANSI rack in the middle position using 19-inch mounting brackets.

  Diagram 2 of Figure 20: Mounting an CPT 50 Shelf in a Rack, on page 81 shows the CPT 50 shelf mounted on an ETSI rack in the front position using mounting brackets.

Figure 20: Mounting an CPT 50 Shelf in a Rack



Step 3 Lift the shelf to the desired position in the rack.

Step 4 Align the screw holes on the mounting brackets with the mounting holes in the rack.

Step 5 Using the Phillips Dynamometric screwdriver, install one mounting screw in each side of the assembly:

- For an ANSI rack, use 12-24 x 3/4 pan-head Phillips mounting screws and tighten it to a torque value of 22 in-lbs (2.5 Nm)
- For an ETSI rack, use M6 mounting screws and tighten it to a torque value of 22 in-lbs (2.5 Nm)

Step 6 When the shelf assembly is secured to the rack, install the remaining two mounting screws on either sides of the shelf assembly.

Step 7 Return to your originating procedure (NTP).

DLP-J177 Mount the CPT 50 Shelf on the Wall

Purpose	This task explains how to mount the CPT 50 shelf on the wall.
Tools/Equipment	• #2 Phillips Dynamometric screwdriver
Prerequisite Procedures	NTP-J53 Unpack and Inspect the CPT 50 Shelf, on page 65
Required/As Needed	As Needed
Onsite/Remote	Onsite
Security Level	None

Note The CPT 50 shelf requires a minimum of 23.65 inches (600-mm) vertical length and a minimum of 15.75 inches (400-mm) horizontal width on the wall. Wall mount brackets are used to mount the CPT 50 shelf on the wall. The type of screws used to mount the brackets on the wall depends on the wall-type; wall mount brackets are not provided by Cisco. The screws used must be able to sustain an overall weight of at least 10 kg (22 lb).

Procedure

Step 1 Verify that the proper fuse panel has been installed in the top mounting space. If a fuse panel is not present, you must install one according to manufacturer instructions:

- For a 48 V DC power supply, the fuse rating must not exceed 10 A.
- For a 24 V DC power supply, the fuse rating must not exceed 15 A.
- For an AC power supply, the fuse rating must not exceed 10 A or 15 A, depending on the standards in various countries. The overcurrent and short circuit protection must be in accordance with local and national electrical codes.

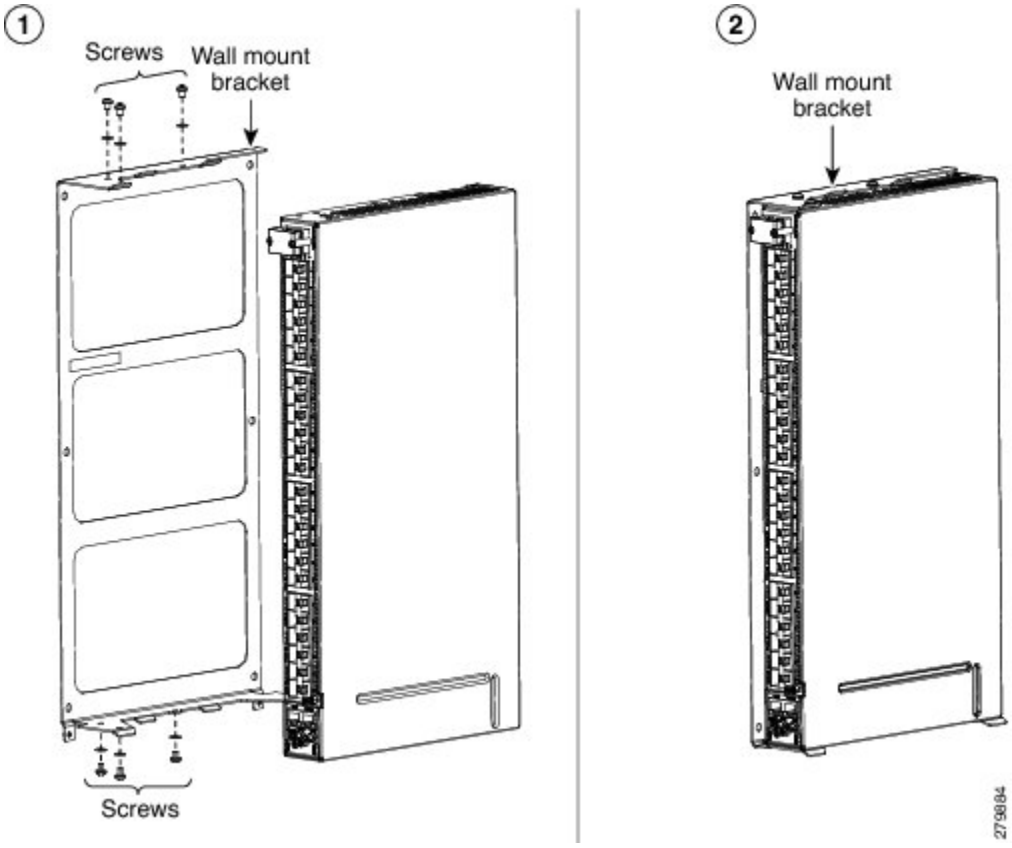
Step 2 Mount the bracket on the wall, as shown in Figure 21: Wall Mounting of the CPT 50 Shelf, on page 83. To mount the bracket on a non-concrete wall, choose the bracket holes based on the wall structure. At least four

screws must be used to mount the bracket on the wall. Based on the wall material, apply the torque value provided by the screw vendor.

Step 3 Align the mounting bracket screw holes against the shelf screw holes, as shown in diagram 1 of Figure 21: Wall Mounting of the CPT 50 Shelf, on page 83.

Step 4 Insert six M4 pan-head screws and tighten them to a torque value of 11.5 in-lbs (1.3 N-m), as shown in diagram 2 of Figure 21: Wall Mounting of the CPT 50 Shelf, on page 83.

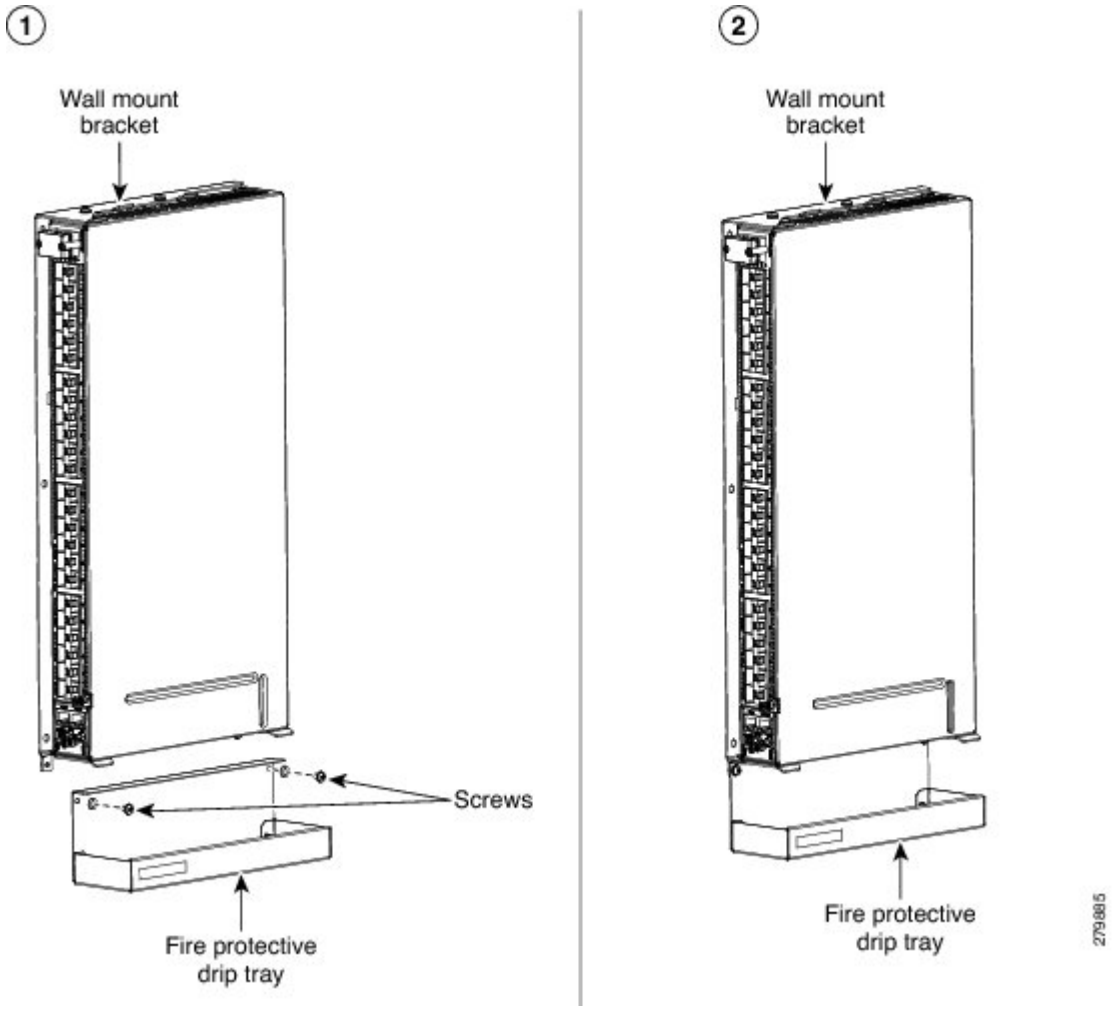
Figure 21: Wall Mounting of the CPT 50 Shelf



Step 5 Align the fire protective drip tray screw holes against the wall mounting bracket screw holes, as shown in diagram 1 of Figure 22: Mounting the Fire Protective Cover, on page 84. The fire protective drip tray is present in the wall mount accessory kit provided by Cisco.
The part number of the fire protective drip tray is Cisco PN 700-31762-XX. The product identifier (PID) of the wall mount accessory kit is CPT-50-BRKTWM= and the part number is Cisco PN 53-3513-XX.

Step 6 Insert two M4 pan-head screws and tighten them to a torque value of 11.5 in-lbs (1.3 N-m), as shown in diagram 2 of Figure 22: Mounting the Fire Protective Cover, on page 84.

Figure 22: Mounting the Fire Protective Cover



Step 7 Return to your originating procedure (NTP).

DLP-J178 Mount the CPT 50 Shelf on the Desktop

Purpose	This task explains how to mount the shelf on the desktop.
Tools/Equipment	• #2 Phillips Dynamometric screwdriver

Prerequisite Procedures	NTP-J53 Unpack and Inspect the CPT 50 Shelf, on page 65
Required/As Needed	As Needed
Onsite/Remote	Onsite
Security Level	None

Procedure

Step 1 Verify that the proper fuse panel has been installed in the top mounting space. If a fuse panel is not present, you must install one according to manufacturer instructions:

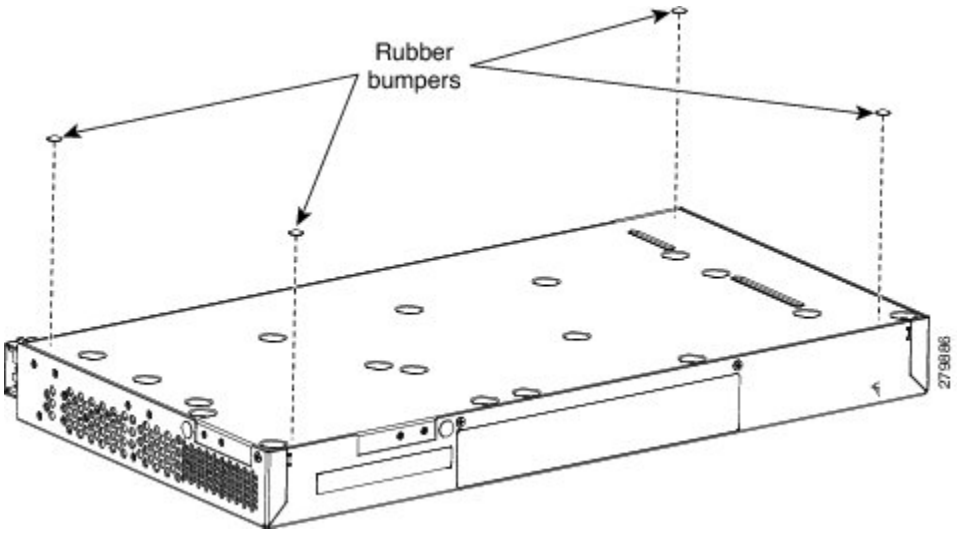
- For a 48 V DC power supply, the fuse rating must not exceed 10 A.
- For a 24 V DC power supply, the fuse rating must not exceed 15 A.
- For an AC power supply, the fuse rating must not exceed 10 A or 15 A, depending on the standards in various countries. The overcurrent and short circuit protection must be in accordance with local and national electrical codes.

Step 2 Locate the rubber bumpers provided in the accessory tool kit.

Step 3 Place the CPT 50 shelf upside down on a smooth, flat surface.

Step 4 Peel off the rubber bumpers from the adhesive strip and place it adhesive-side down onto all the four corners of the surface, as shown in this figure.

Figure 23: Desktop Mounting of the CPT 50 shelf



Step 5 Place the CPT 50 shelf on a desktop, or other flat and secure surface.

Step 6 Return to your originating procedure (NTP).

Power Module

The CPT 50 shelf is available in four variations based on the power module :

- CPT 50 shelf with an AC power module for ANSI and ETSI standards
- CPT 50 shelf with a DC power module (48 V) for ANSI standard
- CPT 50 shelf with a DC power module (48 V) for ETSI standard
- CPT 50 shelf with a DC power module (24 V) for ANSI standard

Note Do not remove the top cover of the CPT 50 shelf.

CPT 50 Shelf with an AC Power Module

The AC power module converts the AC input current to DC output current. The AC power module has one AC single phase with 3- pole (line L, Neutral N, and Protective Earth PE) input connector.

CPT 50 Shelf with a DC Power Module

The CPT 50 shelf with a DC power module can be powered by redundant DC power lines, however a single power line can power the entire CPT 50 shelf.

The CPT 50 shelf with DC power module for ETSI standard has two input battery connectors (two poles)—–48V, RET for power terminals A and B.

The CPT 50 shelf with DC power module for ANSI standard has single terminal block with four poles—–48V, RET for power terminals A and B.

Fan-Tray Assembly

The fan-tray assembly is preinstalled on the right side of the CPT 50 shelf. The fan-tray assembly is removable and holds fans and fan-control circuitry for the CPT 50 shelf. The fan-tray assembly should be accessed only if a fan failure occurs.

The fan-tray assembly has the following ports:

- EOBC (Ethernet Out-of-Band Channel)—An RJ-45 port that supports high bandwidth external connectivity. If the CPT-50 shelf fails to boot up, the EOBC port also called as the disaster recovery port is used to log in to the CPT-50 shelf for troubleshooting.

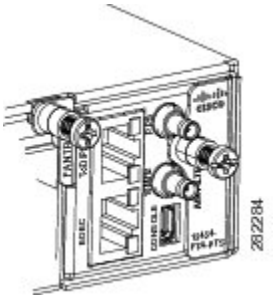
  Note The EOBC port is meant only for TAC (Technical Assistance Center) usage.

- PPS (Pulse Per Second)—A mini BNC output port that provides timing signals to an external equipment from the CPT 50 shelf .

- 10MH—A mini BNC output port that provides timing signals at a frequency of 10 MHz to an external equipment from the CPT 50 shelf and RET for power terminals A and B.
- ToD/PPS (Time of Day/Pulse Per Second)—An RJ-45 serial output port that provides time and day information and timing signals to an external equipment from the CPT 50 shelf.
- CONSOLE—A USB port that is used to connect a console terminal. The console terminal can be one of the following:
  - An ASCII terminal or a PC running terminal emulation software
  - A modem

The following figure shows the ports on the fan-tray assembly:

Figure 24: Ports on the Fan-Tray Assembly



Note The timing signals are compliant with the IEEE 1588 standard.

The console port provides access to the CPT 50 shelf either locally (using a console terminal), or remotely (using a modem). Console connections transmit at slower speeds than modems; therefore, the console connection is suited for use with console terminals.

Note An RJ-45 serial port is used for TOD/PPS functionality. The two RJ-45 pins 7 and 8 is used for TOD (Time Of Day) functionality and the other two RJ-45 pins 1 and 2 are used for PPS functionality. Even though an RJ-45 cable is used for TOD/PPS connection, a serial link is established. Two mini coax connectors with RG316 1.0/2.3 M/M cables (50 ohm) are used for PPS (Pulse Per Second) and for 10MHz sinusoidal signal. Cable for TOD/PPS and 10MHz shall be shielded.

Note For rules about provisioning timing references, see Telcordia SR-NWT-002224.

Fan Speed

Fan speed is controlled by the microprocessor present in the CPT 50 shelf. The sensors measure the critical component temperature of the CPT 50 shelf. Fan speed options are low, medium, and high.

Fan Failure

If one or more fans fail on the fan-tray assembly, replace the entire assembly. You cannot replace individual fans. The red Fan Fail LED on the front of the CPT 50 shelf illuminates when one or more fans fail. The red Fan Fail LED clears after you install a working fan-tray.

NTP-J55 Replace the Fan-Tray Assembly in the CPT 50 Shelf

Purpose	This procedure describes how to replace the fan-tray assembly in the CPT 50 shelf.
Tools/Equipment	#2 Phillips Dynamometric screwdriver
Prerequisite Procedures	• NTP-J54 Install the CPT 50 Shelf, on page 71 • Connect the chassis to the office ground. For detailed instructions on how to ground the chassis, see the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Caution Do not operate an CPT 50 shelf without an air filter.

Note The estimated time for a skilled technician to replace an equipment fan or fan tray is 2 minutes.

Note The fan or the cooling unit can be replaced without service interruption.

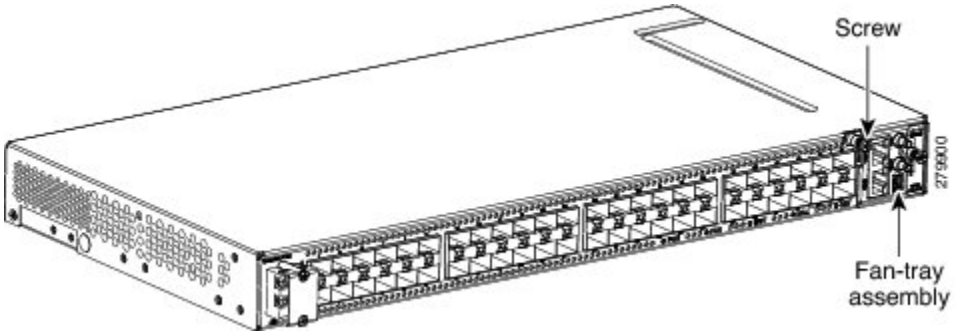
Caution Do not force a fan-tray module into place. Doing so can damage either the connectors on the fan tray or the connectors on the back panel of the shelf assembly, or both.

Note Error messages appear on the TNC or TSC card, the fan-tray LED, and in Cisco Transport Controller (CTC) when the fan-tray module is removed from the shelf or when one fan is not working.

Procedure

Step 1 Loosen the screw on the fan-tray assembly, as shown in this figure.

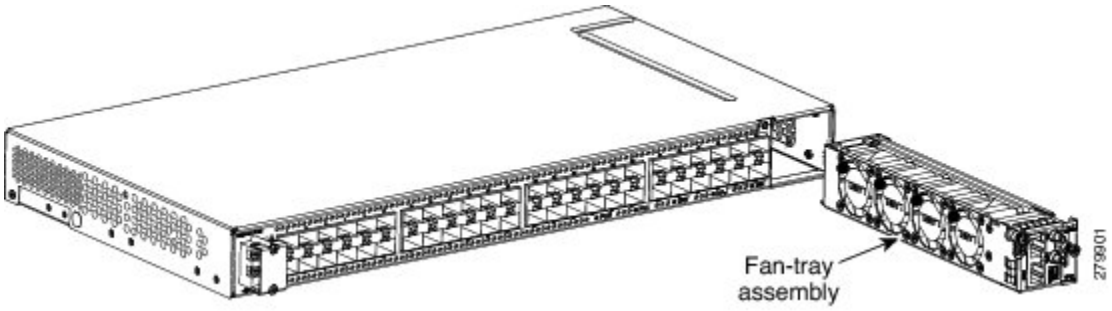
Figure 25: Fan-Tray Assembly in the CPT-50 Shelf



Step 2 Extract the fan-tray assembly partially (not more than 1 inch) to disconnect the backplane connector and wait until the fan stops.

Step 3 When the fans have stopped, pull the fan-tray assembly completely out of the shelf, as shown this figure.

Figure 26: Fan-Tray Extracted



Step 4 Slide the new fan-tray assembly into the shelf until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.

Step 5 Tighten the M3 screw to a torque value of 4 in-lbs (0.45 N-m) on the fan-tray assembly.
Stop. You have completed this procedure.

NTP-J56 Replace the Air Filter in the CPT 50 Shelf

Purpose	This procedure explains how to replace the air filter of the CPT 50 shelf.
Tools/Equipment	#2 Phillips Dynamometric screwdriver

Prerequisite Procedures	• NTP-J54 Install the CPT 50 Shelf, on page 71 • Connect the chassis to the office ground. For detailed instructions on how to ground the chassis, refer to the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

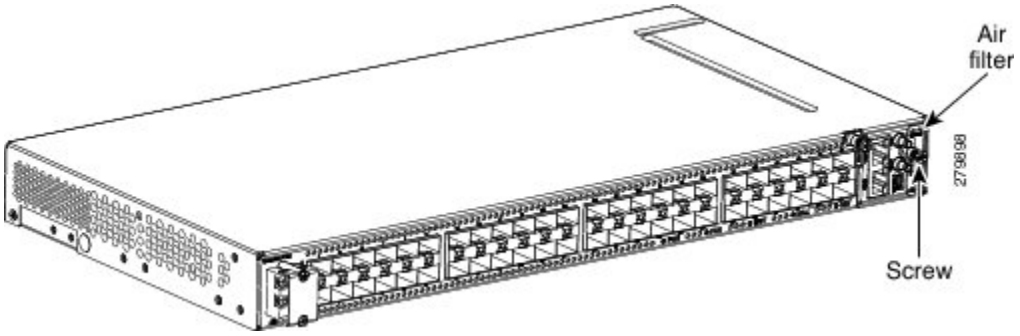
Caution Do not operate a CPT 50 shelf without an air filter.

Note Replacement or cleaning of an air filter is recommended every 60 days. Air filters are replaceable or reusable.

Procedure

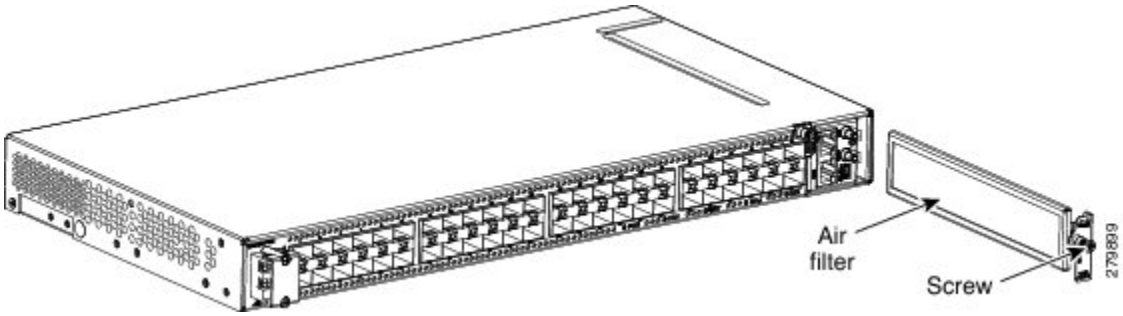
Step 1 Loosen the screw on the air filter faceplate, as shown in this figure.

Figure 27: Removing the Air Filter



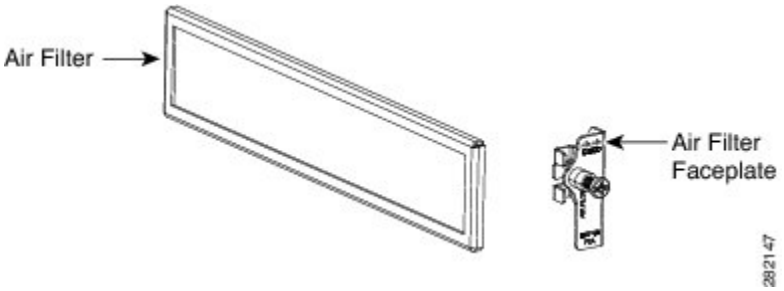
Step 2 Extract the air filter from the shelf, as shown in this figure.

Figure 28: Replacing the Air Filter



Step 3 Remove the air filter faceplate from the air filter frame, as shown in this figure.

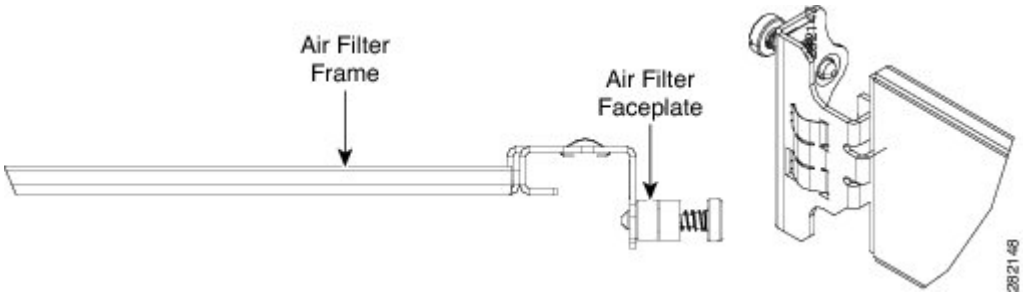
Figure 29: Removing Air filter from the Face Plate



Step 4 Clean or replace the air filter.

Step 5 Insert the air filter faceplate engaging the air filter frame, as shown in this figure.

Figure 30: Attach the Air Filter Faceplate to the Air Filter Frame



Step 6 Insert the air filter into the shelf.

Step 7 Tighten the M3 screw to a torque value of 4.0 in-lbs (0.45 N-m) on the air-filter.
Stop. You have completed this procedure.

Power and Ground Description

Ground the equipment according to Telcordia standards or local practices. The following sections describe how to power and ground the CPT 50 shelf.

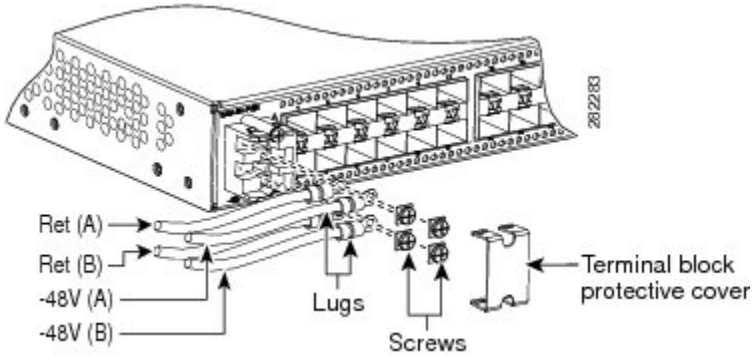
Note For detailed instructions on grounding the CPT 50 shelf, refer to the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.

ANSI Power and Ground

For AC power feed, use the power cable shipped with the CPT 50 shelf. For an AC power supply, the fuse rating must not exceed 10 A or 15 A, depending on the standards in various countries. The overcurrent and short circuit protection must be in accordance with local and national electrical codes. The voltage rating value for AC power ranges between 100 VAC to 240 VAC depending on the standards in various countries. This product is intended for use on the TN and TT power systems.

The CPT 50 shelf for 48 VDC power supply has redundant –48 VDC #14 single-hole lug power terminals. The terminals are labeled RET(A), RET(B), -48V(A), and -48V(B) on the power module. See the figure below:

Figure 31: CPT 50 Shelf for 48 VDC Power Supply



The CPT 50 shelf for 24 VDC power supply has redundant –24 VDC #14 single-hole lug power terminals. The terminals are labeled RET(A), RET(B), -24V(A), and -24V(B) on the power module.

To install redundant DC power feeds, use four power cables and one ground cable. For a single power feed, only two power cables (#14 AWG or larger, copper conductor, 194 degrees Fahrenheit [90 degrees Celsius] minimum) and one ground cable (#8 AWG or larger) are required. Use a conductor with low impedance to ensure circuit overcurrent protection. However, the conductor must have the capability to safely conduct any faulty current that might be imposed.

For a 24 VDC power supply, the fuse rating must not exceed 15 A. The voltages –20 VDC and –28.3 VDC are, respectively, the minimum and maximum voltages required to power the chassis. The nominal steady state voltage is -24 VDC.

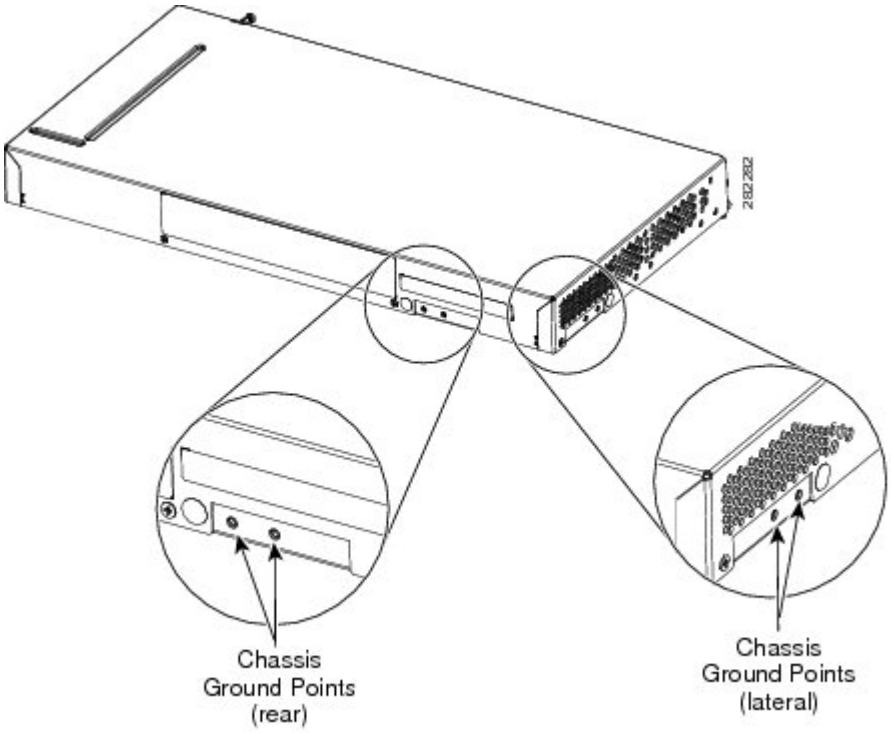
For a 48 VDC power supply, the fuse rating must not exceed 10 A. The voltages –40.5 VDC and –57.6 VDC are, respectively, the minimum and maximum voltages required to power the chassis. Functionality is guaranteed at -40 VDC input voltage, according to GR-1089. The nominal steady state voltage is -48 VDC.

We recommend the following wiring conventions, but customer conventions prevail:

- Red wire for battery connections (–48 VDC or -24 VDC).
- Black wire for battery return connections (RET).
- The battery return connection is treated as DC-I, as defined in Telcordia GR-1089-CORE.

The ground lug must be a dual-hole type, UL Listed, CSA certified, and rated to accept the #8 AWG cable. Two ground threaded holes with M4 screws are provided on the CPT 50 shelf to accommodate the dual-hole lug. See the figure below:

Figure 32: Ground Points on the CPT 50 Shelf



ETSI Power and Ground

The CPT 50 shelf for ETSI has redundant –48 VDC power connectors (DSUB for DC power module) on the DC power module. To install redundant power feeds, use the two power cables shipped with the CPT 50 shelf and one ground cable. For a DC power supply, the fuse rating must not exceed 10 A. The voltages –40.5 VDC and –57.6 VDC are, respectively, the minimum and maximum voltages required to power the chassis. The nominal steady state voltage is -48 VDC.

For AC power feed, use the power cable shipped with the CPT 50 shelf. For an AC power supply, the fuse rating must not exceed 10 A or 15 A, depending on the standards in various countries. The overcurrent and short circuit protection must be in accordance with local and national electrical codes. The voltage rating value for AC power ranges between 100 VAC to 240 VAC depending on the standards in various countries. This product is intended for use on the TN and TT power systems.

⚠

Caution Use only the power cables shipped with the CPT 50 shelf. The part number of the cables is Cisco PN 72-4974-XX and the PID is CPT-DC-CBL-E=.

NTP-J57 Install the Power Feeds and Ground to the CPT 50 Shelf

Purpose	This procedure explains how to install power feeds and ground the CPT 50 shelf.
Tools/Equipment	ANSI and ETSI: • #2 Phillips Dynamometric screwdriver • Medium slot-head screwdriver • Small slot-head screwdriver • Screws • Ground cable 8.37-mm² (#8 AWG) stranded • Listed pressure dual-holes lugs suitable for #14 AWG or larger copper conductors • Wire cutters • Wire strippers • Crimp tool • Fuse panel • ETSI only: ◦ Power cable (from the fuse panel to the power modules), shipped with the CPT 50 shelf ◦ Two-hole grounding lug, shipped with the CPT 50 shelf • ANSI only: ◦ Power cable (from the fuse panel to the assembly), #14 AWG or larger copper conductors, 194°F [90°C])
Prerequisite Procedures	Connect the chassis to the office ground. For detailed instructions on how to ground the chassis, see the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

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

Warning To reduce the risk of electric shock, switch on the power only after the power cord is completely installed into the power module. Statement 390

Warning When stranded wiring is required, use approved wiring terminations, such as closed-loop or spade-type with upturned lugs. These terminations should be the appropriate size for the wires and should clamp both the insulation and conductor. Statement 1002

Warning Before performing any of the following procedures, ensure that power is removed from the DC circuit. Statement 1003

Warning Before working on a chassis or working near power supplies, unplug the power cord on AC units. Statement 246

Warning This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use. Statement 39

Warning Use copper conductors only. Statement 1025

Warning Connect the unit only to DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC 60950-1 based safety standards. Statement 1033

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

Warning This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 10A for CPT 50 shelf with 48 VDC power supply; 15A for CPT 50 shelf with 24 VDC power supply. Statement 1005

Warning This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 10A-15A, 100-240VAC~. Statement 1005

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

Warning This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028

Caution Always use the supplied ESD wristband when working with a powered CPT 50 shelf. For detailed instructions on how to wear the ESD wristband, see the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.

Procedure

Step 1 Verify that the correct fuse panel is installed in the top mounting space:

- For a 48 VDC power supply, the fuse rating must not exceed 10 A.
- For a 24 VDC power supply, the fuse rating must not exceed 15 A.
- For an AC power supply, the fuse rating must not exceed 10 A or 15 A, depending on the standards in various countries. The overcurrent and short circuit protection must be in accordance with local and national electrical codes.

Step 2 Depending on the shelf and the power module installed, complete the necessary task:

- DLP-J179 Connect Office Power (AC) to the CPT 50 Shelf, on page 98.
- DLP-J180 Connect Office Power (DC) to the CPT 50 Shelf (ANSI Only), on page 101.
- DLP-J181 Connect Office Power (DC) to the CPT 50 Shelf (ETSI Only), on page 105.

Step 3 Connect the office ground to the CPT 50 shelf. For detailed instructions on grounding, refer to the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.

Step 4 Complete the DLP-J182 Turn On and Verify AC Office Power on the CPT 50 Shelf, on page 108 or DLP-J183 Turn On and Verify DC Office Power on the CPT 50 Shelf, on page 109 as necessary.
Stop. You have completed this procedure.

DLP-J179 Connect Office Power (AC) to the CPT 50 Shelf

Purpose	This task explains how to connect AC power to the CPT 50 shelf.
Tools/Equipment	• #2 Phillips Dynamometric screwdriver • Medium slot-head screwdriver • Small slot-head screwdriver • Wire wrapper • Wire cutters • Wire strippers • Crimp tool • Fuse panel • Ground cable 8.37-mm² (#8 AWG) stranded
Prerequisite Procedures	• NTP-J54 Install the CPT 50 Shelf, on page 71 • Connect the chassis to the office ground. For detailed instructions on how to ground the chassis, see the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note This product is intended for use on the TN and TT power systems.

Warning When installing or replacing the unit, the ground connection must always be made first and disconnected last. Statement 1046

Warning This equipment shall be connected to AC mains provided with a surge protective device (SPD) at the service equipment complying with NFPA 70, the National Electrical Code (NEC). Statement 7012

Caution The CPT 50 shelf relies on the protective devices in the building installation to protect against short circuit, overcurrent, and ground faults. Ensure that the protective devices are properly rated and comply with national and local codes.

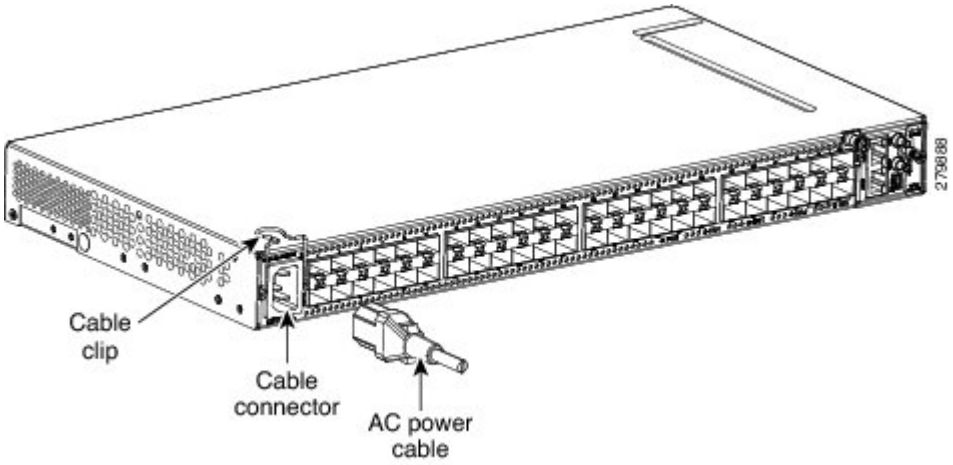
Caution When terminating the frame ground, do not use soldering lug connectors, screwless (push-in) connectors, quick connect connectors, or other friction-fit connectors.

Note If the CPT-50 shelf loses its connection to the line or fabric card, the CPT-50 shelf resets until the connection to the line or fabric card is re-established.

Procedure

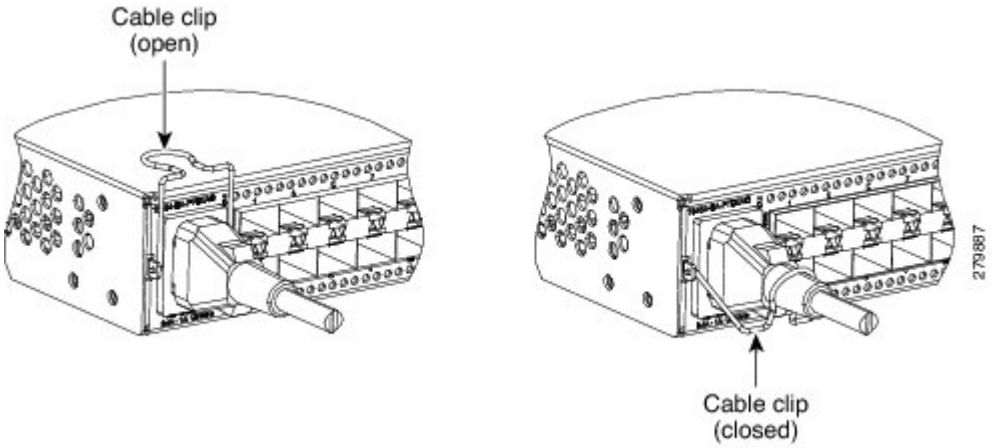
Step 1 Attach the AC power cable to the cable connector in the AC power module, as shown in this figure.

Figure 33: Connecting Office Power—AC Power



Step 2 Close the cable clip to secure the power cable, as shown in this figure.

Figure 34: Cable Clip to Secure the Power Cable



Step 3 Connect the power cable to the fuse panel or power source.

Note The voltage rating value for AC power ranges between 100 VAC to 240 VAC depending on the standards in various countries.

Step 4 Return to your originating procedure (NTP).

DLP-J180 Connect Office Power (DC) to the CPT 50 Shelf (ANSI Only)

Purpose	This task explains how to connect the DC power to the CPT 50 shelf (ANSI Only).
Tools/Equipment	• #2 Phillips Dynamometric screwdriver • Medium slot-head screwdriver • Small slot-head screwdriver • Wire cutters • Wire strippers • Crimp tool • Fuse panel • Ground cable 8.37-mm² (#8 AWG) stranded • Power cable (from fuse panel to assembly), #14 AWG or larger copper conductors, 194°F [90°C]) • Listed pressure dual-holes lugs suitable for #14 AWG or larger copper conductors
Prerequisite Procedures	• NTP-J54 Install the CPT 50 Shelf, on page 71 • Connect the chassis to the office ground. For detailed instructions on how to ground the chassis, see the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning When installing or replacing the unit, the ground connection must always be made first and disconnected last. Statement 1046

Warning Hazardous voltage or energy may be present on DC power terminals. Always replace cover when terminals are not in service. Be sure uninsulated conductors are not accessible when cover is in place. Statement 1075

Caution The CPT 50 shelf relies on the protective devices in the building installation to protect against short circuit, overcurrent, and ground faults. Ensure that the protective devices are properly rated and comply with national and local codes.

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

Note If the CPT-50 shelf loses its connection to the line or fabric card, the CPT-50 shelf resets until the connection to the line or fabric card is re-established.

Procedure

Step 1 Connect the return cables of the power supply to the Earth ground located at the power supply side.

Step 2 Connect the office power according to the fuse panel engineering specifications.

Step 3 Measure and cut the cables as needed to reach the CPT 50 shelf from the fuse panel.

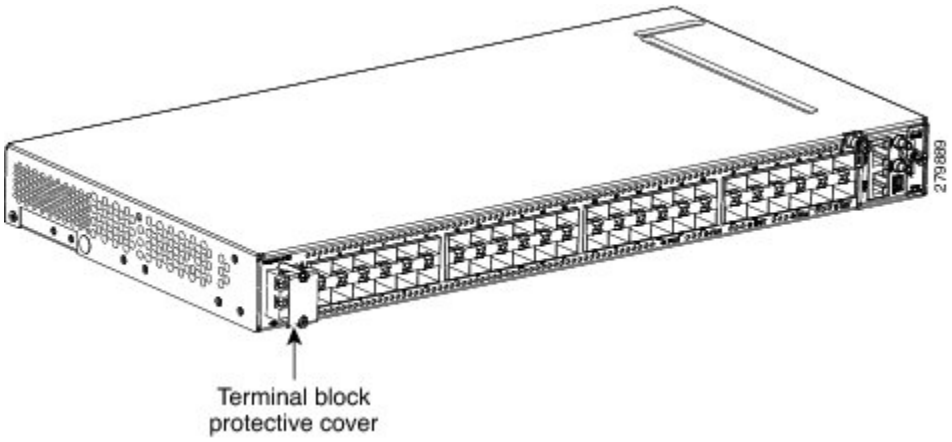
Step 4 Dress the power according to local site practice.

Step 5 Strip 1/2 inch (12.7 mm) of insulation from all power cables that you will use.

Step 6 Crimp the lugs onto the ends of all the power leads.

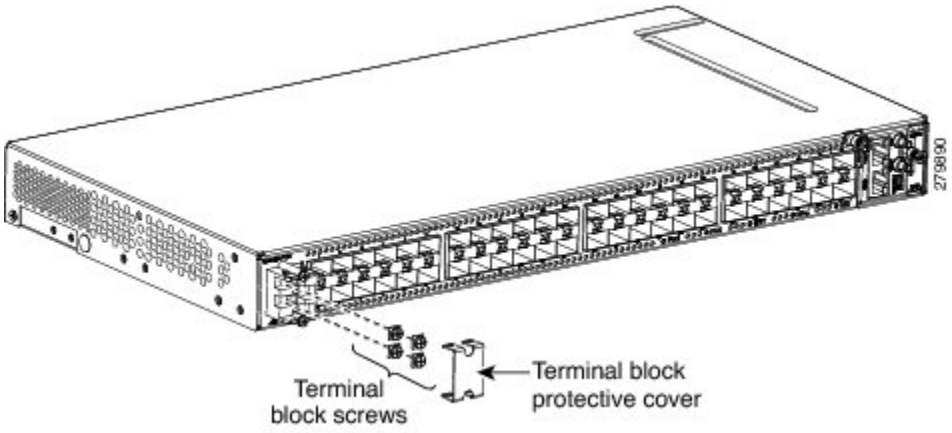
Step 7 Remove the terminal block protective cover, as shown in this figure.

Figure 35: Removing the Terminal Block Protective Cover



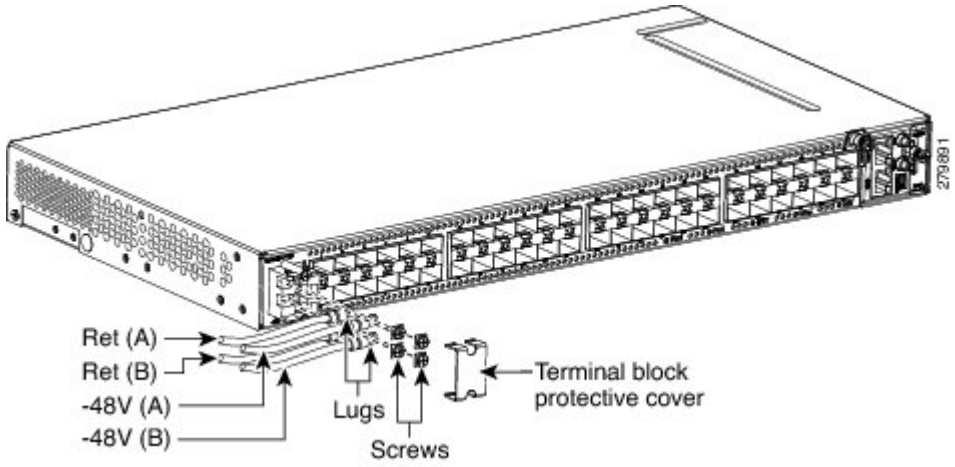
Step 8 Untighten the terminal block screws, as shown in this figure.

Figure 36: Loosening the Terminal Block Screws



Step 9 Insert the lugs, as shown in this figure.

Figure 37: Inserting the Lugs



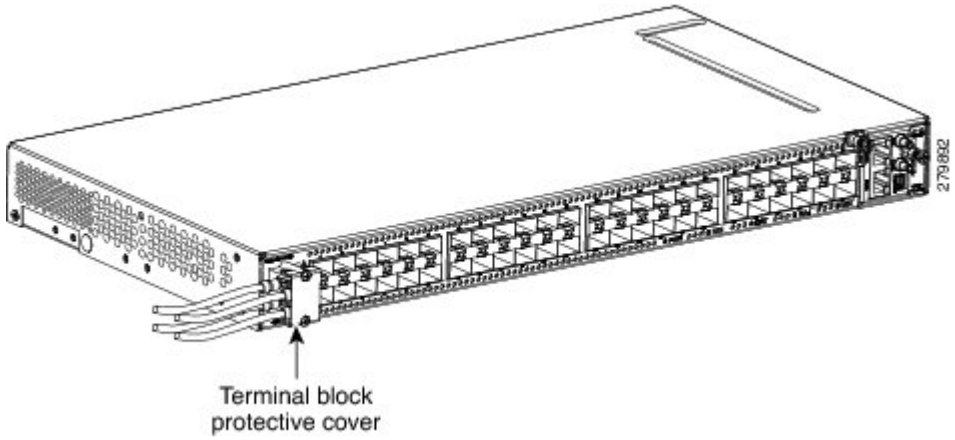
Note There are two DC power terminals—A and B. Each power terminal is connected with two cables—one for RET and the other for -48V.

Step 10 Tighten the M3.5 screws to a torque value of 7 in-lbs (0.79 N-m) to lock the lugs.

Step 11 Mount the terminal block protective cover on the CPT 50 shelf (see the following figure, "Connecting Office Power—DC Power Modules (ANSI Only)").

Note Use only pressure terminal connectors, such as ring and fork types, when terminating the battery, battery return, and frame ground conductors.

Figure 38: Replacing the Terminal Block Protective Cover



Caution Before you make any crimp connections, coat all bare conductors (battery, battery return, and frame ground) with an appropriate antioxidant compound. Bring all unplated connectors, braided strap, and bus bars to a bright finish, then coat with an antioxidant before you connect them. You do not need to prepare tinned, solder-plated, or silver-plated connectors and other plated connection surfaces, but always keep them clean and free of contaminants.

Caution When terminating the power, return (RET), and frame ground, do not use soldering lug, screwless (push-in) connectors, quick-connect, or other friction-fit connectors.

Step 12 Return to your originating procedure (NTP).

DLP-J181 Connect Office Power (DC) to the CPT 50 Shelf (ETSI Only)

Purpose	This task explains how to connect the DC power to the CPT 50 shelf (ETSI Only).
Tools/Equipment	• #2 Phillips Dynamometric screwdriver • Medium slot-head screwdriver • Small slot-head screwdriver • Wire wrapper • Wire cutters • Wire strippers • Crimp tool • Fuse panel • Ground cable 8.37-mm² (#8 AWG) stranded
Prerequisite Procedures	• NTP-J54 Install the CPT 50 Shelf, on page 71 • Connect the chassis to the office ground. For detailed instructions on how to ground the chassis, see the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning When installing or replacing the unit, the ground connection must always be made first and disconnected last. Statement 1046

Warning Hazardous voltage or energy may be present on DC power terminals. Always replace cover when terminals are not in service. Be sure uninsulated conductors are not accessible when cover is in place. Statement 1075

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

Caution The CPT 50 shelf relies on the protective devices in the building installation to protect against short circuit, overcurrent, and ground faults. Ensure that the protective devices are properly rated and comply with national and local codes.

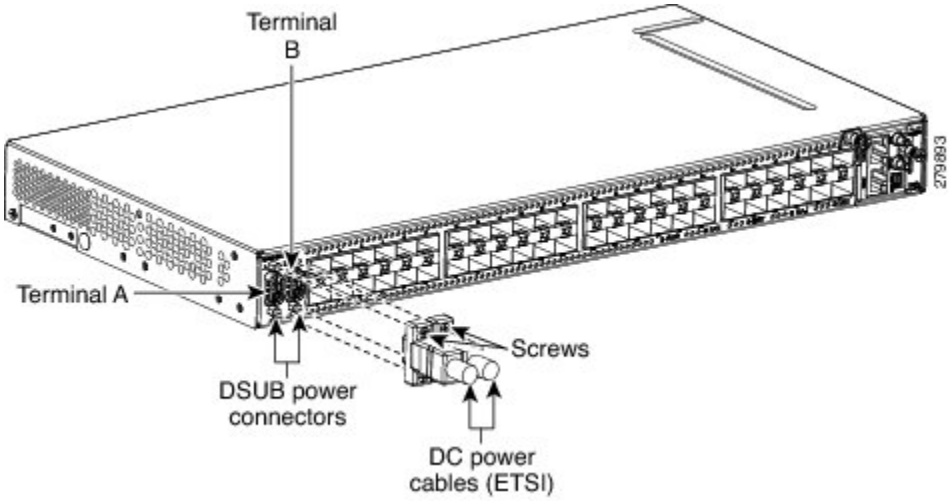
Note If the CPT 50 shelf loses its connection to the line or fabric card, the CPT 50 shelf resets until the connection to the line or fabric card is re-established.

Procedure

Step 1 Connect the return cables of the power supply to the Earth ground located at the power supply side.

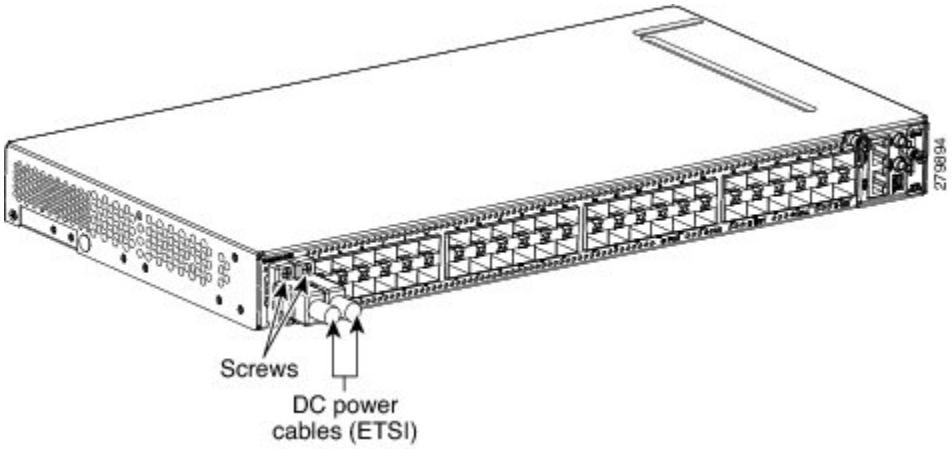
Step 2 Attach the DC ETSI power cables to the DSUB power connectors of the DC power module, as shown in this figure.

Figure 39: Connecting DC ETSI Power Cables to the DSUB Power Connectors



Step 3 Tighten the M3 pan-head screws to a torque value of 4 in-lbs (0.45 N-m) to secure the cable, as shown in this figure.

Figure 40: Securing the DC Power Cables



Note Use only pressure terminal connectors, such as ring and fork types, when terminating the battery, battery return, and frame ground conductors.

Caution Before you make any crimp connections, coat all bare conductors (battery, battery return, and frame ground) with an appropriate antioxidant compound. Bring all unplated connectors, braided strap, and bus bars to a bright finish, then coat with an antioxidant before you connect them. You do not need to prepare tinned, solder-plated, or silver-plated connectors and other plated connection surfaces, but always keep them clean and free of contaminants.

Caution When terminating power, return, and frame ground, do not use soldering lug, screwless (push-in) connectors, quick-connect, or other friction-fit connectors.

Step 4 Return to your originating procedure (NTP).

DLP-J182 Turn On and Verify AC Office Power on the CPT 50 Shelf

Purpose	This task explains how to measure the power to verify correct power and returns for the CPT 50 shelf.
Tools/Equipment	Voltmeter
Prerequisite Procedures	• NTP-J54 Install the CPT 50 Shelf, on page 71 • Connect the chassis to the office ground. For detailed instructions on how to ground the chassis, see the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*. • DLP-J179 Connect Office Power (AC) to the CPT 50 Shelf, on page 98
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning To reduce the risk of electric shock, switch on the power only after the power cord is completely installed into the power module. Statement 390

Caution Do not apply power to the shelf assembly until you complete all the installation steps.

Procedure

Step 1 To power up the node, insert the fuse into the fuse position according to site practice. For an AC power supply, the fuse rating must not exceed 10 A or 15 A, depending on the standards in various countries.

Step 2 If the CPT 50 shelf does not power up, check the voltage at the power source using a voltmeter. The voltage should be 100 VAC to 240 VAC +/-10 percent.

Step 3 Return to your originating procedure (NTP).

DLP-J183 Turn On and Verify DC Office Power on the CPT 50 Shelf

Purpose	This task explains how to measure the power to verify correct power and returns for the CPT 50 shelf.
Tools/Equipment	Voltmeter
Prerequisite Procedures	• NTP-J54 Install the CPT 50 Shelf, on page 71 • Connect the chassis to the office ground. For detailed instructions on how to ground the chassis, see the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*. • DLP-J180 Connect Office Power (DC) to the CPT 50 Shelf (ANSI Only), on page 101 (or) • DLP-J181 Connect Office Power (DC) to the CPT 50 Shelf (ETSI Only), on page 105
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning To reduce the risk of electric shock, switch on the power only after the power cord is completely installed into the power module. Statement 390

Caution Do not apply power to the shelf assembly until you complete all the installation steps.

Procedure

Step 1 Using a voltmeter, verify the office battery and ground at the following points on the fuse panel:

a) To verify the power, place the black test lead of the voltmeter to the return (RET). Place the red test lead on the BAT-A connection and verify that:

- For a 24 VDC power supply, the voltage is between –20 VDC and –28.3 VDC. Place the red test lead on the BAT-B connection and verify that it is between –20 VDC and –28.3 VDC.

  Note The voltages –20 VDC and –28.3 VDC are, respectively, the minimum and maximum voltages required to power the CPT 50 shelf that has 24V DC power supply. The nominal steady state voltage is -24 VDC.

- For a 48 VDC power supply, the voltage is between –40.5 VDC and –57.6 VDC. Place the red test lead on the BAT-B connection and verify that it is between –40.5 VDC and –57.6 VDC.

  Note The voltages –40.5 VDC and –57.6 VDC are, respectively, the minimum and maximum voltages required to power the CPT 50 shelf that has 48V DC power supply. The nominal steady state voltage is -48 VDC.

b) To verify the ground, place the black test lead of the voltmeter to the frame ground. Place the red test lead on the BAT-A return ground and verify that no voltage is present, that is, meter reading must be 0 VDC. Place the red test lead on the BAT-B return ground and verify that no voltage is present, that is, meter reading must be 0 VDC.

Step 2 To power up the node, insert the fuse into the fuse position according to site practice. For a 24 VDC power supply, the fuse rating must not exceed 15 A. For a 48V DC power supply, the fuse rating must not exceed 10 A.

Step 3 Using a voltmeter, verify the CPT 50 shelf for –48 VDC or –24 VDC battery and return:

a) To verify the BAT-A of the shelf, place the black lead of the voltmeter to the return. Place the red test lead to the –48V or –24V (BAT-A battery connection) red cable. For a 48 VDC power supply, verify that it reads between –40.5 VDC and –57.6 VDC. For a 24 VDC power supply, verify that the voltage reads between –20 VDC and –28.3 VDC. Then place the red test lead of the voltmeter to the RET1 (BAT-A return ground) black cable and verify that no voltage is present, that is, meter reading must be 0 VDC.

Note For a CPT 50 shelf that has 24 VDC power supply, the voltages –20 VDC and –28.3 VDC are, respectively, the minimum and maximum voltages required to power the CPT 50 shelf. The nominal steady state voltage is –24 VDC. To prevent damage to the CPT 50 shelf, the voltage must not exceed -30 VDC.

Note For a CPT 50 shelf that has 48 VDC power supply, the voltages –40.5 VDC and –57.6 VDC. are, respectively, the minimum and maximum voltages required to power the CPT 50 shelf. The nominal steady state voltage is –48 VDC.

b) To verify the BAT-B of the shelf, place the black test lead of the voltmeter to the return. Place the red test lead to the –48 V or –24 V (BAT-B battery connection) red cable. For a 48 VDC power supply, verify that it reads between –40.5 VDC and –57.6 VDC. For a 24 VDC power supply, verify that the voltage reads between –20 VDC and –28.3 VDC. Then place the red test lead of the voltmeter to the RET2 (BAT-B return ground) black cable and verify that no voltage is present, that is, meter reading must be 0 VDC.

c) To verify the ground, place the black test lead of the voltmeter to the frame ground. Place the red test lead on the BAT-A return ground and verify that no voltage is present, that is, meter reading must be 0 VDC.

Place the red test lead on the BAT-B return ground and verify that no voltage is present, that is, meter reading must be 0 VDC.

Step 4 Return to your originating procedure (NTP).

NTP-J58 Connecting Cables to the EOBC, Timing, and Console Ports

Purpose	This procedure describes how to connect cables to the EOBC, timing, and console ports in the CPT 50 shelf.
Tools/Equipment	• Mini-BNC cables (Cisco PN 72-5118-XX) • USB cable • CAT-5 Ethernet cable
Prerequisite Procedures	• NTP-J54 Install the CPT 50 Shelf, on page 71 • Connect the chassis to the office ground. For detailed instructions on how to ground the chassis, refer to the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution Always use the supplied Electrostatic Discharge (ESD) wristband when working with a powered CPT 50 shelf. For detailed instructions on how to wear the ESD wristband, see the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.

Procedure

Step 1 Complete the DLP-J184 Connect the Timing Cables to the PPS, 10MHz, and ToD/PPS Ports, on page 112 to connect timing to an external equipment.

Step 2 Complete the DLP-J185 Install Cables to the EOBC or Console Port, on page 113 to install the cables to the EOBC or console port.

Stop. You have completed this procedure.

DLP-J184 Connect the Timing Cables to the PPS, 10MHz, and ToD/PPS Ports

Purpose	This procedure describes how to connect the timing cables to the PPS, 10 MHz, and ToD/PPS ports on the CPT 50 shelf.
Tools/Equipment	• Mini-BNC cables (Cisco PN 72-5118-XX) • CAT-5 Ethernet cable
Prerequisite Procedures	• NTP-J54 Install the CPT 50 Shelf, on page 71 • Connect the chassis to the office ground. For detailed instructions on how to ground the chassis, refer to the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning The intra-building ports of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring. **Statement 7005**

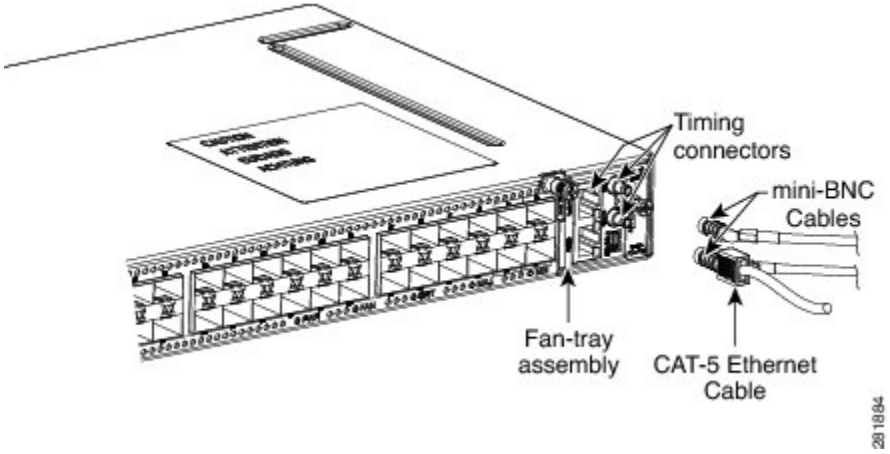
Note For rules about provisioning timing references, see ITU-T G.813.

Note To unplug the RJ-45 cables connected to the ToD/PPS and EOBC ports on the fan-tray, use small pliers or a screwdriver.

Procedure

Step 1 Locate the timing connectors (PPS, 10 MHz, or ToD/PPS) on the fan-tray assembly of the CPT 50 shelf, as shown in this figure.

Figure 41: Timing Connectors (PPS, 10 MHz, or ToD/PPS) on the Fan-Tray Assembly



Step 2 To connect the PPS or 10 MHz port:

a) Connect one end of the mini-BNC cable to the PPS or 10 MHz mini-BNC output port.
b) Connect the other end of the mini-BNC cable to an external equipment to provide timing signals.

Step 3 To connect the ToD/PPS RJ-45 output port:

a) Connect one end of a standard CAT-5 Ethernet cable to the ToD/PPS RJ-45 output port.
b) Connect the other end of the CAT-5 Ethernet cable to an external equipment to provide timing signals.

Step 4 Return to your originating procedure (NTP).

DLP-J185 Install Cables to the EOBC or Console Port

Purpose	This procedure explains how to connect cables to the EOBC or console port on the CPT 50 shelf.
Tools/Equipment	• USB cable • CAT-5 Ethernet cable

Prerequisite Procedures	• NTP-J54 Install the CPT 50 Shelf, on page 71 • Connect the chassis to the office ground. For detailed instructions on how to ground the chassis, refer to the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning The intra-building ports of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring. **Statement 7005**.

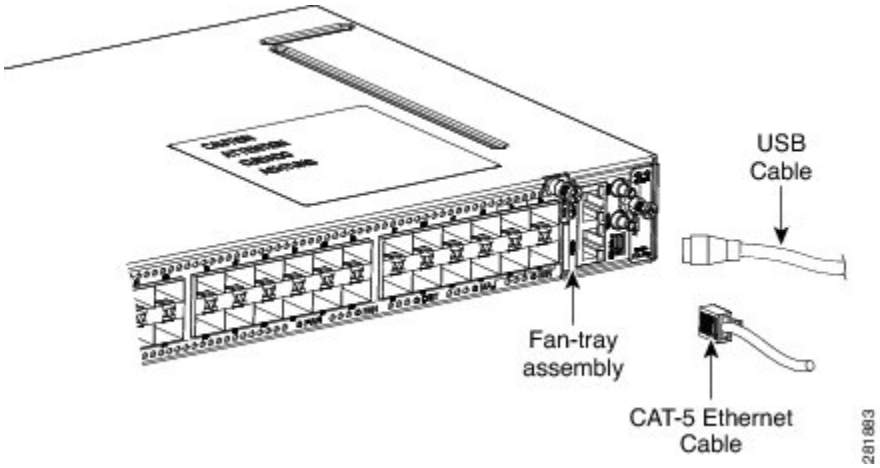
Note The console port is used for the setup and maintenance of the CPT 50 shelf and the EOBC port is used for disaster recovery, that is, to log in to the CPT 50 shelf for troubleshooting when the connection between the CPT 50 shelf and CPT 600 shelf is lost.

Note To unplug the RJ-45 cables connected to the ToD/PPS and EOBC ports on the fan-tray, use small pliers or a screwdriver.

Procedure

Step 1 Locate the EOBC port or the console port on the fan tray assembly of the CPT 50 shelf, as shown in this figure.

Figure 42: EOBC or Console Port on the Fan-Tray Assembly



Step 2 To connect the EOBC port:

a) Connect one end of a standard CAT-5 Ethernet cable to the EOBC port.
b) Connect the other end of the CAT-5 Ethernet cable to establish external connectivity.

Step 3 To connect the console port:

a) Connect one end of the USB cable to the console port.
b) Connect the other end of the USB cable to the console terminal or a modem that connects to the console terminal.

Step 4 Return to your originating procedure (NTP).

NTP-J59 Install and Route Fiber-Optic Cables

Purpose	This task describes how to install and route fiber-optic cables.
Tools/Equipment	• Cables • Tie-wrap
Prerequisite Procedures	None
Required/As Needed	Required

Onsite/Remote	Onsite
Security Level	None

Warning Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments. Statement 1051

Caution When connecting an optical fiber patch cord between the CPT 50 shelf and the optical card ports in the Cisco ONS 15454 M6 or Cisco ONS 15454 M2, use the electrostatic discharge wristband supplied with the Cisco ONS 15454 M6 or M2.

Note Always clean all the fiber connectors thoroughly before making the connection with the mating adapter. Very small particles can permanently damage the end of the mating fiber inside the CPT 50 shelf, which makes regular cleaning imperative. For cleaning instructions, see NTP-J60 Clean Fiber Connectors, on page 118.

Note The CPT 50 shelf features LC/UPC bulkhead adapters. Always use fiber-optic cables equipped with the corresponding (LC/UPC) connector type. Using any other type of connector results in damage to the connector or adapter, or both.

Procedure

Step 1 Place the LC/UPC cable connector in front of the corresponding bulkhead adapter on the front panel of the CPT 50 shelf.

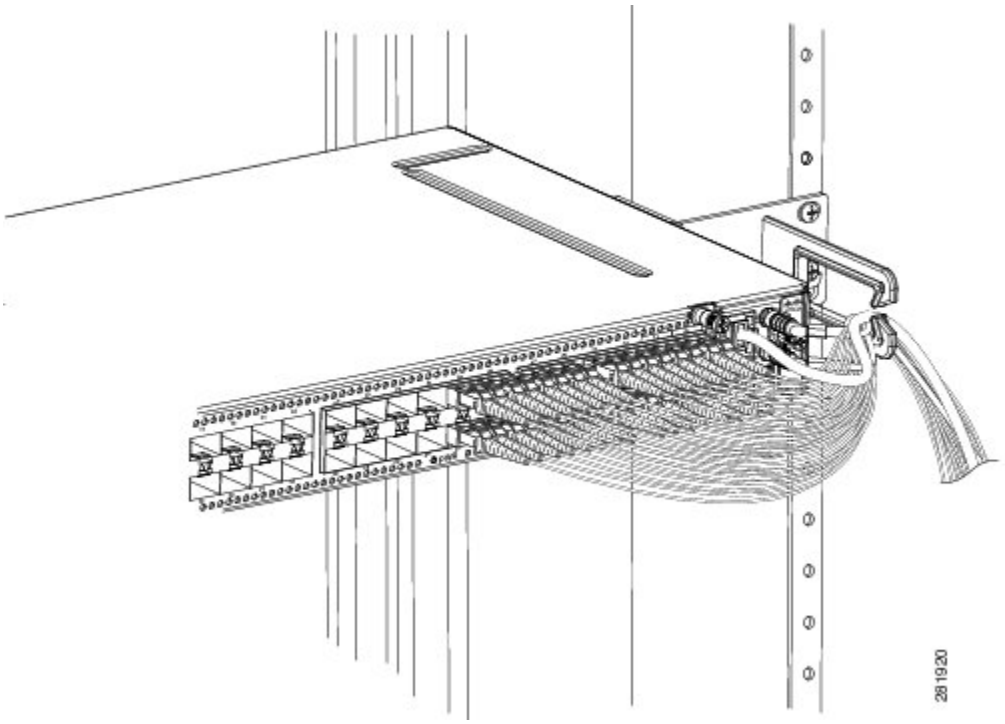
Step 2 Align the keyed ridge of the cable connector with the slot in the receiving adapter.

Step 3 Gently push the cable connector into the adapter until you hear a click, which indicates that the latching system is engaged.

Step 4 Route the fiber cables through the cable guide (left and right side). A tie-wrap is tied around the fiber and cables through the cable guide.

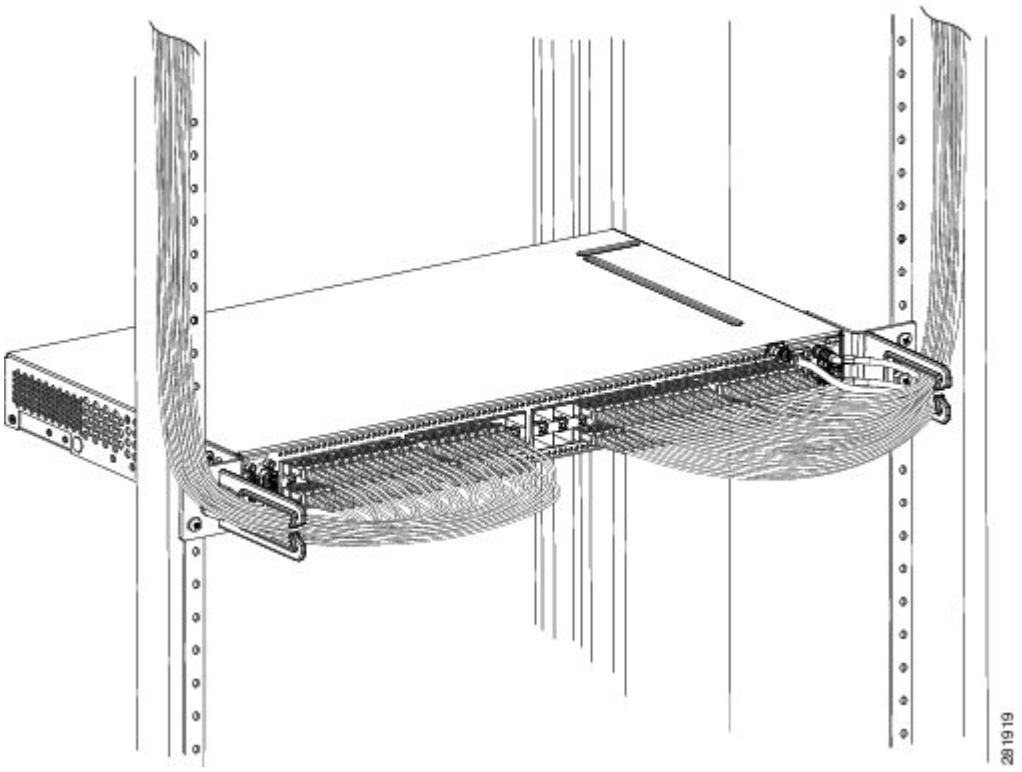
The cables are routed through the cable guide in an ANSI (23-inch) rack configuration, as shown in this figure.

Figure 43: Cable Management in an ANSI Rack Configuration



The cables are routed through the cable guide in an ETSI rack configuration, as shown in this figure.

Figure 44: Cable Management in an ETSI Rack Configuration



Note If no cable guide is installed, bind the cables and fibers using the tie-wrap.

NTP-J60 Clean Fiber Connectors

Purpose	This procedure explains how to clean the fiber connectors.
Tools/Equipment	• Type A Fiber-Optic Connector Cleaner (CLETOP reel) • Inspection microscope • Optical swab • Optical receiver cleaning stick
Prerequisite Procedures	None

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

Procedure

Step 1 Using an inspection microscope, inspect each fiber connector for dirt, cracks, or scratches.

Step 2 Replace any damaged fiber connectors.

Note Replace all dust caps whenever the equipment is unused for 30 minutes or more.

Step 3 Complete the DLP-J186 Clean Fiber Connectors with CLETOP, on page 119 as necessary.

Step 4 Complete the DLP-J187 Clean the Fiber Adapters, on page 120 as necessary.

Step 5 Stop. You have completed this procedure.

DLP-J186 Clean Fiber Connectors with CLETOP

Purpose	This task explains how to clean the fiber connectors with CLETOP.
Tools/Equipment	• Type A Fiber-Optic Connector Cleaner (CLETOP reel) • Optical receiver cleaning stick
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Procedure

Step 1 Remove the dust cap from the fiber connector.

Step 2 Press the lever up to open the shutter door. Each time you press the lever, you expose a clean wiping surface.

Step 3 Insert the connector into the CLETOP cleaning cassette slot, rotate one quarter turn, and gently swipe downwards.

Step 4 Use an inspection microscope to inspect each fiber connector for dirt, cracks, or scratches. If the connector is not clean, repeat Step 1 to Step 3.

Step 5 Insert the fiber connector into the applicable adapter or attach a dust cap to the fiber connector.

Step 6 Return to your originating procedure (NTP).

DLP-J187 Clean the Fiber Adapters

Purpose	This task explains how to clean the fiber adapters.
Tools/Equipment	CLETOP stick swab
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Procedure

Step 1 Remove the dust plug from the fiber adapter.

Step 2 Insert a CLETOP stick swab (14100400) into the adapter opening and rotate the swab.

Step 3 Place dust plugs on the fiber adapters when not in use.

Step 4 Return to your originating procedure (NTP).

NTP-J61 Perform the CPT 50 Shelf Installation Acceptance Test

Purpose	This procedure describes how to perform a shelf installation acceptance test for the CPT 50 shelf.
Tools/Equipment	Voltmeter
Prerequisite Procedures	Applicable procedures in this chapter

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

Procedure

Step 1 If you installed a CPT 50 shelf, verify that each applicable procedure listed in the below table was completed.

Table 7: CPT 50 Shelf Installation Task Summary

Description	Completed
NTP-J53 Unpack and Inspect the CPT 50 Shelf, on page 65	
NTP-J54 Install the CPT 50 Shelf, on page 71	
Connect the chassis to the office ground. For detailed instructions on how to ground the chassis, see the *Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms*.	
NTP-J57 Install the Power Feeds and Ground to the CPT 50 Shelf, on page 95	
NTP-J58 Connecting Cables to the EOBC, Timing, and Console Ports, on page 111	
NTP-J59 Install and Route Fiber-Optic Cables, on page 115	

Step 2 DLP-J188 Inspect the CPT 50 Shelf Installation and Connections , on page 121.

Step 3 DLP-J189 Measure DC Voltage on the CPT 50 shelf, on page 122.

Step 4 Continue with NTP-J21 Set Up the Computer for CTC, on page 11 and NTP-J22 Log into CTC, on page 15.

Stop. You have completed this procedure.

DLP-J188 Inspect the CPT 50 Shelf Installation and Connections

Purpose	This task describes how to inspect the shelf installation and connections and verify that everything is installed and connected properly.
Tools/Equipment	None

Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Procedure

Step 1 Make sure that all external wiring connections (that is, power, ground, alarms, and so on) are secure. If a wire or cable is loose, return to the appropriate procedure in this chapter to correct it.

Step 2 Return to your originating procedure (NTP).

DLP-J189 Measure DC Voltage on the CPT 50 shelf

Purpose	This task describes how to measure the power to verify correct power and returns.
Tools/Equipment	Voltmeter
Prerequisite Procedures	Before installing the DC power, check the voltage
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning To reduce the risk of electric shock, switch on the power only after the power cord is completely installed into the power module. Statement 390

Caution Do not apply power to the shelf assembly until you complete all the installation steps.

Procedure

Step 1 Using a voltmeter, verify the office ground and power:

a) Place the black lead (positive) on the return (RET). Hold it there while completing Step b.

b) Place the red lead (negative) on the fuse power points on the third-party power distribution panel to verify that they read between:

- –40.5 VDC and –57.6 VDC (power) and 0 (return ground) for a 48 V power source.
- –20 VDC and –28.3 VDC (power) and 0 (return ground) for a 24 V power source

Step 2 Using a voltmeter, verify the shelf ground and power wiring:
Place the black lead (positive) on the RET1(A) and the red lead on the -48 V (A) or -24 V (A) point.

- For the CPT 50 shelf with 48 V power supply, verify a reading between –40.5 VDC and –57.6 VDC.
- For the CPT 50 shelf with 24 V power supply, verify a reading between –20 VDC and –28.3 VDC.

If there is no voltage, check the following and correct if necessary:

- Battery and ground are reversed to the shelf.
- Battery is open or missing.
- Return is open or missing.

Step 3 Repeat Step 1 and Step 2 for the RET2 (B) and -48 V (B) or -24 V (B) of the redundant power supply input.

Step 4 Return to your originating procedure (NTP).

Hardware Specifications

This chapter contains product names and hardware specifications for CPT 50 shelf, fabric card, and line card.

Product Names

The product names for the CPT 50 shelf, fabric, and line cards are listed in this table.

Card / Shelf	Product Name
Fabric Card	CPT-PTF256-10GX4=
Line Card	CPT-PTM-10GX4=
CPT 50 Shelf with 48 V AC power module	CPT-50-44GE-AC=
CPT 50 Shelf with 48 V DC power module for ANSI standard	CPT-50-44GE-48A
CPT 50 Shelf with 48 V DC power module for ETSI standard	CPT-50-44GE-48E=
CPT 50 Shelf with 24 DC power module for ANSI standard	CPT-50-44GE-24A=

Caution In order to ensure system reliability, the CPT 600 or CPT 200 shelf must have all their slots equipped with either cards or fillers.

Note The fabric and line cards are inserted in a CPT 600 or CPT 200 shelf. The line card filler (15454-M-FILLER) must be installed in unused and empty slots to ensure proper air flow and electromagnetic interference (EMI) requirements during the CPT 200 or CPT 600 operation. In the CPT 200 shelf, the line card filler can be installed in Slot 2 and Slot 3. In the CPT 600 shelf, the line card filler can be installed in slots 2, 3, 4, 5, 6, and 7. The line card fillers have no card-level LED indicators. CTC does not detect filler cards. This support may be added in later releases.

CPT Specifications

This section provides the specifications for timing, power, and environmental specifications, card and shelf dimensions.

GPS (Global Positioning System) Interface (1PPS and 10Mhz) of CPT 50 Shelf

	10 MHz Specification	1 PPS Specification
Waveform	Sine wave	Pulse
Frequency	10 MHz	1 PPS
Amplitude	>1 V LVTTL Compatible	>1 V LVTTL Compatible
Impedance	50 Ω	50 Ω

TOD/1PPS RS422 Interface— RJ45 Pinout of CPT 50

The pinout of the TOD (Time of Day) RJ45 port is listed in this table.

Pin	Signal Name	Description
1	1PPS_N	1PPS RS422 output signal
2	1PPS_P	1PPS RS422 output signal
3	NC	No Connect
4	GND	—
5	GND	—
6	NC	No Connect
7	TOD_P	Time of Day RS422 output
8	TOD_N	Time of Day RS422 output

System Power for CPT 50 Shelf

The power specifications for the CPT 50 shelf is listed in this table.

Shelf	Input Voltage	Power Consumption	Power Terminals	Fuse Rating
CPT 50 shelf with AC power module for ANSI and ETSI standards	100V - 240V AC depending on the standards in various countries	100 VAC 2.4 A ; 240 VAC 1A	One AC single phase with 3-pole (line L, Neutral N, and Protective Earth PE) input connector.	Must not exceed 10 A or 15 A, depending on the standards in various countries.
CPT 50 shelf with 48 V DC power module for ANSI standard	Voltages –40.5 VDC and –57.6 VDC are, respectively, the minimum and maximum voltages required to power the chassis. The nominal steady state voltage is -48 VDC. Functionality is guaranteed at -40 VDC input voltage, according to GR-1089.	48 V DC 5 A	Single terminal block with four poles— –48V, RET for power terminals A and B.	Must not exceed 10 A
CPT 50 shelf with 48 V DC power module for ETSI standard	Voltages –40.5 VDC and –57.6 VDC are, respectively, the minimum and maximum voltages required to power the chassis. The nominal steady state voltage is -48 VDC.	48 VDC 5 A	DSUB 2 poles	Must not exceed 10 A
CPT 50 shelf with 24 V DC power module for ANSI standard	Voltages –20 VDC and –28.3 VDC are, respectively, the minimum and maximum voltages required to power the chassis. The nominal steady state voltage is -24 VDC.	24VDC 10 A	Single terminal block with four poles— –24V, RET for power terminals A and B.	Must not exceed 15 A.

Fan Tray

The following table lists power requirements for the fan-tray assembly.

Table 8: Fan-Tray Power Requirements

Fan Tray	Watts	Amps
12 V supplied by CPT 50 shelf	36	3

Fabric Card and Line Card Power Specifications

This section provides power specifications for fabric and line cards.

Card	Maximum Power in Watts	Typical Power in Watts	Amperes at -48 V (Maximum)
Fabric Card	200	150	4.1
Line Card	150	100	2.1

CPT 50 Shelf, Fabric, and Line Card Dimensions

Card / Shelf	Physical Dimensions							
	Measurement in inches				Measurement in mm			
	Height	Width	Depth	Weight in Kg	Height	Width	Depth	Weight in Kg
Fabric and Line Card (Single Slot)	12.650	0.921	9.000	• Fabric—1.2 • Line—1.04	321.3	23.4	228.6	• Fabric—1.22 • Line—1.04

Card / Shelf	Physical Dimensions							
	Measurement in inches				Measurement in mm			
CPT 50 Shelf	1.7	• 19 or 23 inches with mounting ears attached for ANSI rack configuration • 21 inches with mounting ears attached for ETSI rack configuration	9.1	• CPT with AC power module— 4.06 kg • CPT with DC power module— 4.22 kg	43.1	• 482.6 or 584.2 with mounting ears attached for ANSI rack configuration • 533.4 mm with mounting ears attached for ETSI rack configuration	231.1	• CPT with AC power module— 4.06 kg • CPT with DC power module— 4.22 kg

CPT 50 Shelf, Fabric, and Line Card Environmental Specifications

The operating temperature and humidity for CPT 50 shelf, fabric, and line cards are as follows:

- Operating Temperature— 32 to 131 degrees Fahrenheit, 0 to +55 degrees Celsius)
- Operating Humidity— 5 to 85%, noncondensing; functionality is guaranteed up to 5 to 95%, noncondensing.

Other Specifications

Card / Shelf	Interface	Switching Capacity
Fabric Card	• Two 10GE XFP ports (OTN enabled) • Two 10GE SFP+ ports • Mini USB port (local craft access RS232 for CTC software	256 G

Card / Shelf	Interface	Switching Capacity
Line Card	• Four 10GE SFP+ ports • Mini USB port (local craft access RS232 for CTC software	40 G
CPT 50 Shelf	• 44 GE 10/100/1000Mbps SFP ports • Four 10GE SFP+ ports	44 G

SFP, SFP+, and XFP Modules

SFP, SFP+, and 10-Gbps SFP (XFP) modules are integrated fiber optic transceivers that provide high-speed serial links from a port or slot to the network. For more information on SFP/SFP+/XFP modules and for a list of SFP/SFP+/XFP modules supported by the CPT, see Installing the SFP, SFP+, and XFP Modules in Cisco CPT. In CTC, SFP, SFP+, and XFP modules are called pluggable port modules (PPMs).

DLP-J339 Provision TDM SFP using CTC

Below section explains provisioning of TDM SFP using CTC.

Procedure

Step 1 Complete theNTP-J22 Log into CTC, on page 15procedure at a node on the network where you want to provision TDM SFP.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**.

Step 4 Double-click a CPT50 panel.

Step 5 In **Ports** tab, set the interface to admin down (OOS) state.

Step 6 In **Ethernet** tab, set the appropriate Media type and click **Apply** button.

Step 7 In **PDH Ethernet Parameters** tab, provide MPLS Inner Label and MPLS Outer Label. Double click on selected port to edit parameters and click **Apply** button.

- Once service is provisioned, TDM SFP on the given interface cannot be provisioned or it's labels cannot be set to default value.
- In case of VPWS circuit , default labels will be allocated by CTC and it is not recommended to change the labels assigned.
- In case of Carrier Ethernet Circuit User MUST manually set inner and outer label as 16 at both end points
- Before removing TDM SFP physically, it is recommended to un-provision TDM SFP from CTC. Assigned labels will be not deallocated if not un-provisioned.

Step 8 In **Electrical Lines** tab, select appropriate frame type (i.e. E1 , E3 , T1 or T3) and set their line type & clock. Click **Apply** button.
Below are the framing recommendations:

Media Type	Encapsulation	
	SAToP	**CESoPSN**
T1	Unframed	Framed.ESF,D4
E1	Unframed	Framed
T3	Framed(M23,C-bit),Unframed	Not supported
E3	Framed(G.832,G.751),unframed	Not supported

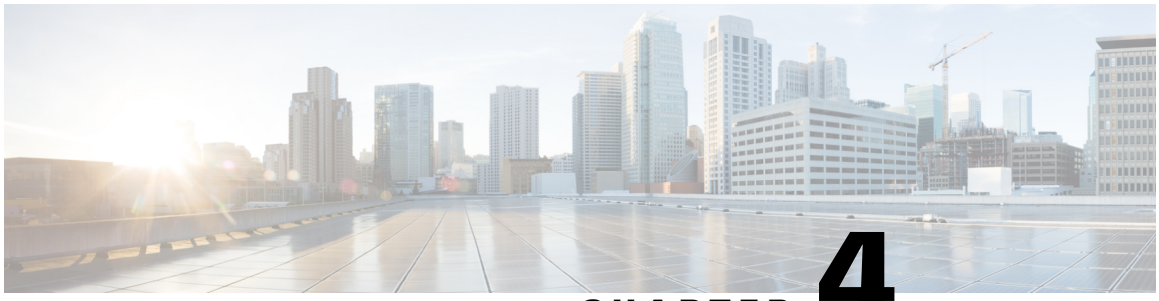
Below are the timing recommendations:

Tester A	MiTOP A		MiTOP B	Tester B
INT	LBT	-->	ADP	LBT
LBT	INT	-->	ADP	LBT
INT	ADP	-->	ADP	INT
LBT	Sync -E	-->	Sync-E	LBT

Step 9 In **Ports** tab, set the interface to admin up (IS) state.

Step 10 Wait for couple of minutes since programming into TDM pluggable will take time.

Step 11 Return to your originating procedure (NTP).
test ppmAgent tdmdump tdmDumpData <ppmId : (interface number -1)> is debug command that can be executed on CPT50 to check TDM configurations. It will display labels allocated for TDM SFP.



CHAPTER 4

Configuring Ethernet Virtual Circuit

This chapter describes Ethernet Virtual Circuit (EVC), EVC types, Ethernet Flow Point (EFP), and bridge domain. This chapter also describes procedures to configure EVC.

This chapter includes the following topics:

Understanding Carrier Ethernet

The Carrier Ethernet uses a high bandwidth Ethernet technology to deliver dedicated connectivity. It provides network connectivity by connecting to the customer site through a private Layer 2 Ethernet circuit. The available interfaces are normally 10Mbps and 100Mbps Fast Ethernet and 1000Mb/s Gigabit Ethernet.

The Carrier Ethernet enables you to run different services over a single connection. Next Generation Networks, VoIP, Storage, and Managed Security are some of the services that can run over a single Carrier Ethernet connection.

The Metro Ethernet Forum (MEF) defines the following five attributes to define an Ethernet as Carrier class:

- Standardized Services
- Quality of Service
- Scalability
- Service Management
- Reliability

Carrier Ethernet can be deployed in many ways:

- Ethernet over SDH/SONET
- Ethernet over MPLS
- Native Ethernet

Note Carrier Packet Transport (CPT) system does not support Ethernet over SDH/SONET.

Understanding Ethernet Virtual Circuit

The Ethernet Virtual Circuit (EVC) represents a logical relationship between Ethernet User–Network interfaces (UNI) in a provider–based Ethernet service. The EVC represents the service offered and is carried through the provider network. Each EVC is configured by its unique name across the provider network.

An EVC is an end–to–end representation of a single instance of a Layer 2 service that a service provider offers. It embodies the different parameters based on which the service is offered. EVC prevents data transfer between sites that are not part of the same EVC.

In simple terms, EVC is the A–Z circuit that enables you to pass customer VLANs from one port on a node to another port on another node in the network. EVC represents a Carrier Ethernet Service and is an entity that provides end–to–end connection between two or more customer end points.

EVC Attributes

Some of the global EVC attributes are:

- EVC ID—An unique identifier that identifies the EVC

- EVC Type—E-LINE, E-LAN, or E-TREE
- List of associated EFPs that belong to an EVC

Understanding Ethernet Flow Point

The traffic for the service needs to pass through several switches in the provider network to connect customer sites across the provider network. The instance of a specific EVC service on the physical interface of each network device through which the EVC passes through is called an Ethernet Flow Point (EFP). An EFP is a logical demarcation point of an EVC on an interface. An EFP can be associated with a bridge domain.

In simple terms, an EFP is defined as an end point of an EVC within a node. Because multiple EVCs can pass through one physical interface, the main purpose of an EFP configuration is to recognize the traffic belonging to a specific EVC on that interface and to apply the forwarding behavior and features specific to that EVC.

The possible EFP administrative states are UP and DOWN. This administrative state maps to the EFP administrative state in IOS.

EFP Attributes

The key attributes of an EFP are:

- Encapsulation string—Defines the classification criteria for an incoming packet.
- Forwarding operations—Defines the forwarding operation to be applied on frames that belong to this EFP.
- Ingress rewrite operation—Defines the rewrites to be performed on the frames that belong to this EFP before proceeding with the forwarding operations.

Note supports only the Ingress rewrite operation and all the rewrite operations are symmetric in nature.

Understanding Bridge Domain

The bridge domain is an Ethernet broadcast domain internal to the device. The bridge domain enables you to decouple the VLAN from the broadcast domain. The bridge domain has one to many mapping with EFPs.

All the EFPs in a node for a specific EVC are grouped using the bridge domain. If EFPs belong to the same bridge domain and have the same bridge domain number, the EFPs receive traffic even if they have different VLAN numbers.

The bridge domain number is local to the node. Different nodes that are part of an EVC can have the same or different bridge domain number. However, the bridge domain number is unique for an EVC within a node.

For EVC, the bridge domain number is from 1 to 16384.

Configuration Constraint

The encapsulation and rewrite operations are not allowed if the bridge domain is configured on the EFP. Remove the existing bridge domain from the EFP and then change the encapsulation and rewrite operations.

Types of Bridge Domains

The bridge domain can be configured to operate in point–to–point and point–to–multipoint modes. The default configuration mode of the bridge domain is point–to–multipoint.

The types of bridge domains supported are:

Bridge Domain Type	Description
Point–to–point	This bridge domain can be used for Ethernet Private Line (EPL) and Ethernet Virtual Private Line (EVPL). CPT supports up to 16384 point–to–point bridge domains. MAC learning is not supported for point–to–point bridge domains. REP does not block EFPs that are in point–to–point bridge domain. In a ring scenario, the point–to–multipoint bridge domain is needed.
Point–to–multipoint	This bridge domain can be used for Ethernet Private LAN (EPLAN) and Ethernet Virtual Private LAN (EVPLAN). CPT supports up to 4000 point–to–multipoint bridge domains. MAC learning is supported for point–to–multipoint bridge domains. The point–to–multipoint bridge domain is supported over REP.

EVC Features

EVC in CPT supports the following features:

- Create, delete, or modify EFPs
- Add EFPs as members of a bridge domain
- Map Traffic to EFPs based on:
  - 802.1q VLANS (Single VLAN, list, range)
  - Cisco Q-in-Q VLANS (Single outer and single inner VLAN)
  - Proprietary Q-in-Q VLANS (9100, 9200)
  - 802.1ad Provider Bridges (encapsulation and rewrite)
- Map VLAN—Push, Pop, Translate Single VLAN tag
- Support for rewriting single or double VLAN tags
- Support for grouping VLANs from several UNI to a single EVC
- Support for Ethernet UNI with dual VLAN tag (Cisco-QinQ or IEEE 802.1ad)
- Support for 802.1Q VLAN ID translation on the 802.1q tagged traffic on the UNI
- Support for point–to–point EVC, multipoint–to–multipoint EVC, and rooted multipoint EVC
- Support for Ethernet over MPLS

- Support for 1:2 VLAN translation and 2:2 VLAN translation
- EVC MAC address aging
- Flex Service Mapping (Advanced VLAN translations).
  - Support for dot1ad and Cisco Q-in-Q etype for S-tag
- Support for Layer 2 Protocol Tunneling (L2PT) for each port

EVC Types

supports the following categories of EVCs:

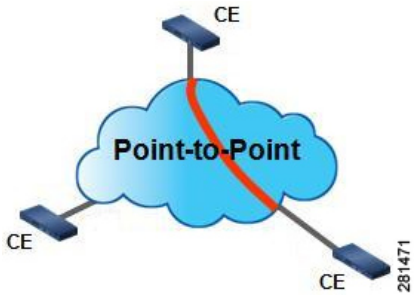
- Point–to–point EVCs (E-LINE services)
- Multipoint–to–multipoint EVCs (E-LAN services)
- Rooted Multipoint EVCs (E-TREE services). CTC handles E-TREE services as a special case of EPLAN/EVPLAN.

CPT supports the following types of EVCs:

Ethernet Private Line

An Ethernet Private Line (EPL) is a point–to–point EVC. EPL is an EVC that supports communication between two UNIs. In EPL, only one EVC can exist on a port and the port can have only one EFP. See Figure 45: Ethernet Private Line, on page 135.

Figure 45: Ethernet Private Line

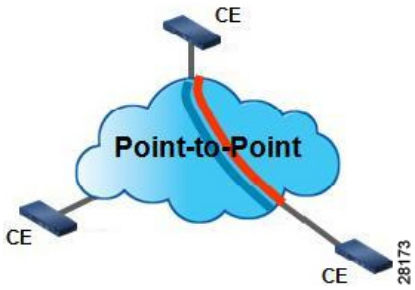


Ethernet Virtual Private Line

An Ethernet Virtual Private Line (EVPL) is a point–to–point EVC. EVPL is an EVC that supports communication between two UNIs. In EVPL, multiple EVCs can exist on a port and the port can have multiple

EFPs. Each EFP is associated with a different bridge domain. See Figure 46: Ethernet Virtual Private Line, on page 136.

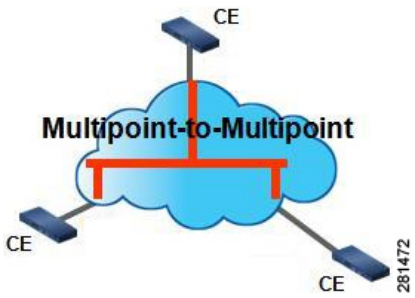
Figure 46: Ethernet Virtual Private Line



Ethernet Private LAN

An Ethernet Private LAN (EPLAN) is a multipoint–to–multipoint EVC. EPLAN is an EVC that supports communication between two or more UNIs. In EPLAN, only one EVC can exist on a port and the port can have only one EFP. See Figure 47: Ethernet Private LAN, on page 136.

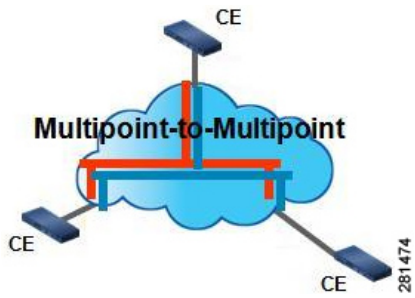
Figure 47: Ethernet Private LAN



Ethernet Virtual Private LAN

An Ethernet Virtual Private LAN (EVPLAN) is a multipoint–to–multipoint EVC. EVPLAN is an EVC that supports communication between two or more UNIs. In EVPLAN, multiple EVCs can exist on a port and the port can have multiple EFPs. Each EFP is associated with a different bridge domain. See Figure 48: Ethernet Virtual Private LAN, on page 136.

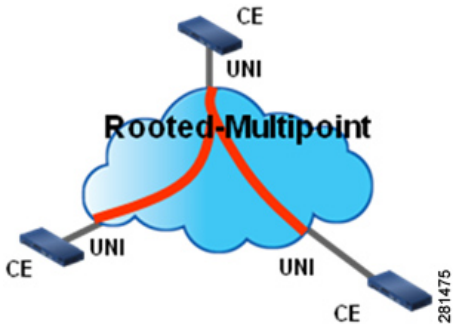
Figure 48: Ethernet Virtual Private LAN



Rooted Multipoint EVC

A rooted Multipoint EVC is a multipoint–to–multipoint EVC. In this EVC, the split horizon is configured on the access side EFPs. Figure 49: Rooted Multipoint EVC, on page 137 shows a rooted multipoint EVC with a split horizon configured between the two UNIs.

Figure 49: Rooted Multipoint EVC



CTC handles E-TREE services as a special case of EPLAN or EVPLAN.

Split Horizon

The rooted multipoint EVC supports split horizon. A split horizon is a subset of the members of a bridge domain.

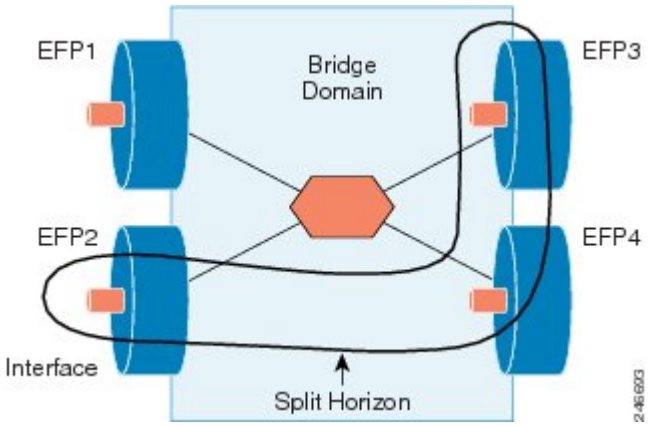
The split horizon can be enabled for the service instances that are members of the multipoint bridge domain. This disables traffic among all the members of the bridge domain where split horizon is configured.

Note does not support split horizon groups.

Figure 50: Bridge Domain with Four EFPs, on page 138 shows an example of a multipoint bridge domain with four EFPs. The split horizon is configured on the three EFPs (EFP2, EFP3, and EFP4). The traffic is disabled among these three EFPs. Therefore, these three EFPs can only pass traffic to EFP1 and receive traffic from EFP1.

If the split horizon is configured on a Link Aggregation Group (LAG), the configurations apply to the entire LAG and not to the individual member ports.

Figure 50: Bridge Domain with Four EFPs



Counters

The following counters are supported for EFPs:

- Ingress packet counts
- Egress packet counts
- Ingress bytes
- Egress bytes

For point–to–multipoint bridge domains, all the counters are enabled by default. For point–to–point bridge domains, the ingress counters are enabled by default and the egress counters are disabled by default.

Note The hardware resources for point–to–point EFPs and point–to–multipoint EFPs are shared across Multiprotocol Label Switching (MPLS) and Quality of Service (Qos) and therefore, scalability of these counters for these EFPs are subject to availability of resources. A single 64-bit counter cannot be split among two byte counters or two packets counters.

Note The egress statistics for point–to–point EFPs is collected using a shared hardware resource. You can enable the egress statistics collection for each point–to– point EFP using the **evc-enable-stats** command.

EVC and EFP Limitations and Restrictions in CPT

These limitations and restrictions apply to EVC and EFP in CPT:

- The EFP point–to–point service does not support MAC learning and rewrite egress operations. It supports only the symmetric rewrite operation.
- The EFP multipoint–to–multipoint service supports the rewrite ingress option with the symmetric option. It does not support the rewrite egress operation.
- Different EFPs cannot have encapsulation for the same VLAN ID on a single interface. For example, dot1q 10 and dot1q 1-20 are not supported on a single interface because both include the same VLAN 10.
- Two different Ethernet types are not supported on a single interface. For example, encapsulations dot1q and dot1ad are not supported on the same interface.
- Rewrite Push 1 tag operation is not supported for encapsulations with double tag.
- Rewrite Push 2 tag operation is not supported for encapsulations with single or double tag.
- Translate rewrite operations are not supported for encapsulations such as untagged, any, default, and encapsulations involving VLAN range and list.
- If encapsulation default is configured on an EFP, no other encapsulation match on a EFP can be configured.
- Two EFPs on the same bridge domain and on the same interface is not supported.
- Encapsulation range limits—only up to 4 ranges are allowed for each EFP and only up to 8 VLAN ranges are allowed for each port.
- The point–to–point traffic flow is limited to 99% because of the 4 byte overhead that is added to the frames carrying point–to–point traffic.
- To create an EVC on the CPT 50 in a ring, the source and the destination of the EVC can be provisioned only on that CPT 50.
- Only Ethernet Private LAN (EPLAN) and Ethernet Virtual Private LAN (EVPLAN) EVCs are supported for a ring.

Configuration Procedures

The following procedures can be performed using Cisco IOS commands to configure EVC and Layer 2 protocol tunneling:

- DLP-J216 Configure a Bridge Domain Using Cisco IOS Commands, on page 140
- DLP-J1 Configure an Ethernet Service Instance Using Cisco IOS Commands, on page 141
- DLP-J212 Configure Layer 2 Protocol Tunneling Using Cisco IOS Commands, on page 155

The following procedures can be performed using CTC to configure EVC and Layer 2 protocol tunneling:

- DLP-J2 Create an EVC Circuit Using CTC, on page 143
- DLP-J3 Edit an EVC Circuit Using CTC, on page 147
- DLP-J4 Query an EVC Circuit Using CTC, on page 151
- DLP-J213 Configure Layer 2 Protocol Tunneling Using CTC, on page 156

NTP-J1 Configure an EVC Circuit

Purpose	This procedure configures an EVC circuit.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J216 Configure a Bridge Domain Using Cisco IOS Commands, on page 140
- DLP-J1 Configure an Ethernet Service Instance Using Cisco IOS Commands, on page 141
- DLP-J2 Create an EVC Circuit Using CTC, on page 143
- DLP-J3 Edit an EVC Circuit Using CTC, on page 147
- DLP-J4 Query an EVC Circuit Using CTC, on page 151
- DLP-J212 Configure Layer 2 Protocol Tunneling Using Cisco IOS Commands, on page 155
- DLP-J213 Configure Layer 2 Protocol Tunneling Using CTC, on page 156

Stop. You have completed this procedure.

DLP-J216 Configure a Bridge Domain Using Cisco IOS Commands

Purpose	This procedure configures a bridge domain using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**bridge-domain** *bridge-id* [**split-horizon**] **Example:** Router(config)# bridge-domain 12	Creates a bridge domain where *bridge-id* is the identifier for the bridge domain instance.
Step 4	**mode p2p** **Example:** Router(config)# mode p2p	Configures the p2p (point–to–point) bridge domain. The default mode of the bridge domain is p2mp (point–to–multipoint).
Step 5	**no mode p2p** **Example:** Router(config)# no mode p2p	Configures the point–to–multipoint bridge domain.
Step 6	**exit** **Example:** Router(config)# exit	Exits global configuration mode.
Step 7	Return to your originating procedure (NTP). **Example:** —	

DLP-J1 Configure an Ethernet Service Instance Using Cisco IOS Commands

Purpose	This procedure configures an Ethernet service instance using Cisco IOS commands.
Tools/Equipment	None

Prerequisite Procedures	DLP-J216 Configure a Bridge Domain Using Cisco IOS Commands, on page 140
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Perform these steps to configure an EVC service instance under the point–to–multipoint bridge domain. To configure an EVC service instance under the point–to–point bridge domain, perform the DLP-J216 Configure a Bridge Domain Using Cisco IOS Commands, on page 140 procedure first and then perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**service instance** *id* **ethernet** [*evc-id*] **Example:** Router(config-if)# service instance 101 ethernet	Configures an Ethernet service instance on an interface and enters service instance configuration mode.
Step 5	**encapsulation dot1q** {*any* | *vlan-id* [*vlan-id* [*-vlan-id*]]} **second-dot1q** {*any* | *vlan-id* [*vlan-id* [*-vlan-id*]]} **Example:** Router(config-if-srv)# encapsulation dot1q 100 second dot1q 200	Defines the matching criteria that maps the ingress dot1q, QinQ, or untagged frames on an interface to the appropriate service instance.
Step 6	**rewrite ingress tag** {**push** {**dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **pop** {**1** | **2**} | **translate** {**1-to-1** {**dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **2-to-1 dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **1-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **2-to-2**	Specifies the rewrite operation to be applied on the frame ingress to the service instance.

	Command or Action	Purpose
	{**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*}} {**symmetric**} **Example:** Router(config-if-srv)# rewrite ingress tag push dot1q 20	
Step 7	**bridge-domain** *bridge-id* [**split-horizon**] **Example:** Router(config-if-srv)# bridge-domain 12	Binds the Ethernet service instance to a bridge domain instance where *bridge-id* is the identifier for the bridge domain instance.
Step 8	**exit** **Example:** Router(config-if-srv)# exit	Exits the service instance configuration mode.
Step 9	Return to your originating procedure (NTP). **Example:** —	

Configure an Ethernet Service Instance

The following example shows how to configure an Ethernet service instance using Cisco IOS commands.

```
Router> enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# service instance 101 ethernet
Router(config-if-srv)# encapsulation  dot1q 100
Router(config-if-srv)# rewrite ingress tag push dot1q 20 symmetric
Router(config-if-srv)# bridge-domain 12
Router(config-if-srv)# exit
```

DLP-J2 Create an EVC Circuit Using CTC

Purpose	This procedure creates an EVC circuit using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The layer 2 services on CPT can be created on top of layer 2 PPCs or OCHTrails.

CPT supports Client/Trunk to Client/Trunk (layer 2) PPC for topology discovery and layer 2 service routing. If CPT is used in the GNE-ENE mode of configuration, then generic communications channels (GCC) can be used for topology discovery and layer 2 PPCs for layer 2 service routing. Both layer 2 PPC and GCC can be created between the same set of ports. However, this is not mandatory.

CPT also supports OCH Trunk to OCH Filter PPCs to connect CPT to MSTP nodes. If you want to route the traffic from a non co-located CPT node to a DWDM network, use OCH Trunk to OCH Filter PPCs to connect CPT and MSTP nodes. The OCHTrail can be created on top of this and the layer 2 services can be created on top of OCHTrails.

To provision EVC on TDM interface, edit the TDM labels to the default value.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to create an EVC circuit.

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

Step 3 Click the **Layer2+** tab.

Step 4 Click **Carrier Ethernet**.

Step 5 Click **Create**. The Circuit Creation wizard appears.

Step 6 In the Circuit Attributes screen of the wizard:

a) Enter the name of the service that you want to provision in the Name field.
When a name is not specified, CTC automatically creates a name with a random number at the end.

b) Enter the description of the service in the Description field.

c) From the EVC Type drop-down list, choose the service type that you want to provision.
The supported EVC types are:

- Ethernet Private Line
- Ethernet Virtual Private Line
- Ethernet Private LAN
- Ethernet Virtual Private LAN

d) From the EFP State drop-down list, choose UP or DOWN. The default value is UP. This EFP state maps to the EFP admin state in IOS.

e) Specify the bandwidth of the EVC in Kbps, Mbps, or Gbps and click **Next**.

Step 7 In the Source screen of the wizard:

a) From the Node drop-down list, choose the source node where you want to provision the EVC. The EFP A section appears. The Shelf field displays the shelf automatically assigned to the EVC.

b) To choose a CPT 50 in a ring, to serve as the source EFP, complete the following:

1 Check the check box adjacent to the Ring drop-down list. The Ring drop-down list gets enabled.

Note This check box is enabled only if the service state of the ring is enabled.

2 From the Ring drop–down list, choose a ring.

c) To choose a port, complete the following:

1 From the Slot drop-down list, choose a slot.

2 From the Port drop-down list, choose a port to serve as the source EFP.

d) If you want to choose a channel group to serve as the source EFP:

1 Check the **CHGRP as EFP** check box.

2 From the CHGRP drop-down list, choose a channel group to serve as the source EFP.

3 Click **Manual Load Balancing** to configure manual load balancing on the ports of the channel group. The Manual Load Balancing dialog box appears.

4 From the Primary Loadbalanced Link list, choose a port.

5 Click **Apply**.

e) Click **Next**.

Step 8 In the Destination screen of the wizard:

a) From the Node drop-down list, choose the destination node that you want to provision the EVC. The EFP Z section appears.

b) If you want to choose a port to serve as the destination EFP, complete the following:

1 From the Slot drop-down list, choose a slot.

2 From the Port drop-down list, choose a port to serve as the destination EFP.

c) If you want to choose a channel group to serve as the destination EFP:

1 Check the **CHGRP as EFP** check box.

2 From the CHGRP drop-down list, choose a channel group to serve as the destination EFP.

3 Click **Manual Load Balancing** to configure manual load balancing on the ports of the channel group. The Manual Load Balancing dialog appears.

4 From the Primary Loadbalanced Link list, choose a port.

5 Click **Apply**.

d) Click **Next**.

Step 9 In the EVC Circuit Routing Preview screen of the wizard, CTC displays the shortest route of the EVC circuit. You can specify the nodes that need to be included or excluded in the EVC circuit.

a) Click the **Constraints** tab.

b) Choose the nodes appropriately and click **Include** or **Exclude**.

c) Click **Apply** to apply the constraints.

d) Click **Next**.

Step 10 In the EFP Configuration Preview screen of the wizard, specify the VLAN configuration for EFPs.

a) Select an EFP in the EVC path.
The node and ports are populated in the EFP Selection area.

b) In the Outer VLAN Configuration area, choose the type of VLAN tagging:

- Double Tagged
- Single Tagged
- Untagged
- Default
- Any

Note The VLAN tagging type chosen for Ethernet Private Line and Ethernet Private LAN is Default. Do not change this option for the source EFP.

c) From the TPID drop-down list, choose a TPID—dot1q, dot1ad, 0x9100, or 0x9200.
d) Enter a VLAN tag in the VLAN Tag field. For example, enter 10,20,30-50 without white spaces in the VLAN Tag field.
e) Check the **exact** check box to specify the exact encapsulation value.
f) In the Inner VLAN Configuration area, enter the VLAN tag. You cannot enter VLAN range for inner VLANs. The TPID is dot1q and cannot be changed.
g) In the Rewrite Ingress Operation area, choose the rewrite operation:

- PUSH 1
- PUSH 2
- POP 1
- POP 2
- TRANSLATE 1-to-1
- TRANSLATE 1-to-2
- TRANSLATE 2-to-1
- TRANSLATE 2-to-2

h) From the Outer VLAN TPID drop-down list, choose a TPID—dot1q, dot1ad, 0x9100, or 0x9200.
i) Enter the outer VLAN tag in the Outer VLAN Tag field.
j) Enter the inner VLAN tag in the Inner VLAN Tag field. The Inner VLAN TPID is dot1q and cannot be changed.
k) (Only for Ethernet Private LAN and Ethernet Virtual Private LAN EVC types) In the Split Horizon area, check the **Enable Split Horizon** check box to enable the split horizon for the EFPs.
l) In the Enable Statistics area, check **Ingress** or **Egress** as appropriate.
m) Click **Save** to apply this configuration to the selected EFP.
n) To create a configuration for another EFP, select the node from the map and select the EFP from the Available Ports drop-down list.
If you have selected the Ethernet Private Line or Ethernet Virtual Private Line as the EVC type in the Circuit Attributes screen, you can configure only two EFPs, namely EFP A and EFP Z. If you have selected Ethernet Private LAN and Ethernet Virtual Private LAN in the Circuit Attributes screen, you can configure more than two EFPs.

You cannot configure same VLAN ID for different services.

o) Click **Apply to All** to derive the EFP configuration on all the intermediate EFPs in the EVC path from the source UNI and NNI EFP configuration.
The source node UNI and NNI EFP configuration that is specified are copied to the destination node UNI and NNI respectively. You can choose to copy the source node NNI configuration without rewrite to all the other EFPs. If the EVC has only one node, the **Apply to All** button does not function.

Step 11 Click **Finish** to create a EVC circuit. The created EVC circuit appear in the list of EVC circuits.

Step 12 Return to your originating procedure (NTP).

DLP-J3 Edit an EVC Circuit Using CTC

Purpose	This procedure edits an EVC circuit using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J2 Create an EVC Circuit Using CTC, on page 143
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

This procedure allows you to perform the following:

- Create new end point EFPs for the EVC
- View the configurations of the EFPs
- Specify the QoS policies to apply on individual EFPs
- Specify the IGMP Snooping settings for the bridge domain
- Specify the MAC learning settings for the bridge domain
- Specify the multicast settings for the bridge domain

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to edit an EVC circuit.

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

Step 3 Click the **Layer2+** tab.

Step 4 Click **Carrier Ethernet**.

Step 5 From the list of EVC circuits, select an EVC circuit to edit.

Step 6 Click **Edit**. The Edit Circuit dialog box appears.

Step 7 In the General tab, view the name, service ID, description, EVC type, and bandwidth of the EVC circuit.

Step 8 In the Endpoint EFPs tab, view the EFPs that are part of this EVC. You can create new end points only for Ethernet Private LAN and Ethernet Virtual Private LAN. To create a new end point EFP for this EVC:

a) Click **Create**. The Define New Drop wizard appears.

b) In the New Drop screen of the wizard, choose a node from the Node drop-down list.

c) To choose a port to serve as the EFP:

1. From the Slot drop-down list, choose a slot.
2. From the Port drop-down list, choose a port to serve as the EFP.

d) To choose a channel group to serve as the EFP:

1. Check the **CHGRP as EFP** check box.
2. From the CHGRP drop-down list, choose a channel group to serve as the EFP.
3. Click **Manual Load Balancing** to configure manual load balancing on the ports of the channel group. The Manual Load Balancing dialog box appears.
4. From the Primary Loadbalanced Link list, choose a port.
5. Click **Apply**.

e) Click **Next**.

f) In the EVC Circuit Routing Preview screen of the wizard, CTC displays the route of the EVC circuit. Specify the nodes that need to be included or excluded in the EVC circuit.

g) Click the **Constraints** tab.

h) Choose the nodes appropriately to include or exclude.

i) Click **Apply** to apply the constraints.

j) Click **Next**.

k) In the EFP Configuration Preview screen of the wizard, specify the VLAN configuration for this EFP.

l) Click **Finish** to create a new EFP for this EVC.

Step 9 In the EFP Configuration tab, view the configurations of the EFPs and edit the VLAN configuration for EFPs:

a) From the EFP drop-down list, choose an EFP to view its configuration.

b) From the EFP State drop-down list, choose UP or Down to change the up or down status of the EFP.

c) In the Outer VLAN Configuration area, choose the type of VLAN tagging:

- Double Tagged
- Single Tagged

- Untagged
- Default
- Any

Note The VLAN tagging type chosen for Ethernet Private Line and Ethernet Private LAN is Default. Do not change this option for the source EFP.

d) Enter a VLAN tag in the VLAN Tag field. For example, enter 10,20,30-50 without white spaces in the VLAN Tag field.
e) In the Inner VLAN Configuration area, enter the VLAN tag. You cannot enter VLAN range for inner VLANs. The inner VLAN TPID cannot be changed
f) In the Rewrite Ingress Operation area, choose the rewrite operation:

- PUSH 1
- PUSH 2
- POP 1
- POP 2
- TRANSLATE 1-to-1
- TRANSLATE 1-to-2
- TRANSLATE 2-to-1
- TRANSLATE 2-to-2

g) Enter the outer VLAN tag in the Outer VLAN Tag field. The Outer VLAN TPID cannot be changed.
h) Enter the inner VLAN tag in the Inner VLAN Tag field.
i) Click **Apply** to apply this configuration to the selected EFP
You Cannot edit the VLAN configurations of the EFP for EVC if the following services are present.

- QOS
- Span
- IGMP
- MVR
- CFM
- Y1731

Step 10 In the QoS tab, specify the QoS policies to apply on the individual EFPs:

a) Check the **Enable/Disable Ingress QoS** check box as appropriate.
All the configured ingress QoS policies are populated in the Ingress Policy drop-down list.
b) From the Ingress Policy drop-down list, choose the required policy.
c) Check the **Enable/Disable Egress QoS** check box as appropriate.
All the configured egress QoS policies are populated in the Egress Policy drop-down list.
d) From the Egress Policy drop-down list, choose the required policy.

e) Click **Apply**.

Step 11 (Only for Ethernet Virtual Private LAN EVC type) In the IGMP Snooping tab, specify the settings for the bridge domain.

a) Check the **IGMP Snooping** check box to enable IGMP snooping on this bridge domain.
b) Check the **Immediate Leave** check box. When you enable IGMP immediate leave, IGMP snooping immediately removes a port when it detects an IGMP version 2 leave message on that port.
c) Check the **Report Suppression** check box. When you enable report suppression, the bridge domain forwards only one IGMP report for each multicast query.
d) Check the **IGMP Static Router Port** check box to add a static router to the EFP.
e) Click **Apply**.

Step 12 (Only for Ethernet Private LAN and Ethernet Virtual Private LAN EVC types) In the Mac Learning tab, specify the MAC learning settings for the bridge domain.

a) Check the **MAC Learning** check box to enable MAC learning on this bridge domain. MAC learning is enabled by default for Ethernet Private LAN and Ethernet Virtual Private LAN.
b) Enter the upper limit on the number of MAC addresses that reside in a bridge domain in the Limit field. The maximum MAC address limit on a bridge domain is 128000.
c) Click **Apply**.
d) Click **EFP Static MAC Address Configuration** to enter static MAC addresses for each EFP. The EFP Static MAC Address Configuration dialog box appears.
e) From the EFP drop-down list, choose an EFP.
f) Enter one or more static MAC addresses for this EFP in the MAC Address field. The added MAC addresses appear in the Entered MAC Addresses area.
g) Click **Apply** and close the EFP Static MAC Address Configuration dialog box.
h) Click **Clear MAC Address(es)** to remove a specific MAC addresses from the MAC address table. The Clear MAC Addresses dialog box appears.
i) Select the system where you want to clear the MAC address from.
j) Enter the MAC address in the MAC Address field and click **Add**.
k) Click **Clear** to clear all the MAC addresses in the MAC Addresses to clear area.
l) Click **Clear All** to clear all the MAC addresses learned on the system.
m) Close the Clear MAC Addresses dialog box.
n) Click **Display MAC Address(es)** to display the configured static MAC addresses for each EFP. The Configured EFP Static MAC Addresses dialog box appears.
o) From the EFP drop-down list, choose an EFP.
The MAC addresses configured on the EFP appear in the Configured MAC Addresses area.
p) Close the Configured EFP Static MAC Addresses dialog box.

Step 13 (Only for Ethernet Virtual Private LAN EVC type) In the MVR tab, specify the multicast settings for the bridge domain:

a) Check the **MVR** check box to enable MVR for this bridge domain.
b) Click **Apply**.
c) Click **Multicast IP Address Configuration** to add multicast IP addresses for this bridge domain. The Multicast IP Addresses dialog box appears.
d) Enter one or more multicast IP address in the IP Address field and click **Add**. The added multicast addresses appear in the IP Addresses area.
e) Click **Apply** and close the Multicast IP Addresses dialog box.
f) From the MVR Type drop-down list, choose **None**, **Source** or **Receiver** for each EFP.

g) Click the Source Service ID field and select a MVR enabled service.
h) Check the **Immediate Leave** check box. When you enable immediate leave, MVR immediately removes a port when it detects a leave message on that port.
i) Click **Apply**.

Step 14 Return to your originating procedure (NTP).

DLP-J4 Query an EVC Circuit Using CTC

Purpose	This procedure allows you to discover the EVC services using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J2 Create an EVC Circuit Using CTC, on page 143
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note When the discovered nodes are disconnected, the circuits move to Partial state. When the disconnected nodes become online in CTC, re-query the circuits to move the circuits to Discovered state.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to query for an EVC circuit.
Step 2 From the View menu, choose **Go to Home View**.
Step 3 Click the **Layer2+** tab.
Step 4 From the left pane, click **Carrier Ethernet**.
Step 5 Click **Query**. The L2 Services Query dialog box appears.
Step 6 From the Existing/New Query drop-down list, choose an existing query or a new query.
Step 7 In the Equipment Termination area, choose **Port** or **Query Group**.
Step 8 If you choose Port, specify the following:
a) Click **Port**. The Port/Channel Group Selection dialog box appears.
b) Choose the node, card, and port/channel group and click **OK**.
c) Close the Port/Channel Group Selection dialog box.
Step 9 If you choose Query Group, specify the following:

a) Click **Query Group**. The User Query Group Chooser dialog box appears.
b) From the Group drop-down list, choose a query group.
c) Add the nodes that can be grouped for the query from the Available Nodes area to the Grouped Nodes area.
d) Click **Save** to save the query group and close the User Query Group Chooser dialog box.

Step 10 In the L2 Services Query dialog box, click **Save**. The Store a Set of Query Criteria dialog box appears.

Step 11 Enter the query name in the Name field and click **Save** to save the query.

Step 12 In the L2 Services Query dialog box, click **Run Query**.
The results of the query appear in the Service Query Results area.

Step 13 Click **Discover All** to discover all the EVC services or click **Discover Selected** to discover the selected EVC services.
Close the L2 Services Query dialog box. The discovered EVC services appear in the Carrier Ethernet Circuits area.

Step 14 Return to your originating procedure (NTP).

Interactions of EVC with Other Features

EVC interacts with the following features.

- LAG
- REP
- MPLS
- Dot1ad and Layer 2 Protocol Tunneling
- MAC learning and MAC address limiting
- QoS
- High Availability
- MVR
- IGMP Snooping

EVC with LAG

EFPs can be configured on a channel group. The traffic, carried by the EFPs, is load balanced across the member links. Ingress traffic for a single EVC can arrive on any member of the bundle. All egress traffic for an EFP uses only one of the member links. The load balancing is achieved by distributing EFPs between the member links. The EFPs on a channel group are grouped and each group is associated with a member link. In the default load balancing mechanism, there is no control over how the EFPs are distributed together, and sometimes the EFP distribution is not ideal. The manual load balancing mechanism can be alternatively used to control the EFP grouping.

When you configure a physical port as part of a channel group, you cannot configure EVCs under that physical port.

The number of LAGs supported is 128 with 8 member links for each LAG.

LACP protocol is supported on the LAG.

EVC with REP

EVC supports up to 32 segments. You can configure REP over EVC using the cross–connect or using the bridge domain at the service instance level. REP is not supported on service instances configured with encapsulation untagged or default type.

REP is not supported for Ethernet Private Line and Ethernet Virtual Private Line services.

EVC with MPLS

MPLS pseudowire circuits can be configured over the service instance infrastructure using xconnect commands to bind the EFPs.

All the encapsulation and rewrite operations are supported for MPLS pseudowire EFPs except the following:

- Symmetric rewrites do not support push 2 tag operations.
- Symmetric 1–to–2 and 2–to–1 translate operations are not supported.

EVC with Layer 2 Protocol Tunneling

CPT supports Layer 2 protocol tunneling only at the interface level. Configurations applied at the interface level are applicable to all the EFPs configured on that interface.

The following port actions are supported in this release:

- Forward—Forwards the unmodified ingress BPDUs on the data path.
- Drop—Drops the ingress BPDUs on the interface.
- Peer—Punts BPDUs to the local instance of the protocol.

Note The pass option, tunnel option, and Layer 2 protocol tunneling at the EFP are not supported in this release.

The following protocols are supported for each port action:

Port Action	Supported Protocols
Peer	LACP, CDP
Drop	STP, VTP, DTP, PAGP, DOT1X, LACP, CDP
Forward	STP, VTP, DTP, PAGP, DOT1X, LACP, CDP

The following table lists the default port action for each protocol:

Protocol	Default Port Action
CDP	Peer
VTP	Forward

Protocol	Default Port Action
DTP	Forward
STP	Forward
PAGP	Forward
LACP	Peer
DOT1X	Forward

See DLP-J212 Configure Layer 2 Protocol Tunneling Using Cisco IOS Commands, on page 155 and DLP-J213 Configure Layer 2 Protocol Tunneling Using CTC, on page 156 to configure Layer 2 protocol tunneling.

EVC with MAC Learning and MAC Address Limiting

MAC learning is supported and enabled (by default) only for point–to–multipoint bridge domains. MAC learning can be enabled or disabled for point–to–multipoint bridge domains.

The MAC address limiting for bridge domains provides the capability to control the MAC address learning behavior at the bridge domain level. You can configure an upper limit on the number of MAC addresses that reside in a bridge domain. The remaining MAC addresses are flooded because they are not learned.

The MAC address limiting commands are configured under the bridge domain.

The default MAC address limit on a bridge domain is 1024. The maximum MAC address limit on a bridge domain is 128000.

EVC with QoS

See EVCS QoS Support, on page 459.

EVC with High Availability

All the EFP configurations are synchronized between the active and standby fabric cards.

EVC with MVR

Multicast VLAN Registration (MVR) is supported only for point–to–multipoint services. Twenty bridge domains can be configured for MVR. The multicast traffic flows from MVR source EFP to multiple MVR receiver EFPs.

EVC with IGMP Snooping

Internet Group Management Protocol Snooping (IGMP snooping) is supported only for point–to–multipoint services. IGMP snooping can be enabled only at the bridge domain level.

DLP-J212 Configure Layer 2 Protocol Tunneling Using Cisco IOS Commands

Purpose	This procedure configures Layer 2 protocol tunneling using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**l2protocol** [**drop**|**forward**|**peer**] [**cdp**|**dot1x**|**dtp**|**lacp**|**pagp**|**stp**|**vtp**] **Example:** Router(config-if)# l2protocol forward cdp	Configures Layer 2 protocol tunneling actions for each interface.
Step 5	**exit** **Example:** Router(config-if)# exit	Returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J213 Configure Layer 2 Protocol Tunneling Using CTC

Purpose	This procedure configures Layer 2 protocol tunneling actions for each port using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to configure Layer 2 protocol tunneling.

Step 2 In node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card, line card, or CPT50 panel.

Step 4 Click the **Provisioning > Ether Ports > Ethernet** tabs.

Step 5 Click the **Configure/Edit L2PT** link under L2PT Config field for each port. The L2PT Config dialog box appears.

Step 6 From the Action drop-down list, choose **Drop**, **Forward**, or **Peer** for each Layer 2 protocol.

Step 7 Click **Apply**.
See DLP-J15 Create a Channel Group Using CTC, on page 551 to configure Layer 2 protocol tunneling actions for the member interfaces of the channel group.

Step 8 Return to your originating procedure (NTP).

Supported Encapsulation and Rewrite Operations

The following table lists the supported encapsulation and rewrite operations for point–to–point (P2P) EVC.

Table 9: Supported Encapsulation and Rewrite Operations for P2P EVC

Encapsulation Criterion	Ingress Rewrite Action
encapsulation default	No rewrite
encapsulation dot1q any	No rewrite
encapsulation dot1q range	No rewrite

Encapsulation Criterion	Ingress Rewrite Action
encapsulation dot1q list	No rewrite
encapsulation untagged	No rewrite
encapsulation untagged, dot1q range, list	No rewrite
encapsulation dot1q vlan<id>	No rewrite
encapsulation dot1q vlan<id> exact	No rewrite
encapsulation dot1q range, list exact	No rewrite
encapsulation dot1q range exact	No rewrite
encapsulation dot1q list exact	No rewrite
encapsulation dot1q any second-dot1q vlan <id>	No rewrite
encapsulation dot1q range second-dot1q vlan<id>	No rewrite
encapsulation dot1q vlan <id> second-dot1q vlan<id>	No rewrite
encapsulation dot1q vlan<id> second-dot1q list	No rewrite
encapsulation dot1ad any	No rewrite
encapsulation dot1ad range	No rewrite
encapsulation dot1ad vlan<id>	No rewrite
encapsulation dot1ad vlan<id> exact	No rewrite
encapsulation dot1ad any dot1q vlan<id>	No rewrite
encapsulation dot1ad range dot1q vlan <id>	No rewrite
encapsulation dot1ad vlan <id> dot1q list	No rewrite
encapsulation dot1q any vlan-type <type value>	No rewrite
encapsulation dot1q range vlan-type <type value>	No rewrite
encapsulation dot1q vlan<id> vlan-type <type value>	No rewrite
encapsulation dot1q vlan<id> vlan-type <type value> exact	No rewrite
encapsulation dot1q any vlan-type <type value> dot1q vlan<id>	No rewrite
encapsulation dot1q range vlan-type <type value> dot1q vlan <id>	No rewrite
encapsulation dot1q vlan <id> vlan-type <type value> dot1q vlan<id>	No rewrite
encapsulation dot1q vlan <id> vlan-type <type value> dot1q list	No rewrite
encapsulation default	rewrite ingress tag push dot1q vlan<id>

Encapsulation Criterion	Ingress Rewrite Action
encapsulation dot1q any	rewrite ingress tag push dot1q vlan<id>
encapsulation dot1q range	rewrite ingress tag push dot1q vlan<id>
encapsulation dot1q list	rewrite ingress tag push dot1q vlan<id>
encapsulation untagged	rewrite ingress tag push dot1q vlan<id>
encapsulation untagged, dot1q range, list	rewrite ingress tag push dot1q vlan<id>
encapsulation dot1q vlan<id>	rewrite ingress tag push dot1q vlan<id>
encapsulation dot1q vlan<id> exact	rewrite ingress tag push dot1q vlan<id>
encapsulation dot1q range, list exact	rewrite ingress tag push dot1q vlan<id>
encapsulation dot1q range exact	rewrite ingress tag push dot1q vlan<id>
encapsulation dot1q list exact	rewrite ingress tag push dot1q vlan<id>
encapsulation default	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q any	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q range	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q list	rewrite ingress tag push dot1ad vlan<id>
encapsulation untagged	rewrite ingress tag push dot1ad vlan<id>
encapsulation untagged, dot1q range, list	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q vlan<id>	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q vlan<id> exact	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q range, list exact	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q range exact	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q list exact	rewrite ingress tag push dot1ad vlan<id>
encapsulation default	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation dot1q any	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation dot1q range	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation dot1q list	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation untagged	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation untagged, dot1q range, list	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>

Encapsulation Criterion	Ingress Rewrite Action
encapsulation dot1q vlan<id>	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation dot1q vlan<id> exact	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation dot1q range, list exact	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation dot1q range exact	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation dot1q list exact	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation untagged	rewrite ingress tag push dot1q vlan<id> second-dot1q vlan<id>
encapsulation untagged	rewrite ingress tag push dot1ad vlan <id> dot1q vlan<id>
encapsulation untagged	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>second-dot1q vlan<id>
encapsulation dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1q vlan<id> exact	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1ad vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1ad vlan<id> exact	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value>	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value> exact	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1q vlan <id> vlan-type <type value> dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1q vlan<id> exact	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1ad vlan<id>	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1ad vlan<id> exact	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value>	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>

Encapsulation Criterion	Ingress Rewrite Action
encapsulation dot1q vlan<id> vlan-type <type value> exact	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1q vlan <id> vlan-type <type value> dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1q vlan<id> exact	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1ad vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1ad vlan<id> exact	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1q vlan<id> vlan-type <type value>	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1q vlan<id> vlan-type <type value> exact	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1q vlan <id> vlan-type <type value> dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1q vlan<id>	rewrite ingress tag translate 1-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1q vlan<id> exact	rewrite ingress tag translate 1-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1ad vlan<id>	rewrite ingress tag translate 1-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1ad vlan<id> exact	rewrite ingress tag translate 1-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value>	rewrite ingress tag translate 1-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value> exact	rewrite ingress tag translate 1-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1q vlan<id>	rewrite ingress tag translate 1-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1q vlan<id> exact	rewrite ingress tag translate 1-to-2 dot1ad vlan <id> dot1q vlan <id>

Encapsulation Criterion	Ingress Rewrite Action
encapsulation dot1ad vlan<id>	rewrite ingress tag translate 1-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1ad vlan<id> exact	rewrite ingress tag translate 1-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value>	rewrite ingress tag translate 1-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value> exact	rewrite ingress tag translate 1-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1q vlan<id>	rewrite ingress tag translate 1-to-2 dot1q vlan <id> vlan-type <type-value> second-dot1q vlan <id>
encapsulation dot1q vlan<id> exact	rewrite ingress tag translate 1-to-2 dot1q vlan <id> vlan-type <type-value> second-dot1q vlan <id>
encapsulation dot1ad vlan<id>	rewrite ingress tag translate 1-to-2 dot1q vlan <id> vlan-type <type-value> second-dot1q vlan <id>
encapsulation dot1ad vlan<id> exact	rewrite ingress tag translate 1-to-2 dot1q vlan <id> vlan-type <type-value> second-dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value>	rewrite ingress tag translate 1-to-2 dot1q vlan <id> vlan-type <type-value> second-dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value> exact	rewrite ingress tag translate 1-to-2 dot1q vlan <id> vlan-type <type-value> second-dot1q vlan <id>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1q vlan <id>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1q vlan <id>
encapsulation dot1q vlan <id> vlan-type <type value> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1q vlan <id>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1ad vlan <id>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1ad vlan <id>
encapsulation dot1q vlan <id> vlan-type <type value> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1ad vlan <id>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1q vlan <id> vlan-type <type value>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1q vlan <id> vlan-type <type value>
encapsulation dot1q vlan <id> vlan-type <type value> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1q vlan <id> vlan-type <type value>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1q vlan <id> second-dot1q vlan <id>

Encapsulation Criterion	Ingress Rewrite Action
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1q vlan <id> vlan-type <type value> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1q vlan <id> vlan-type <type value> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1q vlan <id> vlan-type <type value> second-dot1q vlan <id>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1q vlan <id> vlan-type <type value> second-dot1q vlan <id>
encapsulation dot1q vlan <id> vlan-type <type value> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1q vlan <id> vlan-type <type value> second-dot1q vlan <id>

The following table lists the supported encapsulation and rewrite operations for point–to–multipoint (P2MP) EVC :

Table 10: Supported Encapsulation and Rewrite Operations for P2MP EVC

Encapsulation Criterion	Ingress Rewrite Action
encapsulation default	No rewrite
encapsulation dot1q any	No rewrite
encapsulation dot1q range	No rewrite
encapsulation dot1q list	No rewrite
encapsulation untagged	No rewrite
encapsulation untagged, dot1q range, list	No rewrite
encapsulation dot1q vlan<id>	No rewrite
encapsulation dot1q vlan<id> exact	No rewrite
encapsulation dot1q range, list exact	No rewrite
encapsulation dot1q range exact	No rewrite
encapsulation dot1q list exact	No rewrite
encapsulation dot1q any second-dot1q vlan <id>	No rewrite

Encapsulation Criterion	Ingress Rewrite Action
encapsulation dot1q range second-dot1q vlan<id>	No rewrite
encapsulation dot1q vlan <id> second-dot1q vlan<id>	No rewrite
encapsulation dot1q vlan<id> second-dot1q list	No rewrite
encapsulation dot1ad any	No rewrite
encapsulation dot1ad range	No rewrite
encapsulation dot1ad vlan<id>	No rewrite
encapsulation dot1ad vlan<id> exact	No rewrite
encapsulation dot1ad any dot1q vlan<id>	No rewrite
encapsulation dot1ad range dot1q vlan <id>	No rewrite
encapsulation dot1ad vlan <id> dot1q vlan<id>	No rewrite
encapsulation dot1ad vlan <id> dot1q list	No rewrite
encapsulation dot1q any vlan-type <type value>	No rewrite
encapsulation dot1q range vlan-type <type value>	No rewrite
encapsulation dot1q vlan<id> vlan-type <type value>	No rewrite
encapsulation dot1q vlan<id> vlan-type <type value> exact	No rewrite
encapsulation dot1q any vlan-type <type value> dot1q vlan<id>	No rewrite
encapsulation dot1q range vlan-type <type value> dot1q vlan <id>	No rewrite
encapsulation dot1q vlan <id> vlan-type <type value> dot1q vlan<id>	No rewrite
encapsulation dot1q vlan <id> vlan-type <type value> dot1q list	No rewrite
encapsulation default	rewrite ingress tag push dot1q vlan<id>
encapsulation dot1q any	rewrite ingress tag push dot1q vlan<id>
encapsulation dot1q range	rewrite ingress tag push dot1q vlan<id>
encapsulation dot1q list	rewrite ingress tag push dot1q vlan<id>
encapsulation untagged	rewrite ingress tag push dot1q vlan<id>

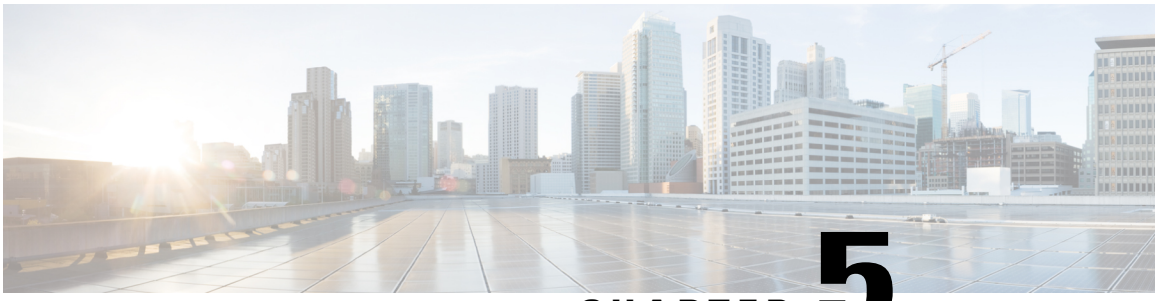
Encapsulation Criterion	Ingress Rewrite Action
encapsulation untagged, dot1q range, list	rewrite ingress tag push dot1q vlan<id>
encapsulation dot1q vlan<id>	rewrite ingress tag push dot1q vlan<id>
encapsulation dot1q vlan<id> exact	rewrite ingress tag push dot1q vlan<id>
encapsulation dot1q range, list exact	rewrite ingress tag push dot1q vlan<id>
encapsulation dot1q range exact	rewrite ingress tag push dot1q vlan<id>
encapsulation dot1q list exact	rewrite ingress tag push dot1q vlan<id>
encapsulation default	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q any	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q range	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q list	rewrite ingress tag push dot1ad vlan<id>
encapsulation untagged	rewrite ingress tag push dot1ad vlan<id>
encapsulation untagged, dot1q range, list	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q vlan<id>	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q vlan<id> exact	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q range, list exact	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q range exact	rewrite ingress tag push dot1ad vlan<id>
encapsulation dot1q list exact	rewrite ingress tag push dot1ad vlan<id>
encapsulation default	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation dot1q any	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation dot1q range	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation dot1q list	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation untagged	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation untagged, dot1q range, list	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation dot1q vlan<id>	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation dot1q vlan<id> exact	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>

Encapsulation Criterion	Ingress Rewrite Action
encapsulation dot1q range, list exact	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation dot1q range exact	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation dot1q list exact	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>
encapsulation untagged	rewrite ingress tag push dot1q vlan<id> second-dot1q vlan<id>
encapsulation untagged	rewrite ingress tag push dot1ad vlan <id> dot1q vlan<id>
encapsulation untagged	rewrite ingress tag push dot1q vlan<id> vlan-type <type value>second-dot1q vlan<id>
encapsulation dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1q vlan<id> exact	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1ad vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1ad vlan<id> exact	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value>	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value> exact	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1q vlan <id> vlan-type <type value>	rewrite ingress tag translate 1-to-1 dot1q vlan <id>
encapsulation dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1q vlan<id> exact	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1ad vlan<id>	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1ad vlan<id> exact	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value>	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value> exact	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>

Encapsulation Criterion	Ingress Rewrite Action
encapsulation dot1q vlan <id> vlan-type <type value> dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1ad vlan <id>
encapsulation dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1q vlan<id> exact	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1ad vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1ad vlan<id> exact	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1q vlan<id> vlan-type <type value>	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1q vlan<id> vlan-type <type value> exact	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1q vlan <id> vlan-type <type value> dot1q vlan<id>	rewrite ingress tag translate 1-to-1 dot1q vlan <id> vlan-type <type-value>
encapsulation dot1q vlan<id>	rewrite ingress tag translate 1-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1q vlan<id> exact	rewrite ingress tag translate 1-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1ad vlan<id>	rewrite ingress tag translate 1-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1ad vlan<id> exact	rewrite ingress tag translate 1-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value>	rewrite ingress tag translate 1-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value> exact	rewrite ingress tag translate 1-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1q vlan<id>	rewrite ingress tag translate 1-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1q vlan<id> exact	rewrite ingress tag translate 1-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1ad vlan<id>	rewrite ingress tag translate 1-to-2 dot1ad vlan <id> dot1q vlan <id>

Encapsulation Criterion	Ingress Rewrite Action
encapsulation dot1ad vlan<id> exact	rewrite ingress tag translate 1-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value>	rewrite ingress tag translate 1-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value> exact	rewrite ingress tag translate 1-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1q vlan<id>	rewrite ingress tag translate 1-to-2 dot1q vlan <id> vlan-type <type-value> second-dot1q vlan <id>
encapsulation dot1q vlan<id> exact	rewrite ingress tag translate 1-to-2 dot1q vlan <id> vlan-type <type-value> second-dot1q vlan <id>
encapsulation dot1ad vlan<id>	rewrite ingress tag translate 1-to-2 dot1q vlan <id> vlan-type <type-value> second-dot1q vlan <id>
encapsulation dot1ad vlan<id> exact	rewrite ingress tag translate 1-to-2 dot1q vlan <id> vlan-type <type-value> second-dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value>	rewrite ingress tag translate 1-to-2 dot1q vlan <id> vlan-type <type-value> second-dot1q vlan <id>
encapsulation dot1q vlan<id> vlan-type <type value> exact	rewrite ingress tag translate 1-to-2 dot1q vlan <id> vlan-type <type-value> second-dot1q vlan <id>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1q vlan <id>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1q vlan <id>
encapsulation dot1q vlan <id> vlan-type <type value>	rewrite ingress tag translate 2-to-1 dot1q vlan <id>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1ad vlan <id>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1ad vlan <id>
encapsulation dot1q vlan <id> vlan-type <type value> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1ad vlan <id>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1q vlan <id> vlan-type <type value>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1q vlan <id> vlan-type <type value>
encapsulation dot1q vlan <id> vlan-type <type value> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-1 dot1q vlan <id> vlan-type <type value>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1q vlan <id> second-dot1q vlan <id>

Encapsulation Criterion	Ingress Rewrite Action
encapsulation dot1q vlan <id> vlan-type <type value> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1q vlan <id> second-dot1q vlan <id>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1q vlan <id> vlan-type <type value> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1ad vlan <id> dot1q vlan <id>
encapsulation dot1q vlan <id> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1q vlan <id> vlan-type <type value> second-dot1q vlan <id>
encapsulation dot1ad vlan <id> dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1q vlan <id> vlan-type <type value> second-dot1q vlan <id>
encapsulation dot1q vlan <id> vlan-type <type value> second-dot1q vlan<id>	rewrite ingress tag translate 2-to-2 dot1q vlan <id> vlan-type <type value> second-dot1q vlan <id>
encapsulation dot1q <vlan> second-dot1q <vlan>	rewrite ingress tag pop 2
encapsulation dot1ad <vlan> dot1q <vlan>	rewrite ingress tag pop 2
encapsulation dot1q <vlan> vlan-type <type value> second-dot1q <vlan>	rewrite ingress tag pop 2
encapsulation dot1q vlan<id>	rewrite ingress tag pop 1
encapsulation dot1q vlan<id> exact	rewrite ingress tag pop 1
encapsulation dot1q vlan<id> second-dot1q vlan<id>	rewrite ingress tag pop 1
encapsulation dot1ad vlan<id>	rewrite ingress tag pop 1
encapsulation dot1ad vlan<id> exact	rewrite ingress tag pop 1
encapsulation dot1ad vlan<id> dot1q vlan<id>	rewrite ingress tag pop 1
encapsulation dot1q vlan<id>vlan-type <type value>	rewrite ingress tag pop 1
encapsulation dot1q vlan<id> vlan-type <type value> exact	rewrite ingress tag pop 1
encapsulation dot1q vlan<id> vlan-type <type value> second-dot1q vlan<id>	rewrite ingress tag pop 1



CHAPTER 5

Configuring Multiprotocol Label Switching

This chapter describes Multiprotocol Label Switching and procedures to configure Multiprotocol Label Switching.

Understanding Multiprotocol Label Switching

Multiprotocol Label Switching (MPLS) is the technology that scales IP networks for the service providers. MPLS provides mechanisms for IP quality of service (QoS) and IP traffic engineering. MPLS is an industry standard on which label switching is based. MPLS is a switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets. The forwarding of MPLS packets is based on preestablished IP routing information.

MPLS enables service providers to offer additional services to their enterprise customers, including VPNs, improved traffic engineering, QoS, Layer 2 tunneling, and multiprotocol support.

There are two ways to set up the MPLS infrastructure—LDP and MPLS–TE. Label Distribution Protocol (LDP) differs from MPLS–TE in terms of the protocol it uses to distribute the labels along the path. LDP uses the Label Distribution Protocol whereas MPLS–TE uses the Resource Reservation Protocol – Traffic Engineering (RSVP–TE) protocol to distribute the labels. However, both LDP and RSVP–TE use the OSPF for the routing protocol.

Note Carrier Packet Transport (CPT) supports OSPF and OSPF-TE.

Understanding Common Terms in MPLS

The following section describes the common terms in MPLS.

- Multiprotocol Label Switching (MPLS)—This technique allows the forwarding of packets based on labels. In a normal IP network, the packets are switched based on the destination IP address. In an MPLS network, the packets are switched based on the label.
- Label Distribution Protocol (LDP)—This protocol (an IETF standard) binds labels to network addresses.
- Resource Reservation Protocol (RSVP)—This protocol distributes labels for traffic engineering.
- Resource Reservation Protocol – Traffic Engineering (RSVP–TE)—This protocol reserves network resources to provide quality of service guarantees to application flows, and distributes labels for traffic engineering. RSVP-TE is an extension to RSVP.
- Label Switched Path (LSP)—This is the path that the label takes to pass through the network. LSPs are unidirectional. LSP is a sequence of hops where a packet travels from one router to another router through label switching mechanisms. A label switched path can be established dynamically based on normal routing mechanisms, or through configuration.
- Label Switch Router (LSR)—This is a device, such as a switch or router, that forwards MPLS packets based on the value of a fixed-length label encapsulated in each packet. LSRs dynamically learn the labels they should use to switch the packets through label distribution protocols, such as LDP and RSVP-TE.
- Label Information Base (LIB)—This is the database that the LSR uses to store labels learned from other LSRs and labels assigned by the local LSR.
- Traffic Engineering (TE)—This provides a set of techniques and processes that causes routed traffic to travel through the network on a path other than the one that is chosen when standard routing methods are used. TE is the ability to dynamically define routes based on known demand or alternate available routes.
- Forwarding Equivalency Class (FEC)—FEC handles a set of packets that can be handled equivalently for the purpose of forwarding to make it suitable for binding to a single label. The set of packets destined for an address prefix is one example of an FEC.
- Tunnel—This refers to a secure communication path between two peers, such as two LSRs.
- Interior Gateway Protocol (IGP)—This protocol uses the Internet protocol to exchange routing information within an autonomous system. Examples of common IGPs include OSPF and Routing Information Protocol (RIP).

- Open Shortest Path First (OSPF)—Link-state, hierarchical IGP routing algorithm proposed as a successor to Routing Information Protocol (RIP) in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing.
- Pseudowire—This refers to emulation of services over the MPLS network. It is a technique to transport any kind of payload over the MPLS network.
- Operations, Administration, and Maintenance (OAM)— This verifies that the packets associated with a specific FEC are forwarded to the correct LSP and are terminated on a LSR that is an egress for that FEC.

NTP-J42 Configure Global Settings for MPLS

Purpose	This procedure configures global settings for MPLS.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J108 Create a Loopback Interface Using Cisco IOS Commands, on page 171
- DLP-J109 Create and Edit a Loopback Interface Using CTC, on page 172
- DLP-J110 Specify the IP Address for Interfaces That Participate in an MPLS Network Using Cisco IOS Commands, on page 173
- DLP-J111 Specify the IP Address for Interfaces That Participate in an MPLS Network Using CTC, on page 174
- DLP-J114 Specify the LDP Router ID Using Cisco IOS Commands, on page 185

Stop. You have completed this procedure.

DLP-J108 Create a Loopback Interface Using Cisco IOS Commands

Purpose	This procedure creates a loopback interface that is used as the LDP router ID.
Tools/Equipment	None

Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *loopbacknumber* **Example:** Router(config)# interface loopback0	Creates a loopback interface.
Step 4	Return to your originating procedure (NTP).	—

DLP-J109 Create and Edit a Loopback Interface Using CTC

Purpose	This procedure creates and edits a loopback interface that is used as the LDP router ID.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

You can create only one loopback interface.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to create or edit a loopback interface.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **Control Plane**.

Step 5 Click the **Loopback/IP** tab.

Step 6 If you want to create a loopback interface, complete the following:

a) In the Loopback Interface area, click **Create**. The Create Loopback Interface dialog box appears.

b) Enter the interface, IP address, and mask in the respective fields and click **OK**.

Step 7 If you want to edit a loopback interface, complete the following:

a) In the Loopback Interface area, select the loopback interface to edit.

b) Click **Edit**. The Edit Loopback Interface dialog box appears.

c) Modify the values of the IP address and mask as required and click **OK**.

Step 8 Return to your originating procedure (NTP).

DLP-J110 Specify the IP Address for Interfaces That Participate in an MPLS Network Using Cisco IOS Commands

Purpose	This procedure specifies the IP addresses for interfaces that participate in an MPLS network using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	Router> enable	
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface and enters interface configuration mode.
Step 4	**ip address** *ip-address mask-value* **Example:** Router(config-if)# ip address 192.168.10.10 255.255.255.255	Assigns an IP network address and network mask to the interface.
Step 5	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J111 Specify the IP Address for Interfaces That Participate in an MPLS Network Using CTC

Purpose	This procedure specifies the IP addresses for interfaces that participate in an MPLS network.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

All the interfaces participating in the MPLS network must specify the IP address and mask.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to specify the IP addresses.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **Control Plane**.

Step 5 Click the **Loopback/IP** tab.

Step 6 In the Interfaces/IP Addressing area, enter the IP address and mask for the interfaces that you want to participate in an MPLS network.

Step 7 Click **Apply** to save the configuration.

Step 8 Return to your originating procedure (NTP).

Understanding OSPF and NSF

Open Shortest Path First (OSPF) is a link–state, hierarchical IGP routing algorithm proposed as a successor to Routing Information Protocol (RIP) in the Internet community. OSPF features include least–cost routing, multipath routing, and load balancing.

LDP and RSVP–TE uses OSPF for the routing protocol. CPT supports OSPF and OSPF–TE.

See Nonstop Forwarding, on page 481 for information on Nonstop Forwarding (NSF).

NTP-J65 Configure OSPF and OSPF–TE

Purpose	This procedure configures OSPF and OSPF–TE protocols.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J112 Enable OSPF Protocol on Specific Interfaces Using Cisco IOS Commands, on page 176

- DLP-J113 Enable OSPF on Specific Interfaces Using CTC, on page 177
- DLP-J209 Configure NSF for OSPF Using CTC, on page 178
- DLP-J221 Configure Cisco NSF for OSPF Using Cisco IOS Commands, on page 179
- DLP-J222 Configure IETF NSF for OSPF Using Cisco IOS Commands, on page 180
- DLP-J138 Configure OSPF to Support Traffic Engineering Using Cisco IOS Commands, on page 182
- DLP-J139 Enable OSPF-TE Protocol on Specific Interfaces Using CTC, on page 183

Stop. You have completed this procedure.

DLP-J112 Enable OSPF Protocol on Specific Interfaces Using Cisco IOS Commands

Purpose	This procedure defines the interfaces where OSPF runs and defines the area ID for those interfaces.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** Router(config)# router ospf 1	Enables OSPF routing and enters router configuration mode.

	Command or Action	Purpose
Step 4	**network** *ip-address wildcard-mask* **area** *area-id* **Example:** Router(config-router)# network 10.0.0.0 0.0.255.255 area 3	Specifies the interface on which OSPF runs and defines the area ID for that interface.
Step 5	**end** **Example:** Router(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J113 Enable OSPF on Specific Interfaces Using CTC

Purpose	This procedure defines the interfaces where OSPF runs and defines the area ID for those interfaces.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note CPT supports OSPF and OSPF-TE. CPT supports only one OSPF instance but multiple OSPF areas.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to enable the OSPF protocol on specific interfaces.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **Control Plane**.

Step 5 Click the **OSPF** tab.

Step 6 In the OSPF Enabled Interfaces area, click **Create**. The Create OSPF Entry dialog box appears.

Step 7 Enter the IP address, wildcard, and area ID of the interface where the OSPF runs and click **OK**.

Step 8 Return to your originating procedure (NTP).

DLP-J209 Configure NSF for OSPF Using CTC

Purpose	This procedure configures NSF for OSPF using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Non Stop Forwarding (NSF) is required for uninterrupted service of OSPF over SSO.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to enable the OSPF NSF.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **Control Plane**.

Step 5 Click the **OSPF** tab.

Step 6 In the OSPF NSF area, check the following check boxes as required:

a) Check the **NSF Cisco** check box to enable Cisco NSF operations on a router that is running OSPF.

b) Check the **NSF Cisco Helper** check box to enable Cisco NSF helper mode on a router that is running OSPF.

c) Check the **NSF IETF** check box to enable Internet Engineering Task Force (IETF) NSF operations on a router that is running OSPF.
d) Check the **NSF IETF Helper** check box to enable IETF NSF helper mode on a router that is running OSPF.
e) Check the **Strict LSA Checking** check box to enable strict link-state advertisement (LSA) checking on a router that is running OSPF.

Step 7 Click **Apply** to save the configuration.

Step 8 Return to your originating procedure (NTP).

DLP-J221 Configure Cisco NSF for OSPF Using Cisco IOS Commands

Purpose	This procedure configures Cisco NSF for OSPF using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** Router(config)# router ospf 12	Enables OSPF and enters router configuration mode.
Step 4	**nsf cisco [enforce global]** **Example:** Router(config-router)# nsf cisco	Enables Cisco NSF restarting mode. • This command is not required on devices that will operate only in NSF helper mode.

	Command or Action	Purpose
Step 5	**no nsf cisco helper disable** **Example:** Router(config-router)# no nsf cisco helper disable	(Optional) Re–enables Cisco NFS helper support. • This command is included here only to show how to reenable Cisco NSF helper mode if helper mode was explicitly disabled.
Step 6	**nsf ietf helper disable** **Example:** Router(config-router)# nsf ietf helper disable	(Optional) Disables IETF NSF helper mode on an NSF-aware device.
Step 7	**end** **Example:** Router(config-router)# end	Exits to privileged EXEC mode.
Step 8	**show ip ospf nsf** **Example:** Router# show ip ospf nsf	Displays OSPF NSF state information.
Step 9	Return to your originating procedure (NTP).	—

DLP-J222 Configure IETF NSF for OSPF Using Cisco IOS Commands

Purpose	This procedure configures IETF NSF for OSPF using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Router> enable	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** Router(config)# router ospf 12	Enables OSPF and enters router configuration mode.
Step 4	**nsf ietf** [**restart-interval**] *seconds* **Example:** Router(config-router)# nsf ietf restart-interval 180	Enables IETF NSF restarting mode. • This command is not required on devices that will operate only in NSF helper mode.
Step 5	**nsf ietf [helper [disable | strict-lsa-checking]]** **Example:** Router(config-router)# nsf ietf helper strict-lsachecking	(Optional) Configures IETF NSF helper mode on neighbor devices that will operate in helper mode.
Step 6	**no nsf ietf helper disable** **Example:** Router(config-router)# no nsf ietf helper disable	(Optional) Reenables IETF NSF helper mode. • This command is included here only to show how to re-enable IETF NSF helper mode if helper mode was explicitly disabled.
Step 7	**nsf cisco helper disable** **Example:** Router(config-router)# nsf cisco helper disable	(Optional) Disables Cisco NSF helper mode on an NSF-aware device.
Step 8	**end** **Example:** Router(config-router)# end	Exits to privileged EXEC mode.
Step 9	**show ip ospf nsf** **Example:** Router# show ip ospf nsf	Displays OSPF NSF state information.
Step 10	Return to your originating procedure (NTP).	—

DLP-J138 Configure OSPF to Support Traffic Engineering Using Cisco IOS Commands

Purpose	This procedure configures OSPF to support traffic engineering.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note MPLS traffic engineering supports only a single IGP instance. MPLS traffic engineering must not be configured in more than one IGP instance.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** Router(config)# router ospf 200	Configures an OSPF routing process for IP and enters router configuration mode. • The value for the **process-id** argument is an internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. Assign a unique value for each OSPF routing process.

	Command or Action	Purpose
Step 4	**mpls traffic-eng area** *number* **Example:** Router(config-router)# mpls traffic-eng area 0	Enables MPLS TE for the indicated OSPF area.
Step 5	**mpls traffic-eng router-id** *interface* **Example:** Router(config-router)# mpls traffic-eng router-id loopback0	Specifies that the TE router identifier for the node is the IP address associated with interface loopback0.
Step 6	**exit** **Example:** Router(config-router)# exit	Exits to global configuration mode.
Step 7	**exit** **Example:** Router(config)# exit	Exits to privileged EXEC mode.
Step 8	Return to your originating procedure (NTP).	—

DLP-J139 Enable OSPF-TE Protocol on Specific Interfaces Using CTC

Purpose	This procedure configures a router running OSPF to flood traffic engineering for specific OSPF areas. In other words, this procedure enables MPLS TE for selected OSPF areas.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to enable the OSPF-TE protocol on specific interfaces.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **MPLS TE**.

Step 5 Click the **OSPF-TE** tab.

Step 6 In the OSPF TE Enabled Areas area, select the area IDs where you want to enable OSPF-TE.

Step 7 Check the **Autoconfig** check box for specific area IDs where you want to enable OSPF-TE.

Step 8 Click **Apply** to save the configuration.

Step 9 Return to your originating procedure (NTP).

Understanding LDP

Label Distribution Protocol (LDP) enables peer label switch routers (LSRs) in an MPLS network to exchange label binding information for supporting hop-by-hop forwarding in an MPLS network. Label switching on a router requires the Cisco Express Forwarding to be enabled on that router.

MPLS LDP enables LSRs to request, distribute, and release label prefix binding information to peer routers in a network. LDP enables LSRs to discover potential peers and to establish LDP sessions with those peers for the purpose of exchanging label binding information.

MPLS LDP enables one LSR to inform another LSR of the label bindings it has made. When a pair of routers communicates the LDP parameters, they establish a label switched path (LSP). MPLS LDP enables LSRs to distribute labels along normally routed paths to support MPLS forwarding. This method of label distribution is called hop-by-hop forwarding. With IP forwarding, when a packet arrives at a router, the router checks the destination address in the IP header, performs a route lookup, and forwards the packet to the next hop. With MPLS forwarding, when a packet arrives at a router, the router checks the incoming label, looks up the label in a table, and then forwards the packet to the next hop. MPLS LDP is useful for applications that require hop-by-hop forwarding, such as MPLS VPNs.

MPLS LDP provides the building blocks for MPLS-enabled applications, such as VPNs.

LDP Label Spaces and LDP Identifiers

An LDP label binding is an association between a destination prefix and a label. The label used in LDP label binding is allocated from a set of possible labels called a label space.

LDP supports two types of label spaces:

- Interface–specific—An interface–specific label space uses interface resources for labels. Depending on its configuration, an LDP platform may support zero, one, or more interface–specific label spaces.
- Platform–wide—An LDP platform supports a single platform–wide label space, which interfaces that share the same labels can use. For Cisco platforms, all interface types, except LC–ATM, use the platform–wide label space.

LDP supports identifiers of 6 bytes that are called LDP Identifiers (LDP ID), which are used to name label spaces. The LDP ID is made up of the following components:

- The first four bytes, called the LDP router ID, identify the LSR that owns the label space.
- The last two bytes, called the local label space ID, identify the label space within the LSR. For the platform–wide label space, the last two bytes of the LDP ID are always both 0.

The LDP ID takes the following form:

<LDP router ID> : <local label space ID>

The examples of LDP IDs are 209.165.200.225 and 209.165.200.226

LDP Router ID

The **mpls ldp router-id** command allows you to establish the IP address of an interface as the LDP router ID.

The following steps describe the normal process to determine the LDP router ID:

1. The router examines the IP addresses of all the operational interfaces.
2. If these IP addresses include loopback interface addresses, the router selects the largest loopback address. Configuring a loopback address helps ensure a stable LDP ID for the router because the state of loopback addresses does not change. However, configuring a loopback interface and IP address on each router is not required.

   If these IP addresses do not include loopback interface addresses, the router selects the largest IP address pertaining to an operational interface as the LDP router ID.

The loopback IP address does not become the router ID of the local LDP ID under the following circumstances:

- If the loopback interface has been explicitly shut down.
- If the **mpls ldp router-id** command specifies that a different interface should be used as the LDP router ID.

If you use a loopback interface, ensure that the IP address for the loopback interface is configured with a /32 network mask. In addition, ensure that the routing protocol in use is configured to advertise the corresponding /32 network.

DLP-J114 Specify the LDP Router ID Using Cisco IOS Commands

Purpose	This procedure establishes the IP address of an interface as the LDP router ID.
Tools/Equipment	None
Prerequisite Procedures	Ensure that the specified interface is operational before assigning it as the LDP router ID.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls ip** **Example:** Router(config)# mpls ip	Configures MPLS hop-by-hop forwarding globally. The **mpls ip** command is enabled by default; you do not have to specify this command. **Note** Globally enabling MPLS forwarding does not enable it on the interfaces. You must enable MPLS forwarding on the interfaces separately.
Step 4	**mpls label protocol ldp** **Example:** Router(config)# mpls label protocol ldp	Configures the use of LDP on all the interfaces.
Step 5	**mpls ldp router-id** *interface* [**force**] **Example:** Router(config)# mpls ldp router-id TenGigabitEthernet 4/1	Specifies the preferred interface for determining the LDP router ID.
Step 6	**exit** **Example:** Router(config)# exit	Exits global configuration mode and enters privileged EXEC mode.
Step 7	**show mpls ldp discovery** [**all** | **detail**] **Example:** Router# show mpls ldp discovery	Displays the LDP identifier for the local router.
Step 8	Return to your originating procedure (NTP).	—

Specify the LDP Router ID

The following example assigns interface TenGigabitEthernet4/1 as the LDP router ID:

```
Router> enable
Router# configure terminal
Router(config)# mpls ip
Router(config)# mpls label protocol ldp
Router(config)# mpls ldp router-id TenGigabitEthernet4/1
```

The following example displays the LDP router ID:

```
Router# show mpls ldp discovery
```

```
Local LDP Identifier:
    10.15.15.15:0
Discovery Sources:
    Interfaces:
       Ethernet4 (ldp): xmit/recv
           LDP Id: 10.14.14.14:0
```

Understanding MPLS LDP Autoconfiguration

To enable LDP, you must configure it globally and on each interface where it is needed. Configuring LDP on many interfaces can be time-consuming.

The MPLS LDP Autoconfiguration feature enables you to globally configure LDP on each interface associated with a specific OSPF instance. OSPF IGPs support this feature. The MPLS LDP Autoconfiguration feature blocks LDPs from enabling on interfaces that you want to prevent from being enabled. This feature makes configuration easier, faster, and error–free.

Restrictions

The MPLS LDP Autoconfiguration feature has the following restrictions:

- If LDP is disabled globally, the **mpls ldp autoconfig** command fails and generates a console message explaining that LDP must first be enabled globally by using the **global mpls ip** command.
- If the **mpls ldp autoconfig** command is configured for the OSPF instance, you cannot use the **global no mpls ip** command. To disable LDP, you must first use the **no mpls ldp autoconfig** command.
- The MPLS LDP Autoconfiguration feature is not supported on traffic engineering tunnel interfaces.

NTP-J43 Configure MPLS LDP Autoconfiguration

Purpose	This procedure configures MPLS LDP autoconfiguration.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J115 Enable MPLS LDP Autoconfiguration Using Cisco IOS Commands, on page 188
- DLP-J116 Disable MPLS LDP Autoconfiguration Using Cisco IOS Commands, on page 190
- DLP-J117 Verify MPLS LDP Autoconfiguration Using Cisco IOS Commands, on page 191
- DLP-J118 Enable or Disable MPLS LDP Autoconfiguration Using CTC, on page 193

Stop. You have completed this procedure.

DLP-J115 Enable MPLS LDP Autoconfiguration Using Cisco IOS Commands

Purpose	This procedure allows you to: • Enable LDP on each interface globally. • Enable LDP on interfaces associated with specific OSPF areas.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	Router# configure terminal	
Step 3	**mpls ip** **Example:** Router(config)# mpls ip	Globally enables MPLS hop-by-hop forwarding.
Step 4	**mpls label protocol ldp** **Example:** Router(config)# mpls label protocol ldp	Specifies LDP as the default label distribution protocol.
Step 5	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure, and enters interface configuration mode.
Step 6	**ip address** *ip-address mask-value* **Example:** Router(config-if)# ip address 10.0.0.11 255.255.255.255	Assigns an IP address and network mask to the interface.
Step 7	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode.
Step 8	**router ospf** *process-id* **Example:** Router(config)# router ospf 1	Enables OSPF routing and enters router configuration mode.
Step 9	**network** *ip-address wildcard-mask* **area** *area-id* **Example:** Router(config-router)# network 10.0.0.0 0.0.255.255 area 3	Specifies the interface where OSPF runs and defines the area ID for that interface.
Step 10	**mpls ldp autoconfig** [**area** *area-id*] **Example:** Router(config-router)# mpls ldp autoconfig area 3	Enables the MPLS LDP Autoconfiguration feature. If no OSPF area is specified, the command applies to all the interfaces associated with the OSPF process. If an area ID is specified, then only the interfaces associated with that OSPF area are enabled with LDP.

	Command or Action	Purpose
Step 11	**end** **Example:** Router(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.
Step 12	Return to your originating procedure (NTP).	—

DLP-J116 Disable MPLS LDP Autoconfiguration Using Cisco IOS Commands

Purpose	This procedure disables the MPLS LDP autoconfiguration feature.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure, and enters interface configuration mode.
Step 4	**no mpls ldp igp autoconfig** [**area** *area-id*] **Example:** Router(config-if)# no mpls ldp igp autoconfig	Disables LDP for that interface.

	Command or Action	Purpose
Step 5	**end** **Example:** Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J117 Verify MPLS LDP Autoconfiguration Using Cisco IOS Commands

Purpose	This procedure verifies LDP autoconfiguration.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**show mpls interfaces** [*type number*] [**all**] [**detail**] [**internal**]
	
	Example:
	Router# show mpls interfaces TenGigabitEthernet4/1 detail
		Displays the method used to enable LDP on an interface.
		The following example shows that LDP was enabled on the interface by both the **mpls ip** and **mpls ldp autoconfig** commands:
		
		`Interface TenGigabitEthernet4/1:`
		`  IP labeling enabled (ldp):`
		`  Interface config`
		`  IGP config`
		`  LSP Tunnel labeling enabled`
		`  BGP labeling not enabled`
		`  MPLS operational`
		`  Fast Switching Vectors:`
		`  IP to MPLS Fast Switching Vector`
		`  MPLS Turbo Vector`
		`  MTU = 1500`

	Command or Action	Purpose

Step 3	**show mpls ldp discovery** [**all**] [**detail**]
	
	Example:
	Router# show mpls ldp discovery detail
		Displays how LDP was enabled on the interface.
		In the following example, LDP was enabled by both the **mpls ip** and **mpls ldp autoconfig** commands:
		
		`Local LDP Identifier:`
		`    10.11.11.11:0`
		`    Discovery Sources:`
		`    Interfaces:`
		`      TenGigabitEthernet4/1 (ldp): xmit/recv`
		
		`        Enabled: Interface config, IGP config;`
		`        Hello interval: 5000 ms; Transport IP addr: 10.11.11.11`
		`        LDP Id: 10.10.10.10:0`
		`          Src IP addr: 10.0.0.1; Transport IP addr: 10.10.10.10`
		`          Hold time: 15 sec; Proposed local/peer: 15/15 sec`

Step 4	Return to your originating procedure (NTP).	—

Example of MPLS LDP Autoconfiguration with OSPF

The following configuration commands enable LDP for OSPF process 1 area 3. The **mpls ldp autoconfig area 3** command and the OSPF **network** commands enable LDP on TenGigabitEthernet interfaces 0/0, 0/1, and 1/1. The **no mpls ldp igp autoconfig** command on TenGigabitEthernet interface 1/0 prevents LDP from being enabled on TenGigabitEthernet interface 1/0, even though OSPF is enabled for that interface.

```
configure terminal
interface TenGigabitEthernet 0/0
ip address 10.0.0.1 255.0.0.0
!
interface TenGigabitEthernet 0/1
ip address 10.0.1.1 255.0.0.1
!
interface TenGigabitEthernet 1/1
ip address 10.1.1.1 255.255.0.0
!
interface TenGigabitEthernet 1/0
ip address 10.1.0.1 0.1.0.255
exit
!
router ospf 1
network 10.0.0.0 0.0.255.255 area 3
network 10.1.0.0 0.0.255.255 area 3
mpls ldp autoconfig area 3
end
interface TenGigabitEthernet 1/0
no mpls ldp igp autoconfig
```

DLP-J118 Enable or Disable MPLS LDP Autoconfiguration Using CTC

Purpose	This procedure allows you to: • Enable LDP on each interface globally. • Enable LDP on interfaces associated with specific OSPF areas. • Disable LDP on each interface globally.
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 NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to enable or disable LDP autoconfiguration.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **Control Plane**.

Step 5 Click the **OSPF** tab.

Step 6 In the LDP Autoconfig area, complete one of the following actions:

a) To globally enable LDP on each interface, click the **Global** radio button.

b) To enable LDP on interfaces associated with specific OSPF areas, click the **Area Id** radio button and check the **Autoconfig** check box for specific area IDs.

c) To globally disable LDP on each interface, click the **Disabled** radio button.

Step 7 Click **Apply** to save the configuration.

Step 8 Return to your originating procedure (NTP).

Understanding MPLS LDP–IGP Synchronization

Packet loss can occur because the IGP and LDP are not synchronized. Packet loss can occur in the following situations:

- When an IGP adjacency is established, the router begins forwarding packets using the new adjacency before the LDP label exchange process completes between the peers on that link.
- If an LDP session closes, the router continues to forward traffic using the link that is associated with the LDP peer rather than an alternate pathway with a fully synchronized LDP session.

The MPLS LDP–IGP Synchronization feature performs the following tasks:

- Enables LDPs and IGPs to synchronize to minimize MPLS packet loss.
- Globally enables LDP–IGP synchronization on each interface that is associated with an IGP OSPF process.
- Disables LDP–IGP synchronization on interfaces that you do not want enabled.
- Prevents MPLS packet loss due to synchronization conflicts.
- Works when LDP is enabled on interfaces using either the **mpls ip** or **mpls ldp autoconfig** command or using the CTC procedure DLP-J118 Enable or Disable MPLS LDP Autoconfiguration Using CTC, on page 193.

If the LDP peer is reachable, the IGP waits indefinitely to synchronize. To limit the length of time an IGP session must wait to synchronize with LDP, enter the **mpls ldp igp sync holddown** command. If the LDP peer is not reachable, the IGP establishes the adjacency to enable the LDP session to be established.

When an IGP adjacency is established on a link but LDP–IGP synchronization is not yet achieved or is lost, the IGP advertises the max–metric on that link.

MPLS LDP–IGP Synchronization with Peers

When the MPLS LDP–IGP Synchronization feature is enabled on an interface, LDP determines if any peer connected by the interface is reachable by checking the peer transport address in the routing table. If a routing entry (including the longest match or the default routing entry) for the peer exists, LDP assumes that LDP–IGP synchronization is required for the interface and notifies the IGP to wait for LDP convergence.

LDP–IGP synchronization with peers requires the routing table to be accurate. If the routing table shows there is a route for the peer transport address, that route must be able to reach the peer transport address. However, if the route is a summary route, a default route, or a statically configured route, it may not the correct route for the peer. You must verify that the route in the routing table can reach the peer transport address.

When the routing table has an inaccurate route for the peer transport address, LDP cannot set up a session with the peer. This delay causes the IGP to wait for LDP convergence unnecessarily for the sync hold–down time.

MPLS LDP–IGP Synchronization Delay Timer

MPLS LDP–IGP Synchronization feature provides the option to configure a delay time for MPLS LDP and IGP synchronization for each interface. Normally, when LDP–IGP synchronization is configured, LDP notifies IGP as soon as LDP is converged. When the delay timer is configured, this notification is delayed.

When LDP is fully established and synchronized, LDP checks the delay timer:

- If you configured a delay time, LDP starts the timer. When the timer expires, LDP checks if the synchronization is still valid and notifies the OSPF process.
- If you did not configure a delay time or if synchronization is disabled or down or if an interface was removed from an IGP process, LDP stops the timer and immediately notifies the OSPF process.

- If you configure a new delay time while a timer is running, LDP saves the new delay time but does not reconfigure the running timer.

MPLS LDP–IGP Synchronization Incompatibility with IGP Nonstop Forwarding

The MPLS LDP–IGP Synchronization feature is not supported during the startup period if IGP Nonstop Forwarding (NSF) is configured. The MPLS LDP–IGP Synchronization feature conflicts with IGP NSF when the IGP is performing NSF during startup. After the NSF startup is complete, the MPLS LDP–IGP Synchronization feature is supported.

MPLS LDP–IGP Synchronization Compatibility with LDP Graceful Restart

LDP graceful restart protects traffic when an LDP session is lost. If an interface that supports a graceful–restart–enabled LDP session fails, MPLS LDP–IGP synchronization is still achieved on the interface while it is protected by Graceful Restart. MPLS LDP–IGP synchronization is eventually lost under the following circumstances:

- If LDP fails to restart before the LDP Graceful Restart reconnect timer expires.
- If an LDP session restarts through other interfaces, but the LDP session on the protected interface fails to recover when the LDP Graceful Restart recovery timer expires.

NTP-J44 Configure MPLS LDP–IGP Synchronization

Purpose	This procedure configures MPLS LDP–IGP synchronization.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J119 Enable MPLS LDP-IGP Synchronization Using Cisco IOS Commands, on page 196
- DLP-J120 Disable MPLS LDP-IGP Synchronization Using Cisco IOS Commands, on page 198
- DLP-J121 Verify MPLS LDP–IGP Synchronization Using Cisco IOS Commands, on page 199
- DLP-J122 Enable MPLS LDP-IGP Synchronization Using CTC, on page 201

Stop. You have completed this procedure.

DLP-J119 Enable MPLS LDP-IGP Synchronization Using Cisco IOS Commands

Purpose	This procedure enables LDP-IGP synchronization on each interface that is associated with an OSPF process. This procedure also limits the number of seconds that an IGP session must wait to synchronize with LDP. By default, the IGP session waits indefinitely if the LDP peer is reachable.
Tools/Equipment	None
Prerequisite Procedures	DLP-J115 Enable MPLS LDP Autoconfiguration Using Cisco IOS Commands, on page 188
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls ip** **Example:** Router(config)# mpls ip	Globally enables MPLS hop-by-hop forwarding.
Step 4	**mpls label protocol ldp** **Example:** Router(config)# mpls label protocol ldp	Specifies LDP as the default label distribution protocol.
Step 5	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.

	Command or Action	Purpose
Step 6	**ip address** *ip-address mask-value* **Example:** Router(config-if)# ip address 10.25.0.11 255.255.255.255	Assigns an IP address and network mask to the interface.
Step 7	**mpls ip** **Example:** Router(config-if)# mpls ip	Enables hop-by-hop forwarding on the interface.
Step 8	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode.
Step 9	**router ospf** *process-id* **Example:** Router(config)# router ospf 1	Enables OSPF routing and enters router configuration mode.
Step 10	**network** *ip-address wildcard-mask* **area** *area-id* **Example:** Router(config-router)# network 10.0.0.0 0.255.255.255 area 3	Defines an interface on which OSPF runs and defines the area ID for that interface.
Step 11	**mpls ldp sync** **Example:** Router(config-router)# mpls ldp sync	Enables MPLS LDP-IGP synchronization for interfaces for an OSPF process.
Step 12	**mpls ldp igp sync holddown** *milliseconds* **Example:** Router(config-router)# mpls ldp igp sync holddown 20	Specifies the period that an IGP session must wait to synchronize with LDP.
Step 13	**end** **Example:** Router(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.
Step 14	Return to your originating procedure (NTP).	—

DLP-J120 Disable MPLS LDP-IGP Synchronization Using Cisco IOS Commands

Purpose	This procedure disables LDP-IGP synchronization on each interface.
Tools/Equipment	None
Prerequisite Procedures	DLP-J115 Enable MPLS LDP Autoconfiguration Using Cisco IOS Commands, on page 188
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**no mpls ldp igp sync** **Example:** Router(config-if)# no mpls ldp igp sync	Disables MPLS LDP-IGP synchronization for that interface.
Step 5	**end** **Example:** Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J121 Verify MPLS LDP–IGP Synchronization Using Cisco IOS Commands

Purpose	This procedure verifies LDP-IGP synchronization on each interface.
Tools/Equipment	None
Prerequisite Procedures	DLP-J115 Enable MPLS LDP Autoconfiguration Using Cisco IOS Commands, on page 188
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

After you configure the interfaces for LDP, OSPF, and LDP–IGP synchronization, verify that the configuration is working correctly using the **show mpls ldp igp sync** and **show ip ospf mpls ldp interface** commands.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**show mpls ldp igp sync** [**all** | **interface** *type number*]
	
	Example:
	Router# show mpls ldp igp sync
		Displays the output of this command in the following example shows that MPLS LDP–IGP synchronization is configured correctly, because LDP is configured and the SYNC status shows that synchronization is enabled.
		
		`TenGigabitEthernet4/1:`
		`  LDP configured; SYNC enabled.`
		`  SYNC status: sync achieved; peer reachable.`
		
		`  IGP holddown time: infinite.`
		`  Peer LDP Ident: 10.0.0.1:0`
		`  IGP enabled: OSPF 1`

Step 3	**show ip ospf** [*process-id*] **mpls ldp interface** [*interface*]
	
	Example:
	Router# show ip ospf mpls ldp interface
		Displays the output of the **show ip ospf mpls ldp interface** command in the following example shows that the interfaces are properly configured.
		
		`TenGigabitEthernet4/1`
		`  Process ID 1, Area 0`
		`  LDP is configured through LDP autoconfig`
		`  LDP-IGP Synchronization: Yes`
		`  Holddown timer is not configured`

	Command or Action	Purpose
		Timer is not running TenGigabitEthernet4/2 Process ID 1, Area 0 LDP is configured through LDP autoconfig LDP-IGP Synchronization: Yes Holddown timer is not configured Timer is not running
Step 4	Return to your originating procedure (NTP).	—

Example of MPLS LDP-IGP Synchronization

The following configuration commands enable LDP for OSPF process 1. The **mpls ldp sync** command and the OSPF **network** commands enable LDP on interfaces TenGigabitEthernet0/0, TenGigabitEthernet0/1, and TenGigabitEthernet1/1, respectively. The **no mpls ldp igp sync** command on interface TenGigabitEthernet1/0 prevents LDP from being enabled on interface TenGigabitEthernet1/0, even though OSPF is enabled for that interface.

```
Router# configure terminal
Router(config)# interface TenGigabitEthernet0/0
Router(config-if)# ip address 10.0.0.1
Router(config-if)# mpls ip
!
Router(config)# interface TenGigabitEthernet0/1
Router(config-if)# ip address 10.0.1.1
Router(config-if)# mpls ip
!
Router(config)# interface TenGigabitEthernet1/1
Router(config-if)# ip address 10.1.1.1
Router(config-if)# mpls ip
!
Router(config)# interface TenGigabitEthernet1/0
Router(config-if)# ip address 10.1.0.1
Router(config-if)# mpls ip
!
Router(config)# router ospf 1
Router(config-router)# network 10.0.0.0 0.0.255.255 area 3
Router(config-router)# network 10.1.0.0 0.0.255.255 area 3
Router(config-router)# mpls ldp sync
Router(config-router)# exit
Router(config)# interface TenGigabitEthernet1/0
Router(config-if)# no mpls ldp igp sync
```

DLP-J122 Enable MPLS LDP-IGP Synchronization Using CTC

Purpose	This procedure enables LDP-IGP synchronization on each interface that is associated with an OSPF process. This procedure also limits the number of seconds that an IGP session must wait to synchronize with LDP. By default, the IGP session waits indefinitely if the LDP peer is reachable.
Tools/Equipment	None
Prerequisite Procedures	DLP-J118 Enable or Disable MPLS LDP Autoconfiguration Using CTC, on page 193
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This feature is supported only on interfaces that are running OSPF processes.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to enable LDP-IGP synchronization.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **Control Plane**.

Step 5 Click the **OSPF** tab.

Step 6 In the LDP Synchronization area, check the **Enabled** check box to enable LDP-IGP synchronization on all the interfaces that belong to an OSPF process.

Step 7 Enter the number of seconds in the Holddown field to specify the period that an IGP session must wait to synchronize with LDP.

Step 8 Click **Apply** to save the configuration.

Step 9 Return to your originating procedure (NTP).

Understanding MPLS LDP Backoff

The LDP backoff mechanism prevents two LSRs that were configured incompatibly from engaging in an unthrottled sequence of session setup failures. For example, an incompatibility arises when two neighboring routers attempt to perform LC-ATM (label-controlled ATM) when they are using different ranges of VPI/VCI values for labels.

If a session setup attempt fails due to an incompatibility, each LSR delays its next attempt (that is, backs off), increasing the delay exponentially with each successive failure until the maximum backoff delay is reached.

The default settings correspond to the lowest settings for initial and maximum backoff values defined by the LDP protocol specification. You should change the settings from the default values only if such settings result in undesirable behavior.

NTP-J45 Configure MPLS LDP Backoff

Purpose	This procedure configures MPLS LDP backoff.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J123 Configure MPLS LDP Backoff Using Cisco IOS Commands, on page 202
- DLP-J124 Configure MPLS LDP Backoff Using CTC, on page 203

Stop. You have completed this procedure.

DLP-J123 Configure MPLS LDP Backoff Using Cisco IOS Commands

Purpose	This procedure configures the parameters for MPLS LDP backoff mechanism using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed

Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls ldp backoff** *initial-backoff maximum-backoff* **Example:** Router(config)# mpls ldp backoff 10 30	Configures MPLS LDP backoff mechanism and specifies the period for initial and maximum backoff. The valid range is from 5 to 2147483.
Step 4	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 5	Return to your originating procedure (NTP).	—

DLP-J124 Configure MPLS LDP Backoff Using CTC

Purpose	This procedure configures the parameters for MPLS LDP backoff mechanism.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to configure the parameters for LDP backoff.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **LDP**.

Step 5 In the Session area, enter the number of seconds in the Holdtime field to specify the period for which an LDP session is maintained in the absence of LDP messages from the session peer.

Step 6 Enter the number of seconds in the Init Backoff field to specify the period for the initial backoff.

Step 7 Enter the number of seconds in the Max Backoff field to specify the period for the maximum backoff.

Step 8 Click **Apply** to save the configuration.

Step 9 Return to your originating procedure (NTP).

Understanding MPLS LDP Session Protection

The MPLS LDP Session Protection feature provides faster label distribution protocol convergence when a link recovers following an outage. MPLS LDP Session Protection feature protects an LDP session between directly connected neighbors or an LDP session established for a TE tunnel.

MPLS LDP Session Protection feature maintains LDP bindings when a link fails. MPLS LDP sessions are protected through the use of LDP Hello messages. When you enable MPLS LDP, the LSRs send messages to find other LSRs with which they can create LDP sessions.

LDP graceful restart must be enabled before establishing a LDP session.

Directly Connected MPLS LDP Sessions

If the LSR is one hop from its neighbor, it is directly connected to its neighbor. The LSR sends out LDP Hello messages as User Datagram Protocol (UDP) packets to all the routers on the subnet. The hello message is called an LDP Link Hello. A neighboring LSR responds to the hello message and the two routers begin to establish an LDP session. This is called basic discovery.

To initiate an LDP session between routers, the routers determine which router will take the active role and which router will take the passive role. The router that takes the active role establishes the LDP TCP connection session and initiates the negotiation of the LDP session parameters. To determine the roles, the two routers compare their transport addresses. The router with the higher IP address takes the active role and establishes the session.

After the LDP TCP connection session is established, the LSRs negotiate the session parameters, including the method of label distribution to be used. Two methods are available:

- Downstream Unsolicited—An LSR advertises label mappings to peers without being asked to.
- Downstream on Demand—An LSR advertises label mappings to a peer only when the peer asks for them.

NTP-J46 Configure MPLS LDP Session Protection

Purpose	This procedure configures MPLS LDP session protection.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J125 Enable MPLS LDP Session Protection Using Cisco IOS Commands, on page 205
- DLP-J126 Verify MPLS LDP Session Protection Using Cisco IOS Commands, on page 207
- DLP-J127 Enable MPLS LDP Session Protection Using CTC, on page 209
- DLP-J128 Enable Directly Connected LDP Sessions Using Cisco IOS Commands, on page 210
- DLP-J130 Create Targeted LDP Sessions Using CTC, on page 211
- DLP-J131 Configure MPLS LDP Discovery Using CTC, on page 212
- DLP-J132 Enable Explicit Null Label Using Cisco IOS Commands, on page 213
- DLP-J133 Enable Explicit Null Label Using CTC, on page 215

Stop. You have completed this procedure.

DLP-J125 Enable MPLS LDP Session Protection Using Cisco IOS Commands

Purpose	This procedure enables MPLS LDP Session Protection. This procedure enables LDP sessions to be protected during a link failure.
Tools/Equipment	None

Prerequisite Procedures	• LSRs must be able to respond to LDP targeted hellos. Otherwise, the LSRs cannot establish a targeted adjacency. • All routers that participate in MPLS LDP Session Protection must be enabled to respond to targeted hellos. • Both neighbor routers must be configured for session protection or one router must be configured for session protection and the other router must be configured to respond to targeted hellos.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ip cef** [**distributed**] **Example:** Router(config)# ip cef	Configures Cisco Express Forwarding.
Step 4	**interface** *loopbacknumber* **Example:** Router(config)# interface loopback0	Configures a loopback interface and enters interface configuration mode.
Step 5	**ip address** *ip-address mask-value* **Example:** Router(config-if)# ip address 10.25.0.11 255.255.255.255	Assigns an IP address and network mask to the loopback interface.

	Command or Action	Purpose
Step 6	**interface** *type number* **Example:** Router(config-if)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 7	**mpls ip** **Example:** Router(config-if)# mpls ip	Configures MPLS hop-by-hop forwarding for a specified interface.
Step 8	**mpls label protocol ldp** **Example:** Router(config-if)# mpls label protocol ldp	Configures the use of LDP on a specific interface.
Step 9	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode and enters global configuration mode.
Step 10	**mpls ldp session protection** [**for acl**] [**duration** {**infinite** | *seconds*}] **Example:** Router(config)# mpls ldp session protection	Enables MPLS LDP Session Protection. The range is from 30 to 2147483 seconds.
Step 11	Return to your originating procedure (NTP).	—

DLP-J126 Verify MPLS LDP Session Protection Using Cisco IOS Commands

Purpose	This procedure verifies MPLS LDP Session Protection.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose

Step 1	**show mpls ldp discovery [all] [detail]**
	
	Example:
	Router# show mpls ldp discovery
		Use this command and check that the output contains xmit/recv to the peer router.
		
		`Local LDP Identifier:`
		`  10.0.0.5:0`
		`  Discovery Sources:`
		`  Interfaces:`
		`  TenGigabitEthernet4/1 (ldp): xmit/recv`
		
		`  LDP Id: 10.0.0.1:0`
		`  Targeted Hellos:`
		`  10.0.0.5 -> 10.0.0.3 (ldp): active, xmit/recv`
		`  LDP Id: 10.0.0.3:0`

Step 2	**show mpls ldp neighbor** [**all**] [*address* | *interface*] [**detail**] [**graceful-restart**]
	
	Example:
	Router# show mpls ldp neighbor
		Use this command to check that the targeted hellos are active.
		
		`Peer LDP Ident: 10.0.0.3:0; Local LDP Ident 10.0.0.5:0`
		`TCP connection: 10.0.0.3.646 - 10.0.0.5.11005`
		`State: Oper; Msgs sent/rcvd: 1453/1464; Downstream`
		`Up time: 21:09:56`
		`LDP discovery sources:`
		`  Targeted Hello 10.0.0.5 -> 10.0.0.3, active`
		`Addresses bound to peer LDP Ident:`
		`  10.3.104.3  10.0.0.2  10.0.0.3`

Step 3	**show mpls ldp neighbor** [**all**] [*address* | *interface*] [**detail**] [**graceful-restart**]
	
	Example:
	Router# show mpls ldp neighbor detail
		Use this command to check that the MPLS LDP Session Protection state is Ready or Protecting. If the second last line of the output shows Incomplete, the Targeted Hello Adjacency is not up yet.
		
		`Peer LDP Ident: 10.16.16.16:0; Local LDP Ident 10.15.15.15:0`
		`  TCP connection: 10.16.16.16.11013 - 10.15.15.15.646`
		`  State: Oper; Msgs sent/rcvd: 53/51; Downstream; Last TIB rev sent 74`
		`  Up time: 00:11:32; UID: 1; Peer Id 0;`
		`  LDP discovery sources:`
		`  Targeted Hello 10.15.15.15 -> 10.16.16.16, active, passive;`
		`  holdtime: infinite, hello interval: 10000 ms`
		`  Addresses bound to peer LDP Ident:`
		`  10.0.0.2  10.16.16.16 10.101.101.101  11.0.0.1`
		`  Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab`

	Command or Action	Purpose

		`Clients: Dir Adj Client`
		`LDP Session Protection enabled, state: Protecting`
		`duration: infinite`

Step 4	Return to your originating procedure (NTP).	—

DLP-J127 Enable MPLS LDP Session Protection Using CTC

Purpose	This procedure enables MPLS LDP session protection and configures its parameters.
Tools/Equipment	None
Prerequisite Procedures	DLP-J135 Configure MPLS LDP Graceful Restart Using CTC, on page 218
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to configure MPLS LDP session protection.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **LDP.**

Step 5 In the Protection area, check the **Enabled** check box to enable MPLS LDP session protection.

Step 6 Click the **Infinite** radio button to enable session protection for infinite duration or enter the number of seconds in the Duration field to specify the period for which the LDP Targeted Hello Adjacency must be retained after a link is lost.

Step 7 Click **Apply** to save the configuration.

DLP-J128 Enable Directly Connected LDP Sessions Using Cisco IOS Commands

Purpose	This procedure configures MPLS LDP sessions between two directly connected routers.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls ip** **Example:** Router(config)# mpls ip	Configures MPLS hop-by-hop forwarding globally.
Step 4	**mpls label protocol ldp** **Example:** Router(config)# mpls label protocol ldp	Configures the use of LDP on all the interfaces.
Step 5	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 6	**mpls ip** **Example:** Router(config-if)# mpls ip	Configures MPLS hop-by-hop forwarding on the interface.

	Command or Action	Purpose
Step 7	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode and enters the global configuration mode.
Step 8	**exit** **Example:** Router(config)# exit	Exits global configuration mode and enters privileged EXEC mode.
Step 9	**show mpls interfaces** [*interface*] [**all**] [**detail**] [**internal**] **Example:** Router# show mpls interfaces	Verifies that the interfaces have been configured to use LDP.
Step 10	**show mpls ldp discovery** [**all**] | [**detail**] **Example:** Router# show mpls ldp discovery	Verifies that the interface is up and is sending Discovery Hello messages.
Step 11	**show mpls ldp neighbor** [**all**] [*address* | *interface*] [**detail**] [**graceful-restart**] **Example:** Router# show mpls ldp neighbor	Displays the status of LDP sessions.
Step 12	Return to your originating procedure (NTP).	—

DLP-J130 Create Targeted LDP Sessions Using CTC

Purpose	This procedure creates targeted LDP sessions using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to create targeted LDP sessions.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **LDP**.

Step 5 In the Targeted LDP Sessions area, click **Create**.
The **Create Targeted LDP Session** dialog box appears.

Step 6 Enter the IP address of the neighboring router in the IP Address field and click **OK**.

Step 7 Return to your originating procedure (NTP).

DLP-J131 Configure MPLS LDP Discovery Using CTC

Purpose	This procedure configures the holdtime and interval between transmission of consecutive LDP discovery hello messages or discovery targeted hello messages between LSRs.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Use the fields in the Hello area to configure the holdtime and interval for LSRs that are directly connected.
- Use the fields in the Targeted Hello area to configure the holdtime and interval for LSRs that are not directly connected.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to configure holdtime and interval for LSRs that are directly connected and indirectly connected.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **LDP.**

Step 5 In the Hello area, enter the number of seconds in the Holdtime field to specify the period a discovered LDP neighbor must wait without receiving a LDP hello message from the neighbor.

Step 6 Enter the number of seconds in the Interval field to specify the period between the sending of consecutive hello messages.

Step 7 In the Targeted Hello area, enter the number of seconds in the Holdtime field to specify the period a discovered LDP neighbor must wait without receiving a LDP targeted hello message from the neighbor.

Step 8 Enter the number of seconds in the Interval field to specify the period between the sending of consecutive targeted hello messages.

Step 9 Click **Apply** to save the configuration.

Step 10 Return to your originating procedure (NTP).

Understanding Explicit Null Label

Normally, LDP advertises an implicit null label for directly connected routes. The implicit null label causes the second last (penultimate) LSR to remove the MPLS header from the packet. In this case, the penultimate LSR and the last LSR do not have access to the quality of service (QoS) values that the packet carried before the MPLS header was removed. To preserve the QoS values, you can configure the LSR to advertise an explicit null label (a label value of zero). The LSR at the penultimate hop forwards MPLS packets with a null label instead of forwarding IP packets.

Note An explicit null label is not needed when the penultimate hop receives MPLS packets with a label stack that contains at least two labels and penultimate hop popping (PHP) is performed. In that case, the inner label can still carry the QoS value needed by the penultimate and edge LSR to implement their QoS policy.

DLP-J132 Enable Explicit Null Label Using Cisco IOS Commands

Purpose	This procedure enables explicit null label using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls ip** **Example:** Router(config)# mpls ip	Configures MPLS hop-by-hop forwarding globally.
Step 4	**mpls label protocol ldp** **Example:** Router(config)# mpls label protocol ldp	Configures the use of LDP on all the interfaces.
Step 5	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure and enters interface configuration mode.
Step 6	**mpls ip** **Example:** Router(config-if)# mpls ip	Configures MPLS hop-by-hop forwarding on the interface.
Step 7	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode and enters global configuration mode.
Step 8	**mpls ldp explicit-null [for** *prefix-acl* | **to** *peer-acl* | **for** *prefix-acl* **to** *peer-acl*] **Example:** Router(config)# mpls ldp explicit-null	Advertises an explicit null label in situations where it would normally advertise an implicit null label.

	Command or Action	Purpose
Step 9	**exit** **Example:** Router(config)# exit	Exits global configuration mode and enters privileged EXEC mode.
Step 10	Return to your originating procedure (NTP).	—

DLP-J133 Enable Explicit Null Label Using CTC

Purpose	This procedure enables explicit null label using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to enable the explicit null label.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **LDP**.

Step 5 In the Explicit Null Label area, check the **Enabled** check box to advertise an explicit null label in situations where it would normally advertise an implicit null label.

Step 6 Click **Apply** to save the changes.

Step 7 Return to your originating procedure (NTP).

Understanding LDP Graceful Restart

LDP graceful restart protects traffic when a LDP session is lost. If an interface that supports a graceful-restart-enabled LDP session fails, MPLS LDP-IGP synchronization is still achieved on the interface while it is protected by graceful restart.

LDP graceful restart must be enabled in the following scenarios:

- Before establishing a LDP session.
- Dynamic pseudowire check point.
- When LDP or RSVP–TE uses a standby fabric port.

NTP-J47 Configure MPLS LDP Graceful Restart

Purpose	This procedure configures MPLS LDP graceful restart.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J134 Configure MPLS LDP Graceful Restart Using Cisco IOS Commands, on page 216
- DLP-J135 Configure MPLS LDP Graceful Restart Using CTC, on page 218

Stop. You have completed this procedure.

DLP-J134 Configure MPLS LDP Graceful Restart Using Cisco IOS Commands

Purpose	This procedure configures the parameters for MPLS LDP graceful restart using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls ldp graceful-restart** **Example:** Router(config)# mpls ldp graceful-restart	Enables MPLS LDP graceful restart.
Step 4	**mpls ldp graceful-restart timers forwarding-holding** *seconds* **Example:** Router(config)# mpls ldp graceful-restart timers forwarding-holding 10	Specifies the period the MPLS forwarding state must hold after the control plane restarts.
Step 5	**mpls ldp graceful-restart timers max-recovery** *seconds* **Example:** Router(config)# mpls ldp graceful-restart timers max-recovery 20	Specifies the period a LSR must hold stale label-forward error correction (FEC) bindings after an LDP session has been reestablished.
Step 6	**mpls ldp graceful-restart timers neighbor-liveness** *seconds* **Example:** Router(config)# mpls ldp graceful-restart timers neighbor-liveness 15	Specifies the period a LSR must wait for an LDP session to be reestablished.
Step 7	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 8	Return to your originating procedure (NTP).	—

DLP-J135 Configure MPLS LDP Graceful Restart Using CTC

Purpose	This procedure configures the parameters for MPLS LDP graceful restart.
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 NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to configure the parameters for MPLS LDP graceful restart.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **LDP.**

Step 5 In the Graceful Restart area, check the **Enabled** check box to enable MPLS LDP graceful restart.

Step 6 Enter the number of seconds in the Forwarding holding field to specify the period the MPLS forwarding state must hold after the control plane restarts.

Step 7 Enter the number of seconds in the Max recovery field to specify the period a LSR must hold stale label-FEC bindings after an LDP session has been reestablished.

Step 8 Enter the number of seconds in the Neighbor liveliness field to specify the period a LSR must wait for an LDP session to be reestablished.

Step 9 Click **Apply** to save the configuration.
Enable OSPF NSF for LDP graceful restart to effectively minimize traffic hits. See DLP-J209 Configure NSF for OSPF Using CTC, on page 178.

Step 10 Return to your originating procedure (NTP).

Examples of Show MPLS Commands

show mpls interfaces

The following **show mpls interfaces** command output shows that the interfaces TenGigabitEthernet4/1 and TenGigabitEthernet4/2 have been configured to use LDP:

```
Router# show mpls interfaces
```

```
Interface    IP         Tunnel    BGP    Static    Operational
TenGigabitEthernet4/1  Yes (ldp)  No       No      No          Yes
TenGigabitEthernet4/2  Yes         No       No      No          Yes
```

show mpls ldp discovery

The following **show mpls ldp discovery** command output shows that the interface is up and is sending LDP Discovery Hello messages.

```
Router# show mpls ldp discovery
```

```
Local LDP Identifier:
   172.16.12.1:0
   Discovery Sources:
   Interfaces:
       TenGigabitEthernet4/1 (ldp): xmit
```

show mpls ldp neighbor

The following **show mpls ldp neighbor** command output shows that the LDP session between routers is successfully established:

```
Router# show mpls ldp neighbor
```

```
Peer LDP Ident: 10.1.1.2:0; Local LDP Ident 10.1.1.1:0
   TCP connection: 10.1.1.2.18 - 10.1.1.1.66
   State: Oper; Msgs sent/rcvd: 12/11; Downstream
   Up time: 00:00:10
   LDP discovery sources:
   TenGigabitEthernet4/1, Src IP addr: 10.20.10.2
   Addresses bound to peer LDP Ident:
   10.1.1.2  10.20.20.1  10.20.10.2
```

Understanding MPLS-TE

Traffic Engineering is a set of techniques and processes used to cause routed traffic to travel through the network on a path other than the one that is chosen if standard routing methods were used. Traffic Engineering is the ability to dynamically define routes based on known demand or alternate available routes.

MPLS Traffic Engineering (MPLS–TE) is the use of label switching to improve traffic performance along with an efficient use of network resources. MPLS–TE is the process of adjusting bandwidth allocations to ensure that enough bandwidth is left for high priority traffic. In MPLS–TE, the upstream router creates a network tunnel for a particular traffic stream and sets the bandwidth available for that tunnel.

CPT supports OSPF and OSPF-TE in this release.

You can specify the IP address assigned to an interface as the source IP address for control packets. The default behavior is to use the router ID configured in the Interior Gateway Protocol (IGP) using the **mpls traffic-eng router-id** command.

When you configure an MPLS TE tunnel, the address specified in the **tunnel source** command is used as the source IP address for control traffic to signal the tunnel. The source IP address overrides the default IP address taken from the IGP **mpls traffic-eng router-id** command.

The traffic engineering router ID for the node is the IP address associated with the loopback interface. The router ID is not editable.

NTP-J48 Configure MPLS-TE Parameters

Purpose	This procedure configures the parameters for MPLS–TE tunnel.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J136 Configure MPLS and RSVP to Support Traffic Engineering Using Cisco IOS Commands , on page 220
- DLP-J137 Enable MPLS-TE on a System and on Specific Interfaces Using CTC, on page 222
- DLP-J140 Enable RSVP Graceful Restart on an Interface Using Cisco IOS Commands, on page 222
- DLP-J141 Enable RSVP Graceful Restart on an Interface Using CTC, on page 224
- DLP-J142 Configure MPLS-TE Parameters for Each Interface Using CTC, on page 224
- DLP-J143 Change the Periodic Flooding Timer Using Cisco IOS Commands, on page 225
- DLP-J144 Change the Periodic Flooding Timer Using CTC, on page 226

Stop. You have completed this procedure.

DLP-J136 Configure MPLS and RSVP to Support Traffic Engineering Using Cisco IOS Commands

Purpose	This procedure configures MPLS and Resource Reservation Protocol (RSVP) to support traffic engineering on the routers.
Tools/Equipment	None
Prerequisite Procedures	None

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ip cef** **Example:** Router(config)# ip cef	Enables Cisco Express Forwarding.
Step 4	**mpls traffic-eng tunnels** **Example:** Router(config)# mpls traffic-eng tunnels	Enables MPLS traffic engineering tunnel signaling on a device.
Step 5	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface and enters interface configuration mode.
Step 6	**ip address** *ip-address mask-value* **Example:** Router(config-if)# ip address 192.168.10.10 255.255.255.255	Assigns an IP network address and network mask to the interface.
Step 7	**ip rsvp bandwidth** or **ip rsvp bandwidth** *value* or **ip rsvp bandwidth percent** *value* **Example:** Router(config-if)# ip rsvp bandwidth 100	Enables RSVP for IP on an interface to support traffic engineering.
Step 8	**end** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 9	Return to your originating procedure (NTP).	—

DLP-J137 Enable MPLS-TE on a System and on Specific Interfaces Using CTC

Purpose	This procedure enables MPLS-TE tunnel signaling globally on a system and on the desired interfaces.
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 NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to enable MPLS-TE.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **MPLS TE**.

Step 5 Click the **Link TE Attrs** tab.

Step 6 Check the **Enabled** check box at the top to globally enable MPLS-TE tunnel signaling on the system.

Step 7 In the Interfaces area, check the **Enabled** check box for interfaces that you want to enable MPLS-TE tunnel signaling.

Step 8 Click **Apply** to save the configuration.

Step 9 Return to your originating procedure (NTP).

DLP-J140 Enable RSVP Graceful Restart on an Interface Using Cisco IOS Commands

Purpose	This procedure enables RSVP graceful restart on an interface using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None

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

Note You must repeat this procedure for each interface in the neighboring router.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode. Repeat this step as needed to configure the additional interfaces.
Step 4	**ip rsvp signalling hello graceful-restart neighbor** *ip-address* **Example:** Router(config-if)# ip rsvp signalling hello graceful-restart neighbor 10.0.0.0	Enables support for RSVP graceful restart on routers helping their neighbors recover TE tunnels following Stateful Switchover (SSO). Repeat this step as needed to configure additional IP addresses on the interfaces of the neighboring router. **Note** The IP address must be that of the interface of the neighboring router.
Step 5	**exit** **Example:** Router(config-if)# exit	Returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J141 Enable RSVP Graceful Restart on an Interface Using CTC

Purpose	This procedure enables RSVP graceful restart on an interface using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J209 Configure NSF for OSPF Using CTC, on page 178
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to enable RSVP graceful restart on an interface.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **MPLS-TE**.

Step 5 Click the **RSVP-TE** tab.

Step 6 Enter the number of seconds in the Frequency field.

Step 7 In the Graceful Restart area, complete the following:

a) From the Graceful Restart Mode drop-down list, choose **Unprovisioned**, **Full**, or **Help Neighbor**.

b) In the Interfaces area, check the **RSVP Hello Graceful Restart** check box for the interfaces as needed.

Step 8 Click **Apply** to enable RSVP graceful restart on the desired interfaces.

Step 9 Return to your originating procedure (NTP).

DLP-J142 Configure MPLS-TE Parameters for Each Interface Using CTC

Purpose	This procedure configures MPLS-TE parameters for each interface.
Tools/Equipment	None
Prerequisite Procedures	DLP-J137 Enable MPLS-TE on a System and on Specific Interfaces Using CTC, on page 222
Required/As Needed	As needed

Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to configure MPLS-TE parameters for each interface.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **MPLS TE**.

Step 5 Click the **Link TE Attrs** tab.

Step 6 For interfaces that you have enabled MPLS-TE tunnel signaling:

a) Enter the bandwidth in kilobits per second that can be reserved for the interface in the Bandwidth field.

b) Enter the user-specified attribute flags for the interface in the Attribute Flag field.

Note These attributes will be compared to the affinity bits of the tunnel during selection of a path. The valid range is from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits) where the value of an attribute is 0 or 1.

c) Enter the TE metric value for the interface configured using MPLS-TE in the TE Metric field.

d) Enter a value in the SRLG field to configure the Shared Risk Link Group (SRLG) membership for the interface. The valid range is from 0 to 4294967295.

Step 7 Click **Apply** to save the configuration.

Step 8 Return to your originating procedure (NTP).

Understanding Periodic Flooding Timer

When a threshold is crossed, the MPLS traffic engineering link management advertises updated link information. If no thresholds are crossed, changes can be flooded periodically unless periodic flooding is disabled.

Changes in the MPLS TE topology database are flooded by the link state IGP. Some changes, such as those to link status (up or down) or configured parameters, trigger immediate flooding. Other changes are considered less urgent and are flooded periodically. For example, changes to the amount of link bandwidth allocated to TE tunnels are flooded periodically unless the change causes the bandwidth to cross a configurable threshold.

DLP-J143 Change the Periodic Flooding Timer Using Cisco IOS Commands

Purpose	This procedure sets the interval for periodic flooding of traffic engineering topology information using Cisco IOS commands.
Tools/Equipment	None

Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls traffic-eng link-management timers periodic-flooding** *interval* **Example:** Router(config)# mpls traffic-eng link-management timers periodic-flooding 25	Changes the interval used for periodic flooding. The default value is 180 seconds. The range is from 0 to 3600 seconds. A value of 0 turns off periodic flooding. If you set this value anywhere in the range from 1 to 29, it is treated as 30.
Step 4	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 5	Return to your originating procedure (NTP).	—

DLP-J144 Change the Periodic Flooding Timer Using CTC

Purpose	This procedure sets the interval for periodic flooding of traffic engineering topology information.
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 NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to change the periodic flooding timer.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **MPLS TE**.

Step 5 Click the **Link TE Attrs** tab.

Step 6 Enter the value in seconds, in the Periodic Flooding field to change the interval used for periodic flooding. The default value is 180 seconds. The range is 0 to 3600 seconds. A value of 0 turns off periodic flooding. If you set this value anywhere in the range from 1 to 29 seconds, it is treated as 30 seconds.

Step 7 Click **Apply** to save the configuration.

Step 8 Return to your originating procedure (NTP).

Understanding MPLS–TE LSP Attributes

The MPLS Traffic Engineering—LSP Attributes provides an LSP Attribute List feature and a Path Option for Bandwidth Override feature. These features have the following benefits:

- The LSP Attributes List feature provides the ability to configure values for several LSP–specific path options for TE tunnels.
- One or more TE tunnels can specify specific path options by referencing an LSP attribute list.
- The Path Option for Bandwidth Override feature provides a single command that allows a TE tunnel to fall back temporarily to path options that can reduce bandwidth constraints.

Note You can configure LSP attributes for path options associated with MPLS TE tunnels only through Cisco IOS commands and not through CTC.

Several LSP attributes can be applied to path options for TE tunnels using an LSP attribute list. If bandwidth is the only LSP attribute you require, then you can configure a path option for bandwidth override.

Prerequisites

Before configuring either an LSP Attribute List or a Path Option for Bandwidth Override feature, you must configure a MPLS TE tunnel.

Traffic Engineering Bandwidth and Bandwidth Pools

MPLS TE allows constraint–based routing (CBR) of IP traffic. One of the constraints satisfied by CBR is the availability of required bandwidth over a selected path. Regular TE tunnel bandwidth is called the global pool.

You can configure the LSP Attributes bandwidth path option to use the global pool bandwidth. The bandwidth value for the path option may be any valid value and the pool does not have to be the same as that configured on the tunnel.

Autobandwidth and Path Option for Bandwidth Override

If Traffic Engineering automatic bandwidth (autobandwidth) adjustment is configured for a tunnel, traffic engineering automatically adjusts the bandwidth allocation for the traffic engineering tunnel based on its measured usage of the bandwidth of the tunnel.

Traffic engineering autobandwidth samples the average output rate for each tunnel marked for automatic bandwidth adjustment. For each marked tunnel, it periodically adjusts the allocated bandwidth for the tunnel to be the largest sample for the tunnel since the last adjustment. The default reoptimization setting in the MPLS AutoBandwidth feature is every 24 hours.

The frequency at which the tunnel bandwidth is adjusted and the allowable range of adjustments is configured on a per–tunnel basis. In addition, the sampling interval and the interval over which to average tunnel traffic to obtain the average output rate is user–configurable on a per–tunnel basis.

The automatic bandwidth feature allows you to configure and monitor the bandwidth for MPLS TE tunnels. If automatic bandwidth is configured for a tunnel, TE automatically adjusts the tunnel bandwidth.

The Path Option for Bandwidth Override feature allows you to override the bandwidth configured on a TE tunnel. This feature also overrides bandwidth configured or recalculated by automatic bandwidth adjustment if the path option in effect has bandwidth override enabled.

Constraint–Based Routing and Path Option Selection

MPLS traffic engineering automatically establishes and maintains LSPs across the network by using the RSVP. The path that an LSP uses is determined by the LSP resource requirements and network resources, such as bandwidth. Traffic engineering tunnels are calculated at the LSP head based on a fit between required and available resources (constraint–based routing).

Without the Path Option for Bandwidth Override feature, a TE tunnel establishes an LSP based on dynamic or explicit path options in order of preference. However, the bandwidth and other attributes configured on the TE tunnel allow the setup of an LSP only if LSP path options satisfy the constraints. If a path that satisfies the configured path options cannot be found, then the tunnel is not set up.

The Path Option for Bandwidth Override feature provides a fallback path option that allows overriding the bandwidth configured on the TE tunnel interface. For example, you can configure a path option that sets the bandwidth to zero effectively removing the bandwidth constraint imposed by the constraint–based routing calculation.

Tunnel Reoptimization and Path Option Selection

Reoptimization occurs when a device with traffic engineering tunnels periodically examines tunnels with established LSPs to learn if better LSPs are available. If a better LSP is available, the device attempts to signal the better LSP. If the signaling is successful, the device replaces the older LSP with the new LSP.

Reoptimization can be triggered by a timer, the **mpls traffic–eng reoptimize** command, or a configuration change that requires the resignalling of a tunnel. The MPLS AutoBandwidth feature, for example, uses a timer to set the frequency of reoptimization based on the bandwidth path option attribute. The Path Option for

Bandwidth Override feature allows for the switching between bandwidth configured on the TE tunnel interface and bandwidth configured on a specific path option. This increases the success of signaling an LSP for the TE tunnel.

With bandwidth override configured on a path option, traffic engineering attempts to reoptimize the bandwidth every 30 seconds to reestablish the bandwidth configured on the tunnel.

Path Option Selection with Bandwidth Override

The Path Option for Bandwidth Override feature allows you to configure bandwidth parameters on a specific path option using the **bandwidth** keyword in the **tunnel mpls traffic–eng path–option** command. When an LSP is signaled using a path option with a configured bandwidth, the bandwidth associated with the path option is signaled instead of the bandwidth configured directly on the tunnel.

This feature provides you with the ability to configure multiple path options that reduce the bandwidth constraint each time the headend of a tunnel fails to establish an LSP.

Explicit and Dynamic Path Options

You can configure multiple path options for a single tunnel. For example, there can be several explicit path options and a dynamic option for one tunnel.

If you specify the **dynamic** keyword, the physical bandwidth of the interface and the available TE bandwidth are checked to ensure that the requested amount of bandwidth does not exceed the physical bandwidth of any link. To oversubscribe links, you must specify the **explicit** keyword. If you use the **explicit** keyword, the amount of bandwidth that is available on the link for TE is only checked; the amount of bandwidth you configure is not limited to how much physical bandwidth is available on the link.

NTP-J49 Configure MPLS-TE LSP Attributes

Purpose	This procedure configures LSP attributes for MPLS–TE.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J145 Add Attributes to an LSP Attribute List Using Cisco IOS Commands, on page 230
- DLP-J146 Associate an LSP Attribute List with a Path Option for an MPLS TE Tunnel Using Cisco IOS Commands, on page 232
- DLP-J147 Configure an LSP Attribute List Using Cisco IOS Commands, on page 235

- DLP-J148 Modify an Attribute in an LSP Attribute List Using Cisco IOS Commands, on page 238
- DLP-J149 Remove an Attribute from an LSP Attribute List Using Cisco IOS Commands, on page 240
- DLP-J150 Delete an LSP Attribute List Using Cisco IOS Commands, on page 242
- DLP-J151 Verify Attributes Within an LSP Attribute List Using Cisco IOS Commands, on page 243
- DLP-J152 Verify All LSP Attribute Lists Using Cisco IOS Commands, on page 244

Stop. You have completed this procedure.

DLP-J145 Add Attributes to an LSP Attribute List Using Cisco IOS Commands

Purpose	This procedure adds attributes to an LSP attribute list using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

LSP Attributes configuration mode is used to display the specific LSP attributes list and to add or change the required path option attribute.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls traffic-eng lsp attributes** *string* **Example:** Router(config)# mpls traffic-eng lsp attributes 1	Configures an LSP attribute list and enters LSP Attributes configuration mode. • The *string* argument identifies a specific LSP attribute list.

	Command or Action	Purpose
Step 4	**affinity** *value* [**mask** *value*] **Example:** Router(config-lsp-attr)# affinity 0 mask 0	(Optional) Specifies attribute flags for links comprising an LSP. • The *value* argument is a value required for links that make up an LSP. The values of the bits are either 0 or 1. • The **mask** *value* keyword argument combination indicates the attribute values to be checked. ◦ If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant. ◦ If a bit in the mask is 1, the attribute value of that link and the required affinity of the LSP for that bit must match.
Step 5	**bandwidth global** *kbps* **Example:** Router(config-lsp-attr)# bandwidth global 1000	Specifies an LSP bandwidth. • The **global** keyword indicates a global pool path option. • The *kbps* argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295 kbps.
Step 6	**priority** *setup-priority* [*hold-priority*] **Example:** Router(config-lsp-attr)# priority 2 2	Specifies the LSP priority. • The *setup-priority* argument is used when signaling an LSP to determine which existing LSPs can be preempted. The values range from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non 0 priority. • The *hold-priority* argument is associated with an LSP to determine if it should be preempted by other LSPs that are being signaled. The values range from 0 to 7, where a lower number indicates a higher priority.
Step 7	**list** **Example:** Router(config-lsp-attr)# list	(Optional) Displays the contents of the LSP attribute list.
Step 8	**exit** **Example:** Router(config-lsp-attr)# exit	(Optional) Exits LSP Attributes configuration mode.

	Command or Action	Purpose
Step 9	**end** **Example:** Router(config)# end	(Optional) Exits to privileged EXEC mode.
Step 10	Return to your originating procedure (NTP).	—

Example: Add Attributes to an LSP Attribute List

The following example shows how to add the protection attributes to the LSP attribute list identified with the numeral 1:

```
Router(config)# mpls traffic-eng lsp attributes 1
Router(config-lsp-attr)# affinity 7 7
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# exit
```

DLP-J146 Associate an LSP Attribute List with a Path Option for an MPLS TE Tunnel Using Cisco IOS Commands

Purpose	This procedure associates an LSP attribute list with a path option for an MPLS TE tunnel. This procedure is required if you want to apply the LSP attribute list that you configured to path options for your MPLS TE tunnels.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Based on your requirements, you can configure LSP attributes lists with different sets of attributes for different path options. LSP attribute lists also provide an easy way to configure multiple TE tunnels to use the same LSP attributes. You can reference the same LSP attribute list to configure LSP–specific parameters for one or more TE tunnels.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface tunnel 1	Configures an interface type and enters interface configuration mode. • The *type* argument is the type of interface that you want to configure. • The *number* argument is the number of the tunnel interface that you want to create or configure.
Step 4	**tunnel destination** {*hostname* | *ip-address*} **Example:** Router(config-if)# tunnel destination 209.165.200.225	Specifies the destination of the tunnel for this path option. • The *hostname* argument is the name of the host destination. • The *ip-address* argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.
Step 5	**tunnel mode mpls traffic-eng** **Example:** Router(config-if)# tunnel mode mpls traffic-eng	Sets the encapsulation mode for the tunnel for MPLS TE.
Step 6	**tunnel mpls traffic-eng autoroute announce** **Example:** Router(config-if)# tunnel mpls traffic-eng autoroute announce	(Optional) Specifies that the IGP should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation.
Step 7	**tunnel mpls traffic-eng bandwidth** *kbps* **Example:** Router(config-if)# tunnel mpls traffic-eng global bandwidth 1000	Configures the bandwidth required for a MPLS TE tunnel and assigns it to the global pool. The *kbps* argument is the bandwidth, in kilobits per second, set aside for the MPLS TE tunnel. The valid range is from 1 to 4294967295 kbps.

	Command or Action	Purpose
Step 8	**tunnel mpls traffic-eng** *priority* **setup-priority** [*hold-priority*] **Example:** Router(config-if)# tunnel mpls traffic-eng priority 1 1	Sets the priority to be used when the system determines which existing tunnels are eligible to be preempted. • The *setup-priority* argument is the priority used when signaling an LSP for this tunnel to determine which existing tunnels can be preempted. The valid values range from 0 to 7. A lower number indicates a higher priority. An LSP with a setup priority of 0 can preempt any LSP with a non 0 priority. • The *hold-priority* argument is the priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signaled. The valid values range from 0 to 7, where a lower number indicates a higher priority.
Step 9	**tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number*} [**verbatim**]} [**attributes** *string*] [**bandwidth global**] *kbps*] [**lockdown**] **Example:** Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 1	Adds an LSP attribute list to specify LSP-related parameters for path options for an MPLS TE tunnel. • The *number* argument identifies the path option. • The **dynamic** keyword indicates that the path option is dynamically calculated (the router figures out the best path). • The **explicit** keyword indicates that the path option is specified. Specify the IP addresses of the path. • The **name** *path-name* keyword argument combination identifies the name of the explicit path option. • The *path-number* argument identifies the number of the explicit path option. • The **verbatim** keyword bypasses the topology database verification. You can use the verbatim keyword only with the explicit path option. • The **attributes** *string* keyword argument combination names an attribute list to specify path options for the LSP. • The **bandwidth** keyword specifies the LSP bandwidth. • The **global** keyword indicates a global pool path option. • The *kbps* argument is the number of kilobits per second set aside for the path option. The valid range is from 1 to 4294967295 kbps. • The **lockdown** keyword disables reoptimization of the LSP.

	Command or Action	Purpose
Step 10	**end** **Example:** Router(config)# end	(Optional) Exits to privileged EXEC mode.
Step 11	Return to your originating procedure (NTP).	—

Example: Associate an LSP Attribute List with a Path Option for an MPLS TE Tunnel

The following example shows how to associate the LSP attribute list identified by the numeral 3 with path option 1:

```
Router(config)# mpls traffic-eng lsp attributes 3
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 2 2
Router(config-lsp-attr)# exit
!
!
Router(config)# interface Tunnel 1
Router(config-if)# ip unnumbered TenGigabitEthernet4/1
Router(config-if)# tunnel destination 10.112.0.12
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng affinity 1
Router(config-if)# tunnel mpls traffic-eng bandwidth 5000
Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 3
```

DLP-J147 Configure an LSP Attribute List Using Cisco IOS Commands

Purpose	This procedure configures a label switched path (LSP) attribute list with the desired attributes to be applied on a path option.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Based on your requirements, you can configure LSP attributes lists with different sets of attributes for different path options.

LSP attribute lists also provide an easy way to configure multiple TE tunnels to use the same LSP attributes. That is, you can reference the same LSP attribute list to configure LSP–specific parameters for one or more TE tunnels.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls traffic-eng lsp attributes** *string* **Example:** Router(config)# mpls traffic-eng lsp attributes 1	Configures an LSP attribute list and enters LSP Attributes configuration mode. • The *string* argument identifies a specific LSP attribute list.
Step 4	**affinity** *value* [**mask** *value*] **Example:** Router(config-lsp-attr)# affinity 0 mask 0	(Optional) Specifies the attribute flags for links comprising an LSP. • The *value* argument is a value required for links that make up an LSP. The values of the bits are either 0 or 1. • The **mask** *value* keyword argument combination indicates which attribute values should be checked. ◦ If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant. ◦ If a bit in the mask is 1, the attribute value of that link and the required affinity of the LSP for that bit must match.
Step 5	**auto-bw** [**frequency** *secs*] [**max-bw** *kbps*] [**min-bw** *kbps*] [**collect-bw**] **Example:** Router(config-lsp-attr)# auto-bw	(Optional) Specifies the automatic bandwidth configuration. • The **frequency** *secs* keyword argument combination specifies the interval between bandwidth adjustments. The specified interval can be from 300 to 604800 seconds. • The **max-bw** *kbps* keyword argument combination specifies the maximum automatic bandwidth, in kbps, for this path option. The value can be from 0 to 4294967295. • The **min-bw** *kpbs* keyword argument combination specifies the minimum automatic bandwidth, in kbps, for this path option. The value can range from 0 to 4294967295.

	Command or Action	Purpose
		• The **collect-bw** keyword collects output rate information for the path option, but does not adjust the bandwidth of the path option.
Step 6	**bandwidth global** *kbps* **Example:** Router(config-lsp-attr)# bandwidth global 5000	(Optional) Specifies the LSP bandwidth. • The **global** keyword indicates a global pool path option. • The *kbps* argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295 kbps.
Step 7	**list** **Example:** Router(config-lsp-attr)# list	(Optional) Displays the contents of the LSP attribute list.
Step 8	**lockdown** **Example:** Router(config-lsp-attr)# lockdown	(Optional) Disables reoptimization of the LSP.
Step 9	**priority** *setup-priority* [*hold-priority*] **Example:** Router(config-lsp-attr)# priority 1 1	(Optional) Specifies the LSP priority. • The *setup-priority* argument is used when signaling an LSP to determine which existing LSPs can be preempted. The valid values range from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non 0 priority. • The *hold-priority* argument is associated with an LSP to determine if it should be preempted by other LSPs that are being signaled. The valid values range from 0 to 7, where a lower number indicates a higher priority.
Step 10	**record-route** **Example:** Router(config-lsp-attr)# record-route	(Optional) Records the route used by the LSP.
Step 11	**no** *sub-command* **Example:** Router(config-lsp-attr)# no record-route	(Optional) Removes a specific attribute from the LSP attributes list. • The *sub-command* argument names the LSP attribute to remove from the attributes list.
Step 12	**exit** **Example:**	(Optional) Exits from LSP attributes configuration mode.

	Command or Action	Purpose
	Router(config-lsp-attr)# exit	
Step 13	**end** **Example:** Router(config)# end	(Optional) Exits to privileged EXEC mode.
Step 14	Return to your originating procedure (NTP).	—

Example: Configure an LSP Attribute List

This example shows how to configure the affinity, bandwidth, and priority LSP-related attributes in an LSP attribute list identified with the numeral 1:

```
Router(config)# mpls traffic-eng lsp attributes 1
Router(config-lsp-attr)# affinity 7 7
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# exit
```

DLP-J148 Modify an Attribute in an LSP Attribute List Using Cisco IOS Commands

Purpose	This procedure modifies an attribute in an LSP attribute list.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

The LSP attribute list provides a flexible user interface that can be extended or modified an any time to meet the requirements of your MPLS TE tunnel traffic. LSP Attributes configuration mode is used to display the specific LSP attributes list and to modify the required path option attribute.

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Router> enable	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls traffic-eng lsp attributes** *string* **Example:** Router(config)# mpls traffic-eng lsp attributes 1	Configures an LSP attribute list and enters LSP Attributes configuration mode. • The *string* argument identifies a specific LSP attribute list.
Step 4	**affinity** *value* [**mask** *value*] **Example:** Router(config-lsp-attr)# affinity 1 mask 1	Specifies the attribute flags for links comprising an LSP. • The *value* argument is a value required for links comprising an LSP. The valid values of bits are either 0 or 1. • The **mask** *value* keyword argument combination indicates which attribute values should be checked. ◦ If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant. ◦ If a bit in the mask is 1, the attribute value of that link and the required affinity of the tunnel for that bit must match.
Step 5	**list** **Example:** Router(config-lsp-attr)# list	(Optional) Displays the contents of the LSP attribute list. • Use the **list** command to verify that the path option attributes is modified in the attribute list.
Step 6	**exit** **Example:** Router(config-lsp-attr)# exit	(Optional) Exits LSP Attributes configuration mode.
Step 7	**end** **Example:** Router(config)# end	(Optional) Exits to privileged EXEC mode.
Step 8	Return to your originating procedure (NTP).	—

Example: Modify an Attribute in an LSP Attribute List

The following example shows how to modify the bandwidth in an LSP attribute list identified by the numeral 5:

```
Router(config)# mpls traffic-eng lsp attributes 5
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# list

LIST 5
 bandwidth 1000
 priority 1 1

Router(config-lsp-attr)# bandwidth 500
Router(config-lsp-attr)# list

LIST 5
 bandwidth 500
 priority 1 1

Router(config-lsp-attr)# exit
```

DLP-J149 Remove an Attribute from an LSP Attribute List Using Cisco IOS Commands

Purpose	This procedure removes an attribute from an LSP attribute list.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

The LSP attributes list provides a means to easily remove a path option attribute that is not required for your MPLS TE tunnel traffic. The LSP Attributes configuration mode is used to display the specific LSP attribute list and for the **no** sub-command command, which is used to remove the specific attribute from the list. Replace the sub-command argument with the command that you want to remove from the list.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls traffic-eng lsp attributes** *string* **Example:** Router(config)# mpls traffic-eng lsp attributes 1	Configures an LSP attribute list and enters LSP Attributes configuration mode. • The *string* argument identifies a specific LSP attribute list.
Step 4	**no** *sub-command* **Example:** Router(config-lsp-attr)# no priority	Removes a specific attribute from the LSP attribute list. • The *sub-command* argument names the LSP attribute to remove from the attributes list.
Step 5	**list** **Example:** Router(config-lsp-attr)# list	(Optional) Displays the contents of the LSP attribute list. • Use the **list** command to verify that the path option attribute is removed from the attribute list.
Step 6	**exit** **Example:** Router(config-lsp-attr)# exit	(Optional) Exits LSP Attributes configuration mode.
Step 7	**end** **Example:** Router(config)# end	(Optional) Exits to privileged EXEC mode.
Step 8	Return to your originating procedure (NTP).	—

Example: Remove an Attribute from an LSP Attribute List

The following example shows how to remove the priority attribute from the LSP attribute list identified by the string simple:

```
Router(config)# mpls traffic-eng lsp attributes simple
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# list

LIST simple
 priority 1 1
!
```

```
Router(config-lsp-attr)# no priority
Router(config-lsp-attr)# list

LIST simple
!
Router(config-lsp-attr)# exit
```

DLP-J150 Delete an LSP Attribute List Using Cisco IOS Commands

Purpose	This procedure deletes an LSP attribute list.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Perform this task when you no longer require the LSP attribute path options specified in the LSP attribute list for an MPLS TE tunnel.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**no mpls traffic-eng lsp attributes** *string* **Example:** Router(config)# no mpls traffic-eng lsp attributes 1	Removes a specified LSP attribute list from the device configuration. • The *string* argument identifies the specific LSP attribute list to remove.
Step 4	**end** **Example:** Router(config)# end	(Optional) Exits to privileged EXEC mode.
Step 5	**show mpls traffic-eng lsp attributes** [**name** *string*] [**internal**] **Example:**	(Optional) Displays information about configured LSP attribute lists.

	Command or Action	Purpose
	Router# show mpls traffic-eng lsp attributes	• Use the **show mpls traffic-eng lsp attributes** command to verify that the LSP attribute list is deleted.
Step 6	Return to your originating procedure (NTP).	—

Example: Delete an LSP Attribute List

The following example shows how to delete an LSP attribute list identified by numeral 1:

```
Router(config)# mpls traffic-eng lsp attributes 1
Router(config-lsp-attr)# affinity 7 7
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# exit
!
Router(config)# no mpls traffic-eng lsp attributes 1
```

DLP-J151 Verify Attributes Within an LSP Attribute List Using Cisco IOS Commands

Purpose	This procedure verifies the attributes within an LSP attribute list.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	Router# configure terminal	
Step 3	**mpls traffic-eng lsp attributes** *string***list** **Example:** Router(config)# mpls traffic-eng lsp attributes 1 list	Enters LSP Attributes configuration mode for a specific LSP attribute list and verifies that the contents of the attributes list are as expected.
Step 4	**exit** **Example:** Router(config-lsp-attr)# exit	Exits LSP Attributes configuration mode.
Step 5	**end** **Example:** Router(config)# end	(Optional) Exits to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J152 Verify All LSP Attribute Lists Using Cisco IOS Commands

Purpose	This procedure verifies all the configured LSP attribute lists. Use this procedure to display all LSP attribute lists to verify that the attributes lists that you configured are in operation.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show mpls traffic-eng lsp attributes** [**name** *string*] [**internal**] **Example:** Router# show mpls traffic-eng lsp attributes	Verifies that all the configured LSP attribute lists are as expected.
Step 3	**show running-config** | **begin** *text-string* **Example:** Router# show running-config | begin mpls traffic-eng lsp	Verifies that all the configured LSP attribute lists are as expected. Use the **begin** command modifier with the **mpls traffic-eng lsp** text-string to locate the LSP attributes information in the configuration file.
Step 4	**exit** **Example:** Router# exit	Exits user EXEC mode.
Step 5	Return to your originating procedure (NTP).	—

Understanding MPLS–TE Verbatim Path Support

The MPLS Traffic Engineering–Verbatim Path Support feature allows network nodes to support RSVP extensions without supporting IGP extensions for TE, thereby bypassing the topology database verification process.

MPLS TE LSPs usually require that all the nodes in the network are TE aware, meaning they have IGP extensions to TE in place. However, some network administrators want the ability to build TE LSPs to traverse nodes that do not support IGP extensions to TE, but that do support RSVP extensions to TE.

Verbatim LSPs are helpful when all or some of the intermediate nodes in a network do not support IGP extensions for TE.

When this feature is enabled, the IP explicit path is not checked against the TE topology database. Because the TE topology database is not verified, a Path message with IP explicit path information is routed using the shortest path first (SPF) algorithm for IP routing.

NTP-J50 Configure MPLS-TE Verbatim Path Support

Purpose	This procedure configures verbatim path support for MPLS–TE tunnels.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J153 Configure MPLS TE–Verbatim Path Support Using Cisco IOS Commands, on page 246
- DLP-J154 Verify Verbatim LSPs for MPLS TE Tunnels Using Cisco IOS Commands, on page 248

Stop. You have completed this procedure.

DLP-J153 Configure MPLS TE–Verbatim Path Support Using Cisco IOS Commands

Purpose	This procedure configures MPLS traffic engineering–verbatim path support.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:**	Enters interface configuration mode. • The *number* argument identifies the tunnel number to be configured.

	Command or Action	Purpose
	Router(config)# interface tunnel 1	
Step 4	**ip unnumbered loopback** *number* **Example:** Router(config–if)# ip unnumbered loopback 1	Configures an unnumbered IP interface, which enables IP processing without an explicit address. A loopback interface is usually configured with the router ID. **Note** An MPLS traffic engineering tunnel interface must be unnumbered because it represents a unidirectional link.
Step 5	**tunnel destination** {*host–name* | *ip–address*} **Example:** Router(config–if)# tunnel destination 10.100.100.100	Specifies the destination for a tunnel. • The *host–name* argument is the name of the host destination. • The *ip–address* argument is the IPv4 address of the host destination expressed in decimal in four–part, dotted notation.
Step 6	**tunnel mode mpls traffic–eng** **Example:** Router(config–if)# tunnel mode mpls traffic–eng	Sets the tunnel encapsulation mode to MPLS traffic engineering.
Step 7	**tunnel mpls traffic–eng bandwidth** *kbps* **Example:** Router(config–if)# tunnel mpls traffic–eng bandwidth 1000	Configures the bandwidth required for an MPLS TE tunnel and assigns it to the global pool. • The *kbps* argument is the bandwidth, in kilobits per second, set aside for the MPLS TE tunnel. The range is from 1 to 4294967295 kbps.
Step 8	**tunnel mpls traffic–eng autoroute announce** **Example:** Router(config–if)# tunnel mpls traffic–eng autoroute announce	Specifies that IGP must use the tunnel (if the tunnel is up) in its enhanced SPF calculation.
Step 9	**tunnel mpls traffic–eng priority** *setup–priority* [*hold–priority*] **Example:** Router(config–if)# tunnel mpls traffic–eng priority 1 1	Configures the setup and reservation priority for a tunnel. • The *setup–priority* argument is the priority used when signaling an LSP for this tunnel to determine which existing tunnels can be preempted. The valid values range from 0 to 7. A lower number indicates a higher priority. An LSP with a setup priority of 0 can preempt any LSP with a non 0 priority.

	Command or Action	Purpose
		• The *hold–priority* argument is the priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signaled. The valid values range from 0 to 7, where a lower number indicates a higher priority.
Step 10	**tunnel mpls traffic-eng path-option** {*number* {**dynamic** [**attributes** *lsp-attributes* | **bandwidth** *kbps*] [**lockdown**] | **lockdown** [**bandwidth** *kbps*] | **explicit** {**identifier** *path-number* | **name** *path-name*} [**attributes** *lsp-attributes* [**verbatim**]] | **bandwidth** *kbps* [**lockdown**] [**verbatim**]] | **lockdown bandwidth** *kbps* [**verbatim**] | **verbatim bandwidth** *kbps* [**lockdown**]}} **Example:** Router(config–if)# tunnel mpls traffic–eng path–option 1 explicit name test verbatim	Specifies LSP–related parameters, including the **verbatim** keyword used with an explicit path option, for a MPLS TE tunnel.
Step 11	**end** **Example:** Router(config)# end	(Optional) Exits to privileged EXEC mode.
Step 12	Return to your originating procedure (NTP).	—

Example: Configure MPLS TE—Verbatim Path Support

The following example shows how to configure a tunnel with an explicit path option using verbatim.

```
interface tunnel 1
 ip unnumbered loopback 1
 tunnel destination 10.10.100.100
 tunnel mode mpls traffic–eng
 tunnel mpls traffic–eng bandwidth 1000
 tunnel mpls traffic–eng autoroute announce
 tunnel mpls traffic–eng priority 1 1
 tunnel mpls traffic–eng path–option 1 explicit name path1 verbatim
```

DLP-J154 Verify Verbatim LSPs for MPLS TE Tunnels Using Cisco IOS Commands

Purpose	This procedure verifies the verbatim option that is configured for the LSPs for MPLS TE tunnels.

Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show mpls traffic-eng tunnels** *tunnel-interfacenumber* [**brief**] **Example:** Router# show mpls traffic-eng tunnels tunnel1	Displays information about tunnels including those configured with an explicit path option using verbatim.
Step 3	**disable** **Example:** Router# disable	(Optional) Exits to user EXEC mode.
Step 4	Return to your originating procedure (NTP).	—

Example: Verify Verbatim LSPs for MPLS TE Tunnels

In the following example, the **show mpls traffic-eng tunnels** command displays tunnel information, including whether the explicit path option is using verbatim, and the Active Path Options parameters that show the status of verbatim.

```
Router# show mpls traffic-eng tunnels tunnel100

 Name: R259_t5                           (Tunnel100) Destination:
192.168.30.1
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected

    path option 1, type explicit (verbatim) path1 (Basis for Setup, path
 weight 0)

  Config Parameters:
    Bandwidth: 100        kbps (Global)  Priority: 1  1   Affinity:
0x0/0xFFFF
```

```
    Metric Type: TE (default)
   AutoRoute:  disabled  LockDown: disabled  Loadshare: 0       bw-based

    auto-bw: disabled

 Active Path Option Parameters:
    State: explicit path option 1 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: enabled
```

Understanding MPLS–TE Path Protection

Path protection provides an end–to–end failure recovery mechanism (that is, full path protection) for MPLS–TE tunnels. A secondary LSP is established to provide failure protection for the protected LSP that is carrying a tunnel TE traffic. When there is a failure on the protected LSP, the headend router immediately enables the secondary LSP to temporarily carry the tunnel traffic. If there is a failure on the secondary LSP, the tunnel does not have the path protection until the failure along the secondary path is cleared.

The failure detection mechanisms that trigger a switchover to a secondary tunnel include the following:

- Path error from RSVP signaling
- Notification from the RSVP hello that a neighbor is lost
- Notification from the IGP that the adjacency is down
- Local teardown of the LSP of the protected tunnel due to preemption to signal higher priority LSPs, online insertion and removal (OIR), and so forth

Presignaling a secondary LSP is faster than configuring a secondary primary path option or allowing the tunnel headend router to dynamically recalculate a path. The actual recovery time is topology dependent, and affected by delay factors such as propagation delay or switch fabric latency.

Prerequisites

- Ensure that your network supports MPLS TE, Cisco Express Forwarding, or OSPF.
- Enable MPLS.
- Configure TE on the routers.
- Configure a TE tunnel with a primary path option by using the **tunnel mpls traffic-eng path-option** command.
- If your router supports stateful switchover (SSO), configure RSVP Graceful Restart in full mode on the routers.
- If your router supports SSO, you must have configured SSO on the device for Cisco Nonstop Forwarding (NSF) operation.

Restrictions

- Dynamic diverse paths are not supported.
- Do not use link and node protection with path protection on the headend router.

- Do not configure path protection on an automesh tunnel template because the destinations are different and you cannot use the same path option to reach multiple destinations.

Enhanced Path Protection

Enhanced path protection provides support of multiple backup path options for each primary path option. You can configure up to eight backup path options for a given primary path option. Only one of the configured backup path options is actively signaled at any time.

After you enter the **mpls traffic-eng path-option list** command, you can enter the backup path priority in the *number* argument of the **path-option** command. A lower identifier represents a higher priority. Priorities are configurable for each backup path option. Multiple backup path options and a single backup path option cannot coexist to protect a primary path option.

Benefits of MPLS-TE Protection

The following sections describe the benefits of MPLS-TE protection.

Multiple Backup Tunnels Protecting the Same Interface

There is no limit (except memory limitations) to the number of backup tunnels that can protect a given interface. In many topologies, support for node protection requires supporting multiple backup tunnels per protected interface.

The multiple backup tunnels provides the following benefits:

- Redundancy—If one backup tunnel is down, other backup tunnels protect LSPs.
- Increased backup capacity—If the protected interface is a high-capacity link and no single backup path exists with an equal capacity, multiple backup tunnels can protect that one high-capacity link. The LSPs using this link will fail over to different backup tunnels, allowing all of the LSPs to have adequate bandwidth protection during failure (rerouting). If bandwidth protection is not desired, the router spreads LSPs across all available backup tunnels (that is, load balancing is available across the backup tunnels).

RSVP Hello

RSVP Hello allows a router to detect when its neighbor has gone down but its interface to that neighbor is still operational. When Layer 2 link protocols are unable to detect that the neighbor is unreachable, hellos provide the detection mechanism; this allows the router to switch LSPs onto its backup tunnels and avoid packet loss.

NTP-J51 Configure MPLS-TE Path Protection

Purpose	This procedure configures path protection for MPLS–TE tunnels.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J155 Create a Path Option List Using Cisco IOS Commands, on page 252
- DLP-J157 Assign a Secondary Path Option to Protect a Primary Path Option Using Cisco IOS Commands, on page 255
- DLP-J158 Configure Fallback Bandwidth Path Options for TE Tunnels Using Cisco IOS Commands, on page 256
- DLP-J159 Modify the Bandwidth on a Path Option for Bandwidth Override Using Cisco IOS Commands, on page 259
- DLP-J160 Modify a Path Option to Use a Different LSP Attribute List Using Cisco IOS Commands, on page 261
- DLP-J161 Remove a Path Option for Bandwidth Override Using Cisco IOS Commands, on page 263
- DLP-J162 Remove a Path Option for a LSP in a MPLS TE Tunnel Using Cisco IOS Commands, on page 265

Stop. You have completed this procedure.

DLP-J155 Create a Path Option List Using Cisco IOS Commands

Purpose	This procedure creates a path option list of backup paths for a primary path option.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

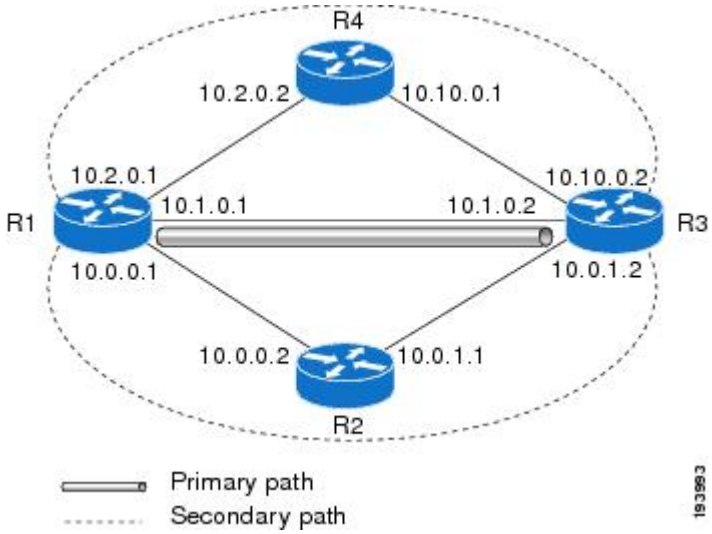
Note To use a secondary path instead, see the DLP-J169 Configure Explicit Paths for Secondary Paths Using Cisco IOS Commands, on page 279.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls traffic-eng path-option list** [**name** *pathlist-name* | **identifier** *pathlist-number*] **Example:** Router(config)# mpls traffic-eng path-option list name pathlist-01	Configures a path option list, and enters path-option list configuration mode.
Step 4	**path-option** *number* **explicit** [*name pathoption-name* | **identifier** *pathoption-number*] **Example:** Router(cfg-pathoption-list)# path-option 10 explicit identifier 200	(Optional) Specifies the name or identification number of the path option to add, edit, or delete. The *pathoption-number* value range is from 1 to 65535.
Step 5	**list** **Example:** Router(cfg-pathoption-list)# list	(Optional) Lists all the path options.
Step 6	**no** [*pathoption-name* | *pathoption-number*] **Example:** Router(cfg-pathoption-list)# no 10	(Optional) Deletes a specified path option.
Step 7	**exit** **Example:** Router(cfg-pathoption-list)# exit	(Optional) Exits path-option list configuration mode and returns to global configuration mode.
Step 8	Return to your originating procedure (NTP).	—

Example: Create a Path Option List

Figure 51: Network Topology for Enhanced Path Protection



The following example shows how to configure two explicit paths named **secondary1** and **secondary2**.

```
Router(config)# ip explicit-path name secondary1
Router(cfg-ip-expl-path)# index 1 next 10.0.0.2
Explicit Path name secondary1:
 1: next-address 10.0.0.2

Router(cfg-ip-expl-path)# index 2 next 10.0.1.2
Explicit Path name secondary1:
 1: next-address 10.0.0.2
 2: next-address 10.0.1.2

Router(cfg-ip-expl-path)# ip explicit-path name secondary2
Router(cfg-ip-expl-path)# index 1 next 10.2.0.2
Explicit Path name secondary2:
 1: next-address 10.2.0.2

Router(cfg-ip-expl-path)# index 2 next 10.10.0.2
Explicit Path name secondary2:
 1: next-address 10.2.0.2
 2: next-address 10.10.0.2

Router(cfg-ip-expl-path)# exit
```

The following example shows how to create a path option list of backup paths. You can define the path option list by using the explicit paths.

```
Router(config)# mpls traffic-eng path-option list name pathlist-01
Router(cfg-pathoption-list)# path-option 10 explicit name secondary1
path-option 10 explicit name secondary1

Router(cfg-pathoption-list)# path-option 20 explicit name secondary2
path-option 10 explicit name secondary1
path-option 20 explicit name secondary2

Router(cfg-pathoption-list)# exit
```

DLP-J157 Assign a Secondary Path Option to Protect a Primary Path Option Using Cisco IOS Commands

Purpose	This procedure assigns a secondary path option to protect a primary path option using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Assign a secondary path option if there is a link or node failure along a path and all the interfaces in the network are not protected.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *tunnelnumber* **Example:** Router(config)# interface tunnel500	Configures a tunnel interface and enters interface configuration mode.
Step 4	**tunnel mpls traffic-eng path-option protect** {*number* {**dynamic** [**attributes** *lsp-attributes* | **bandwidth** *kbps*] [**lockdown**] | **lockdown** [**bandwidth** *kbps*] | **explicit** {**identifier** *path-number* | **name** *path-name*} [**attributes** *lsp-attributes* [**verbatim**]] | **bandwidth** *kbps* [**lockdown**] [**verbatim**]] | **lockdown bandwidth** *kbps* [**lockdown**] [**verbatim**] | **verbatim** [**lockdown**]]} **Example:** Router(config-if)# tunnel mpls traffic-eng path-option protect 10 explicit name path344	Configures a secondary path option for a MPLS TE tunnel.

	Command or Action	Purpose
Step 5	**exit** **Example:** Router(config-if)# exit	(Optional) Exits interface configuration mode and enters global configuration mode.
Step 6	Return to your originating procedure (NTP).	—

Example: Assign a Secondary Path Option to Protect a Primary Path Option

The following example shows how to configure a traffic engineering tunnel.

```
Router> enable
Router# configure terminal
Router(config-if)# interface tunnel500
Router(config-if)# tunnel mpls traffic-eng path-option protect 10 explicit name path344
```

The following **show running interface** command output shows that path protection has been configured. Tunnel 500 has path option 10 using path344 and protected by path3441, and path option 20 using path345 and protected by path348.

```
Router# show running interface tunnel500
```

```
Building configuration...

Current configuration : 497 bytes
!
interface Tunnel500
 ip unnumbered Loopback0
 tunnel destination 10.0.0.9
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 100
 tunnel mpls traffic-eng path-option 10 explicit name path344
 tunnel mpls traffic-eng path-option 20 explicit name path345
 tunnel mpls traffic-eng path-option protect 10 explicit name path3441
 tunnel mpls traffic-eng path-option protect 20 explicit name path348
end
```

DLP-J158 Configure Fallback Bandwidth Path Options for TE Tunnels Using Cisco IOS Commands

Purpose	This procedure configures the fallback bandwidth path options for a TE tunnel.
Tools/Equipment	None
Prerequisite Procedures	None

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

Use this procedure to configure path options that reduce the bandwidth constraint each time the headend of a tunnel fails to establish an LSP.

Configuration of the Path Option for Bandwidth Override feature can reduce bandwidth constraints on path options temporarily and improve the chances to set up an LSP for the TE tunnel. When a TE tunnel uses a path option with bandwidth override, the traffic engineering attempts every 30 seconds to reoptimize the tunnel to use the preferred path option with the original configured bandwidth. The Path Option for Bandwidth Override feature is designed as a temporary reduction in bandwidth constraint. To force immediate reoptimization of all traffic engineering tunnels, you can use the **mpls traffic-eng reoptimize** command. You can also configure the **lockdown** command with bandwidth override to prevent automatic reoptimization.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface tunnel 1	Configures the interface type and enters the interface configuration mode. • The *type* argument is the type of interface that you want to configure. • The *number* argument is the number of the tunnel interface that you want to create or configure.
Step 4	**tunnel destination** {*hostname* | *ip-address*} **Example:** Router(config-if)# tunnel destination 209.165.200.225	Specifies the destination of the tunnel for this path option. • The *hostname* argument is the name of the host destination. • The *ip-address* argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.
Step 5	**tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number*} [**verbatim**]	Adds a path option for bandwidth override to specify a bandwidth fallback for a path option for an MPLS TE tunnel. • The *number* argument identifies the path option.

	Command or Action	Purpose
	[**attributes** *string*] [**bandwidth global**] *kbps*] }[**lockdown**] **Example:** Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic bandwidth 500	• The **dynamic** keyword indicates that the path option is dynamically calculated (the router figures out the best path). • The **explicit** keyword indicates that the path option is specified. Specify the IP address of the path. • The **name** *path-name* keyword argument combination identifies the name of the explicit path option. • The *path-number* argument identifies the number of the explicit path option. • The **verbatim** keyword bypasses the topology database verification. You can use the verbatim keyword only with the explicit path option. • The **attributes** *string* keyword argument combination names an attribute list to specify path options for the LSP. • The **bandwidth** keyword specifies the LSP bandwidth. • The **global** keyword indicates a global pool path option. • The *kbps* argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295 kbps. • The **lockdown** keyword disables reoptimization of the LSP.
Step 6	**end** **Example:** Router(config-if)# end	(Optional) Exits to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

Example: Configure Fallback Bandwidth Path Options for TE Tunnels

The following example shows how to configure the multiple path options with the **tunnel mpls traffic-eng path-option** command:

```
interface Tunnel 1
 ip unnumbered Loopback0
 tunnel destination 10.10.10.12
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name path1
 tunnel mpls traffic-eng path-option 2 explicit name path2 bandwidth 500
```

```
 tunnel mpls traffic-eng path-option 3 dynamic bandwidth 0
end
```

The device selects a path option for an LSP in the following order of preference:

- The device attempts to signal an LSP using path options starting with path-option 1.

  The device attempts to signal an LSP with the 1000 kbps bandwidth configured on the tunnel interface because path-option 1 has no bandwidth configured.

- If 1000 kbps bandwidth is not available over the network, the device attempts to establish an LSP using path-option 2.

  Path-option 2 has a bandwidth of 500 kbps configured. This reduces the bandwidth constraint from the original 1000 kbps configured on the tunnel interface.

- If 500 kbps is not available, the device attempts to establish an LSP using path-option 3.

  Path-option 3 is configured as dynamic and has bandwidth 0. The device establishes the LSP if an IP path exists to the destination and all other tunnel constraints are met.

DLP-J159 Modify the Bandwidth on a Path Option for Bandwidth Override Using Cisco IOS Commands

Purpose	This procedure modifies the bandwidth on a path option for bandwidth override.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

You might need to further reduce or modify the bandwidth constraint for a path option to ensure that the headend of a tunnel establishes an LSP.

The Path Option for Bandwidth Override feature is designed as a temporary reduction in bandwidth constraint. To force immediate reoptimization of all traffic engineering tunnels, you can use the **mpls traffic-eng reoptimize** command. You can also configure the **lockdown** command with bandwidth override to prevent automatic reoptimization.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface tunnel 1	Configures the interface type and enters the interface configuration mode. • The *type* argument is the type of interface that you want to configure. • The *number* argument is the number of the tunnel interface that you want to create or configure.
Step 4	**tunnel destination** {*hostname* | *ip-address*} **Example:** Router(config-if)# tunnel destination 209.165.200.225	Specifies the destination of the tunnel for this path option. • The *hostname* argument is the name of the host destination. • The *ip-address* argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.
Step 5	**tunnel mpls traffic-eng path-option** {*number* {**dynamic** [**attributes** *lsp-attributes* | **bandwidth** *kbps*] [**lockdown**] | **lockdown** [**bandwidth** *kbps*] | **explicit** {**identifier** *path-number* | **name** *path-name*} [**attributes** *lsp-attributes* [**verbatim**]] | **bandwidth** *kbps* [**lockdown**] [**verbatim**]] | **lockdown bandwidth** *kbps* [**verbatim**] | **verbatim bandwidth** *kbps* [**lockdown**]}} **Example:** Router(config-if)# tunnel mpls traffic-eng path-option 2 dynamic bandwidth 500	Adds a path option for bandwidth override to specify a bandwidth fallback for a path option for an MPLS TE tunnel.
Step 6	**end** **Example:** Router(config-if)# end	(Optional) Exits to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

Example: Modify the Bandwidth on a Path Option for Bandwidth Override

The following example shows how to modify the bandwidth on a path option for bandwidth override. Path-option 3 is changed to an explicit path with a bandwidth of 100 kbps. Path-option 4 is configured with bandwidth 0.

```
interface Tunnel 1
 ip unnumbered Loopback0
 tunnel destination 10.10.10.12
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name path1
 tunnel mpls traffic-eng path-option 2 explicit name path2 bandwidth 500
 tunnel mpls traffic-eng path-option 3 dynamic bandwidth 0
!
!
Router(config)# tunnel mpls traffic-eng path-option 3 explicit name path3 bandwidth 100
Router(config)# tunnel mpls traffic-eng path-option 4 dynamic bandwidth 0
```

DLP-J160 Modify a Path Option to Use a Different LSP Attribute List Using Cisco IOS Commands

Purpose	This procedure modifies the path option to use a different LSP attribute list.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Based on your requirements, you can configure LSP attributes lists with different sets of attributes for different path options or change the set of attributes associated with a path option. Use the **tunnel mpls traffic-eng path-option number dynamic attributes string** command in interface configuration mode to modify the path option to use a different LSP attribute list. The **attributes** keyword and *string* argument combination names the new LSP attribute list for the path option specified.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface tunnel 1	Configures the interface type and enters the interface configuration mode.
Step 4	**tunnel destination** {hostname | ip-address} **Example:** Router(config-if)# tunnel destination 209.165.200.225	Specifies the destination of the tunnel for this path option. • The *hostname* argument is the name of the host destination. • The *ip-address* argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.
Step 5	**tunnel mpls traffic-eng path-option** {*number* {**dynamic** [**attributes** *lsp-attributes* | **bandwidth** *kbps*] [**lockdown**] | **lockdown** [**bandwidth** *kbps*] | **explicit** {**identifier** *path-number* | **name** *path-name*} [**attributes** *lsp-attributes* [**verbatim**]] | **bandwidth** *kbps* [**lockdown**] [**verbatim**]] | **lockdown bandwidth** *kbps* [**verbatim**] | **verbatim bandwidth** *kbps* [**lockdown**]}} **Example:** Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 1	Adds an LSP attribute list to specify LSP-related parameters for a path options for an MPLS TE tunnel.
Step 6	**end** **Example:** Router(config-if)# end	(Optional) Exits to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

Example: Modify a Path Option to Use a Different LSP Attribute List

The following example shows how to modify the path option 1 to use an LSP attribute list identified by the numeral 1:

```
Router(config)# mpls traffic-eng lsp attributes 1
Router(config-lsp-attr)# affinity 7 7
Router(config-lsp-attr)# bandwidth 500
```

```
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# exit

Router(config)# mpls traffic-eng lsp attributes 2
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# exit

Router(config)# interface Tunnel 1
Router(config-if)# ip unnumbered TenGigabitEthernet4/1
Router(config-if)# tunnel destination 10.112.0.12
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng affinity 1
Router(config-if)# tunnel mpls traffic-eng bandwidth 5000
Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 1
```

DLP-J161 Remove a Path Option for Bandwidth Override Using Cisco IOS Commands

Purpose	This procedure removes the bandwidth on the path option for bandwidth override.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface tunnel 1	Configures the interface type and enters the interface configuration mode.
Step 4	**tunnel destination** {*hostname* | *ip-address*} **Example:**	Specifies the destination of the tunnel for this path option.

	Command or Action	Purpose
	Router(config-if)# tunnel destination 209.165.200.225	• The *hostname* argument is the name of the host destination. • The *ip-address* argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.
Step 5	**tunnel mpls traffic-eng path-option** {*number* {**dynamic** [**attributes** *lsp-attributes* | **bandwidth** *kbps*] [**lockdown**] | **lockdown** [**bandwidth** *kbps*] | **explicit** {**identifier** *path-number* | **name** *path-name*} [**attributes** *lsp-attributes* [**verbatim**]] | **bandwidth** *kbps* [**lockdown**] [**verbatim**]] | **lockdown bandwidth** *kbps* [**verbatim**] | **verbatim bandwidth** *kbps* [**lockdown**]}} **Example:** Router(config-if)# no tunnel mpls traffic-eng path-option 2 dynamic bandwidth 500	Removes a path option for bandwidth override that specifies a bandwidth fallback for a path option for an MPLS TE tunnel.
Step 6	**end** **Example:** Router(config-if)# end	(Optional) Exits to privileged EXEC mode.
Step 7	**show mpls traffic-eng tunnels** *tunnel-interface* [**brief**] **Example:** Router# show mpls traffic-eng tunnels tunnel1	(Optional) Displays information about tunnels. • Use the **show mpls traffic-eng tunnels** command to verify which bandwidth path option is in use by the LSP.
Step 8	Return to your originating procedure (NTP).	—

Example: Remove a Path Option for Bandwidth Override

The following example shows how to remove a path option for bandwidth override:

```
Router(config)# interface Tunnel 1
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel destination 10.10.10.12
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng autoroute announce
Router(config-if)# tunnel mpls traffic-eng priority 1 1
Router(config-if)# tunnel mpls traffic-eng bandwidth 1000
Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name path1
Router(config-if)# tunnel mpls traffic-eng path-option 2 explicit name path2 bandwidth 500
Router(config-if)# tunnel mpls traffic-eng path-option 3 explicit name path3 bandwidth 100
Router(config-if)# tunnel mpls traffic-eng path-option 4 dynamic bandwidth 0
!
```

```
Router(config-if)# no tunnel mpls traffic-eng path-option 3 explicit name path3 bandwidth
100
```

DLP-J162 Remove a Path Option for a LSP in a MPLS TE Tunnel Using Cisco IOS Commands

Purpose	This procedure removes a path option for a LSP in a MPLS TE tunnel.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Use this task to remove a path option for a LSP when your MPLS TE tunnel traffic requirements change.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface tunnel 1	Configures the interface type and enters the interface configuration mode.
Step 4	**tunnel destination** {*hostname* | *ip-address*} **Example:** Router(config-if)# tunnel destination 209.165.200.225	Specifies the destination of the tunnel for this path option. • The *hostname* argument is the name of the host destination. • The *ip-address* argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.

	Command or Action	Purpose
Step 5	**no tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number*} [**verbatim**]} [**attributes** *string*] [**bandwidth global**] *kbps*] [**lockdown**] **Example:** Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 1	Removes an LSP attribute list that specifies LSP-related parameters for a path option for an MPLS TE tunnel.
Step 6	**end** **Example:** Router(config-if)# end	(Optional) Exits to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

Example: Remove a Path Option for a LSP in a MPLS TE Tunnel

The following example shows how to remove the path option 1 for an LSP in a TE tunnel:

```
Router(config)# interface Tunnel 1
Router(config-if)# ip unnumbered TenGigabitEthernet4/1
Router(config-if)# tunnel destination 10.112.0.12
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng affinity 1
Router(config-if)# tunnel mpls traffic-eng bandwidth 5000
Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit path1 attributes 1
Router(config-if)# tunnel mpls traffic-eng path-option 2 explicit path2 attributes 2
!
!
Router(config-if)# no tunnel mpls traffic-eng path-option 1 explicit path1 attributes 1
```

Understanding MPLS–TE Tunnels

MPLS TE enables you to build LSPs across your network for forwarding traffic.

MPLS TE LSPs let the headend of a TE tunnel control the path its traffic takes to a particular destination. This method is more flexible than forwarding traffic based only on a destination address.

Interarea tunnels allow you to build:

- TE tunnels between areas (interarea tunnels).
- TE tunnels that start and end in the same area, on multiple areas on a router (intra–area tunnels).

Some tunnels are more important than others. For example, you may have tunnels carrying VoIP traffic and tunnels carrying data traffic that are competing for the same resources. You may have certain data tunnels that are more important than others. MPLS TE allows you to have some tunnels preempt others. Each tunnel has a priority, and more important tunnels take precedence over less important tunnels.

NTP-J51 Configure MPLS-TE Tunnels

Purpose	This procedure configures MPLS–TE tunnels.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J163 Create a MPLS-TE Tunnel Using Cisco IOS Commands, on page 267
- DLP-J164 Enable Automatic Bandwidth Adjustment for a Tunnel Using Cisco IOS Commands, on page 270
- DLP-J165 Configure MPLS–TE–Tunnel Source Using Cisco IOS Commands, on page 271
- DLP–J166 Create an MPLS–TE Tunnel Using CTC, on page 274
- DLP-J167 Edit an MPLS–TE Tunnel Using CTC, on page 277

Stop. You have completed this procedure.

DLP-J163 Create a MPLS-TE Tunnel Using Cisco IOS Commands

Purpose	This procedure creates a MPLS-TE tunnel using Cisco IOS commands.
Tools/Equipment	None

Prerequisite Procedures	• NTP-J42 Configure Global Settings for MPLS, on page 171 • DLP-J138 Configure OSPF to Support Traffic Engineering Using Cisco IOS Commands, on page 182 • NTP-J48 Configure MPLS-TE Parameters, on page 220 • If you want to create an explicit path, see DLP-J168 Create an Explicit Path Using Cisco IOS Commands, on page 278
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** Router(config)# interface tunnel 1	Configures a tunnel interface and enters interface configuration mode.
Step 4	**ip unnumbered** *interface-type interface-number* **Example:** Router(config-if)# ip unnumbered loopback 0	Gives the tunnel interface an IP address that is the same as that of interface loopback0. An MPLS TE tunnel interface must be unnumbered because it represents a unidirectional link. This command is not effective until loopback0 has been configured with an IP address.
Step 5	**tunnel destination** *ip-address* **Example:** Router(config-if)# tunnel destination 209.165.200.225	Specifies the destination for a tunnel. The destination must be the MPLS TE router id of the destination device.

	Command or Action	Purpose
Step 6	**tunnel mode mpls traffic-eng** **Example:** Router(config-if)# tunnel mode mpls traffic-eng	Sets the encapsulation mode of the tunnel to MPLS TE.
Step 7	**tunnel mpls traffic-eng bandwidth** *kbps* **Example:** Router(config-if)# tunnel mpls traffic-eng bandwidth 250	Configures the bandwidth for the MPLS TE tunnel. • The *kbps* argument is the bandwidth, in kilobits per second, set for the MPLS TE tunnel. The range is from 1 to 4294967295 kbps. The default value is 0 kbps. • If automatic bandwidth is configured for the tunnel, the **tunnel mpls traffic-eng bandwidth** command configures the initial tunnel bandwidth, which is adjusted by the autobandwidth mechanism. **Note** If you configure the bandwidth of a tunnel with the **tunnel mpls traffic-eng bandwidth** command, and the minimum amount of automatic bandwidth with the **tunnel mpls traffic-eng auto-bw** command, the minimum amount of automatic bandwidth adjustment is the lower of those two configured values.
Step 8	**tunnel mpls traffic-eng path-option** [**protect**] *preference-number* {**dynamic** | **explicit** | {**name** *path-name* | *path-number*}} [**lockdown**] **Example:** Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit test	Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the TE topology database. A dynamic path is used if an explicit path is currently unavailable.
Step 9	**exit** **Example:** Router(config-if)# exit	Exits to global configuration mode.
Step 10	**exit** **Example:** Router(config)# exit	Exits to privileged EXEC mode.
Step 11	Return to your originating procedure (NTP).	—

DLP-J164 Enable Automatic Bandwidth Adjustment for a Tunnel Using Cisco IOS Commands

Purpose	This procedure enables automatic bandwidth adjustment for a tunnel and constrains the range of automatic bandwidth adjustments applied to the tunnel.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *tunnel-number* **Example:** Router(config)# interface tunnel 1	Configures a tunnel interface and enters interface configuration mode.
Step 4	**tunnel mpls traffic-eng auto-bw** [**collect-bw**] [**frequency** *seconds*] [**max-bw** *kbps*] [**min-bw** *kbps*] **Example:** Router(config-if)# tunnel mpls traffic-eng auto-bw max-bw 2000 min-bw 1000	Enables automatic bandwidth adjustment for the tunnel and controls the manner in which the bandwidth for a tunnel is adjusted.
Step 5	**exit** **Example:** Router(config-if)# exit	Exits to global configuration mode.

	Command or Action	Purpose
Step 6	**exit** **Example:** Router(config)# exit	Exits to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

Example: Tunnel Configuration for Automatic Bandwidth

The following example shows how to use the **tunnel mpls traffic-eng auto-bw** command to enable automatic bandwidth adjustment for Tunnel 1. The command specifies a maximum allowable bandwidth of 2000 kbps, a minimum allowable bandwidth of 1000 kbps, and the default automatic bandwidth adjustment frequency of once a day, be used.

```
interface tunnel1
ip unnumbered loopback 0
tunnel destination 192.168.17.17
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng bandwidth 1500
tunnel mpls traffic-eng priority 1 1
tunnel mpls traffic-eng path-option 1 dynamic
tunnel mpls traffic-eng auto-bw max-bw 2000 min-bw 1000
```

DLP-J165 Configure MPLS–TE–Tunnel Source Using Cisco IOS Commands

Purpose	This procedure specifies a tunnel source for an MPLS TE tunnel using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

You can configure the tunnel source as an IP address or as an interface. If you configure the tunnel source as an interface, then you must configure an IP address for the interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	Router> enable	
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface tunnel 1	Configures a tunnel interface and enters interface configuration mode.
Step 4	**ip unnumbered** *interface-name interface-number* **Example:** Router(config-if)# ip unnumbered loopback0	Configures an unnumbered IP interface, which enables IP processing without an explicit address. An MPLS TE tunnel interface must be unnumbered because it represents a unidirectional link.
Step 5	**no ip directed-broadcast** **Example:** Router(config-if)# no ip directed-broadcast	Disables the translation of a directed broadcast to physical broadcasts.
Step 6	**tunnel source** {*ip-address* | *interface-type interface-number*} **Example:** Router(config-if)# tunnel source loopback1	Configures the tunnel source.
Step 7	**tunnel destination** {*host-name* | *ip-address*} **Example:** Router(config-if)# tunnel destination 192.168.2.1	Specifies the destination for a tunnel. The destination must be the MPLS TE router ID of the destination device.
Step 8	**tunnel mode mpls traffic-eng** **Example:** Router(config-if)# tunnel mode mpls traffic-eng	Sets the encapsulation mode of the tunnel to MPLS TE.
Step 9	**tunnel mpls traffic-eng priority** *setup-priority* [*hold-priority*] **Example:** Router(config-if)# tunnel mpls traffic-eng priority 1 1	Sets the priority to be used when the system determines which existing tunnels are eligible to be preempted. • The *setup-priority* argument is the priority used when signaling an LSP for this tunnel to determine which existing tunnels can be preempted. The valid values are from 0 to 7. A lower number indicates a higher priority. An LSP with a setup priority of 0 can preempt any LSP with a non 0 priority.

	Command or Action	Purpose
		• The *hold-priority* argument is the priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signaled. The valid values are from 0 to 7, where a lower number indicates a higher priority.
Step 10	**tunnel mpls traffic-eng bandwidth** *bandwidth* **Example:** Router(config-if)# tunnel mpls traffic-eng bandwidth 5000	Configures the bandwidth for the MPLS traffic engineering tunnel.
Step 11	**tunnel mpls traffic-eng affinity** *affinity-value* **mask** *mask-value* **Example:** Router(config-if)# tunnel mpls traffic-eng affinity 0x0 mask 0x0	Configures the properties an MPLS TE tunnel requires in its links.
Step 12	**tunnel mpls traffic-eng path-option** *number* **explicit name** *explicit-path-name* **Example:** Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name best-way	Configures a path option for an MPLS TE tunnel. • The **explicit** keyword specifies that the path of the LSP is an IP explicit path.
Step 13	**tunnel mpls traffic-eng autoroute announce** **Example:** Router(config-if)# tunnel mpls traffic-eng autoroute announce	Causes the IGP to use the tunnel in its enhanced shortest path first (SPF) calculation.
Step 14	**end** **Example:** Router(config-if)# end	Exits interface configuration modes and enters privileged EXEC mode.
Step 15	**show ip rsvp sender** **Example:** Router# show ip rsvp sender	Displays the IP address used as the source for tunnel control traffic.
Step 16	Return to your originating procedure (NTP).	—

Example: Configure MPLS TE–Tunnel Source

The output of the **show running-config** command displays the tunnel source configuration. If the **tunnel source** command is not configured, the IP address specified in the IGP command **mpls traffic-eng router-id** is used.

```
Router# show running-config

Building configuration...
Current configuration: 3969 bytes
!
!

Router(config)# interface Tunnel1
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel source loopback1
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel destination 192.168.2.1
Router(config-if)# tunnel mpls traffic-eng priority 1 1
Router(config-if)# tunnel mpls traffic-eng bandwidth 5000
Router(config-if)# tunnel mpls traffic-eng affinity 0x0 mask 0x0
Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name BEST-WAY
Router(config-if)# tunnel mpls traffic-eng autoroute announce
```

DLP–J166 Create an MPLS–TE Tunnel Using CTC

Purpose	This procedure creates an MPLS–TE tunnel using CTC.
Tools/Equipment	None
Prerequisite Procedures	
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You cannot create an MPLS–TE tunnel and an MPLS–TP tunnel on the same interface.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to create an MPLS–TE tunnel.

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

Step 3 Click the **Layer2+** tab.

Step 4 From the left pane, click **Circuits**.

Step 5 Click the **MPLS TE Tunnels** tab.

Step 6 Click **Create**. The Circuit Creation wizard appears.

Step 7 In the Circuit Attributes screen of the wizard:

a) Enter the name of the service that you want to provision in the Name field.

b) Enter the description of the service in the Description field.

c) Check the **Bidirectional** check box to create a bidirectional tunnel. Uncheck the **Bidirectional** check box to create a unidirectional tunnel.

d) From the Admin State drop–down list, choose **UP** or **DOWN**. The default value is UP. Click **Next**.

e) Check the **Create PW Class automatically** check box to automatically create a pseudowire class with default values at the source and destination nodes of the MPLS-TE tunnel.

Step 8 In the Source screen of the wizard, choose the source node from the Node drop–down list.

Step 9 In the Tunnel Attributes area of the Source screen:

a) Enter the ID of the tunnel in the Tunnel ID field.

b) Enter the bandwidth required for a MPLS TE tunnel in the Bandwidth field in Kbps. The range is from 1 to 4294967295 Kbps.

c) (Optional) Click the **Auto BW Configuration** link.
The Auto BW Configuration dialog box appears. Complete the following:

1. Enter the frequency in the Frequency field. The range is 300 to 604800.
2. In the Bandwidth area, check the **Collect BW** check box or check the **Set BW** check box. If you check the **Set BW** check box, specify the minimum and maximum bandwidth.
3. Click **OK**.

d) Enter the Attribute values required for links carrying the MPLS TE tunnel in the Affinity field. A 32–bit decimal number. The Valid values range from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.

e) Enter the link attribute that the router must check in the Mask field. The value must be a 32–bit decimal number. The valid values range from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.

Note If a bit in the mask is 0, an attribute value of a link or that bit is irrelevant. If a bit in the mask is 1, the attribute value of a link and the required affinity of the tunnel for that bit must match. A tunnel can use a link if the tunnel affinity equals the link attributes and the tunnel affinity mask.

f) Enter the setup priority for an MPLS TE tunnel in the Setup Priority field. This priority is used when an LSP is signaled for this tunnel and determines which existing tunnels can be preempted. The valid values are from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non 0 priority.

g) Enter the reservation priority for an MPLS TE field in the Holding Priority field. This priority is the priority associated with an LSP for this tunnel and determines if it should be preempted by other LSPs that are being signaled. The valid values are from 0 to 7, where a lower number indicates a higher priority.

Note Setup priority and hold priority are typically configured to be equal, and setup priority cannot be numerically smaller than the hold priority.

h) From the Path Selection Metric drop–down list, choose **IGP** or **TE**. This selection specifies the metric type to use when calculating the path of the tunnel.

Step 10 Click the **Path Option Configuration** link. The Path Options dialog box appears. To configure a primary path for an MPLS TE tunnel:

a) Click **Add**. The Create Path Option dialog box appears.
b) In the Create Path Option dialog box, enter an ID for the path option type in the Index field.
c) From the Path Option Type drop–down list, choose **Explicit** or **Dynamic**. If you choose Dynamic, the path of the LSP is dynamically calculated. If you choose Explicit, the path of the LSP is an IP explicit path that you specify from the Name drop–down list.
d) (For Explicit path option) From the Name drop–down list, choose an explicit path name.
e) Check the **Bandwidth** check box and specify the bandwidth in Kbps.
f) Check the **Lockdown** check box to specify that the LSP cannot be reoptimized.
g) (For Explicit path option) Check the **Verbatim** check box to ignore the topology database verification process.
h) Click **OK** in the Create Path Option dialog box. The Path Options dialog box appears.
i) In the Path Options dialog box, select the path option you have created and click **OK**. The Source screen of the Circuit Creation wizard reappears.

Step 11 In the Path Protection area of the Source screen, specify the following to configure a secondary path for a MPLS TE tunnel:

a) Check the **Enable** check box to enable path protection for the primary path.
b) Enter the bandwidth value for the secondary path option in the Bandwidth field. The bandwidth value must be the same as the bandwidth value of the primary path option being protected.
c) Click the **Path Option Configuration** link. The Protected Path Options dialog box appears.
d) Click **Add**.
e) In the Create Path Option screen, enter an ID for the path option type in the Index field.
f) From the Path Option Type drop–down list, choose Explicit or Dynamic. If you choose Dynamic, the path of the LSP is dynamically calculated. If you choose Explicit, the path of the LSP is an IP explicit path that you specify from the Name drop–down list.
g) (For Explicit path option) From the Name drop–down list, choose an explicit path name.
h) Check the **Bandwidth** check box and specify the bandwidth in Kbps.
i) Check the **Lockdown** check box to specify that the LSP cannot be reoptimized.
j) (For Explicit path option) Check the **Verbatim** check box to ignore the topology database verification process.

Note It is recommended that the secondary path for an MPLS TE tunnel be an explicit path and not a dynamic path.

k) Click **OK** in the Create Path Option dialog box. The Protected Path Options dialog box appears.
l) In the Protected Path Options dialog box, select the protected path option you have created and click **OK**. The Source screen of the Circuit Creation wizard reappears.
m) In the Source screen of the Circuit Creation wizard, click **Next**.

Step 12 In the Destination screen of the Circuit Creation wizard, specify the following:

a) From the Node drop–down list, choose the destination node for the tunnel.

b) (For unidirectional tunnel) Check the **Unmanaged Node** check box when the destination node is not a node. If this check box is checked, enter the IP address of the unmanaged router in the Router ID field.
c) (For bidirectional tunnel) Specify the path options to configure the primary path and secondary path for the reverse tunnel.
d) Click **Finish** to create a MPLS–TE tunnel.

Step 13 Return to your originating procedure (NTP).

DLP-J167 Edit an MPLS–TE Tunnel Using CTC

Purpose	This procedure edits an MPLS–TE tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP–J166 Create an MPLS–TE Tunnel Using CTC, on page 274
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to edit an MPLS–TE tunnel.
Step 2 From the View menu, choose **Go to Network View**.
Step 3 Click the **Layer2+** tab.
Step 4 From the left pane, click **Circuits**.
Step 5 Click the **MPLS TE Tunnels** tab. The list of MPLS–TE tunnels appear.
Step 6 Select a tunnel to edit.
Step 7 Click **Edit**. The Tunnel Edit dialog box appears that displays the network map.
The nodes in the network map are the nodes, the ports are the ports, links between the nodes are L2 PPC or OchTrail tunnel links. The unmanaged nodes are not displayed in the network map.
Step 8 Click the **General** tab.
Step 9 Modify the values of parameters such as name, description, and admin state as required.
Step 10 Click **Apply** to save the configuration.
Step 11 Return to your originating procedure (NTP).

Understanding Explicit Path

You can configure multiple path options for a single tunnel. For example, there can be several explicit path options and a dynamic option for one tunnel.

If you specify the **dynamic** keyword, the software checks both the physical bandwidth of the interface and the available TE bandwidth to be sure that the requested amount of bandwidth does not exceed the physical bandwidth of any link. To oversubscribe links, you must specify the **explicit** keyword. If you use the **explicit** keyword, the software only checks how much bandwidth is available on the link for TE; the amount of bandwidth you configure is not limited to how much physical bandwidth is available on the link.

NTP-J52 Configure Explicit Paths

Purpose	This procedure configures explicit paths.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J168 Create an Explicit Path Using Cisco IOS Commands, on page 278
- DLP-J169 Configure Explicit Paths for Secondary Paths Using Cisco IOS Commands, on page 279
- DLP-J170 Create an Explicit Path Using CTC, on page 281

Stop. You have completed this procedure.

DLP-J168 Create an Explicit Path Using Cisco IOS Commands

Purpose	This procedure creates an explicit path using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ip explicit-path** {**name** *path-name* | **identifier** *number*} [**enable** | **disable**] **Example:** Router(config)# ip explicit-path name path-tunnel1	Enters IP explicit path configuration mode and creates or modifies the specified path.
Step 4	**next-address** [**loose** | **strict**] *ip-address* **Example:** Router(cfg-ip-expl-path)# next-address loose 192.168.40.40	Specifies the next IP address in the explicit path.
Step 5	**end** **Example:** Router(cfg-ip-expl-path)# end	Returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J169 Configure Explicit Paths for Secondary Paths Using Cisco IOS Commands

Purpose	This procedure configures the explicit paths for secondary paths using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None

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

This procedure configures an explicit path. Use this procedure to specify a secondary path that does not include common links or nodes associated with the primary path in case those links or nodes go down.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ip explicit-path** {**name** *path-name* | **identifier** *number*} [**enable** | **disable**] **Example:** Router(config)# ip explicit-path name path3441 enable	Creates or modifies the explicit path and enters IP explicit path configuration mode.
Step 4	**index** *index* **next-address [loose | strict]** *ip-address* **Example:** Router(cfg-ip-expl-path)# index 1 next-address 10.0.0.1	Inserts or modifies a path entry at a specific index. The IP address represents the node ID.
Step 5	**exit** **Example:** Router(cfg-ip-expl-path)# exit	Exits IP explicit path configuration mode and enters global configuration mode.
Step 6	Return to your originating procedure (NTP).	—

Example: Configure Explicit Paths for Secondary Paths

In the following example, the explicit path is named path3441. There is an **index** command for each router. If there is failure, the secondary path is used.

```
Router(config)# ip explicit-path name path3441 enable
Router(cfg-ip-expl-path)# index 1 next 10.0.0.1
```

```
Explicit Path name path3441:
    1: next-address 10.0.0.1

Router(cfg-ip-expl-path)# index 2 next 10.0.0.2
Explicit Path name path3441:
    1: next-address 10.0.0.1
    2: next-address 10.0.0.2

Router(cfg-ip-expl-path)# index 3 next 10.0.1.1
Explicit Path name path3441:
    1: next-address 10.0.0.1
    2: next-address 10.0.0.2
    3: next-address 10.0.1.1

Router(cfg-ip-expl-path)# index 4 next 10.0.1.2
Explicit Path name path3441:
    1: next-address 10.0.0.1
    2: next-address 10.0.0.2
    3: next-address 10.0.1.1
    4: next-address 10.0.1.2

Router(cfg-ip-expl-path)# exit
```

DLP-J170 Create an Explicit Path Using CTC

Purpose	This procedure creates an explicit path.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note The secondary path for an MPLS TE tunnel can be only an explicit path and not a dynamic path.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to create an explicit path.

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

Step 3 Click the **Layer2+** tab.

Step 4 From the left pane, click **Provisioning**.

Step 5 Click **Explicit Paths**.

Step 6 Click **Create**. The Create Explicit Path dialog box appears that displays the network map.

Step 7 Enter the name for the explicit path in the Name field.

Step 8 Specify one of the following options for the explicit path type:

a) Click the **Strict** radio button to specify that all the hops will be included in the explicit path calculation.

b) Click the **Exclude** radio button to specify the hops that must be avoided in the explicit path calculation.
c) Click the **Loose** radio button. If you select this option, all the hops need not be specified; the missing hops can be any of the LSRs in the path.

Step 9 If you want to include nodes in the explicit path:

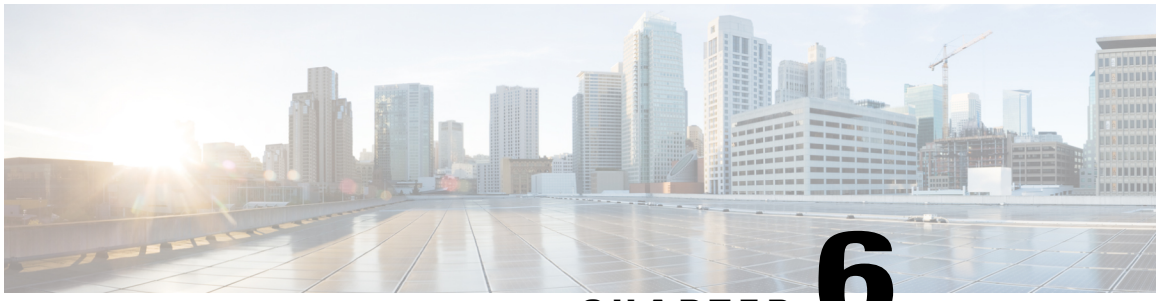
a) Select a node on the network map and click **Add**. The Explicit Path wizard appears.
b) Review the node information and click **Apply**. The selected node appears in the Included Links/Included Nodes/Excluded Nodes area of the Create Explicit Path dialog box.

Step 10 If you want to include an unmanaged node (non node) in the explicit path:

a) Click **Add** without selecting any node on the network map. The Add Node dialog box appears.
b) Check the **Unmanaged** check box.
c) Enter the IP address of the unmanaged node in the IP field.
d) Click **Apply** and close the Add Node dialog box. The unmanaged node appears in the Included Links/Included Nodes/Excluded Nodes area of the Create Explicit Path dialog box.

Step 11 Click **Apply** in the Create Explicit Path dialog box and close the dialog box.

Step 12 Return to your originating procedure (NTP).



CHAPTER 6

Configuring MPLS–Transport Profile

This chapter describes the MPLS–Transport Profile and procedures to configure MPLS–Transport Profile.

Understanding Multiprotocol Label Switching Transport Profile

Multiprotocol Label Switching Transport Profile (MPLS–TP) is a carrier–grade packet transport technology that enables service providers to move from Synchronous Optical Networking (SONET) and Synchronous

Digital Hierarchy (SDH) time–division multiplexing (TDM) to packet switching. MPLS–TP enables MPLS to be deployed in a transport network to support packet transport services with a similar degree of predictability to that found in existing transport networks.

The goal of MPLS–TP is to provide connection–oriented transport for packet and TDM services over optical networks leveraging the widely deployed MPLS technology. Operations, Administration, and Maintenance (OAM) and resiliency features are defined and implemented in MPLS–TP to ensure the capabilities needed for carrier–grade packet transport networks—scalable operations, high availability, performance monitoring and multidomain support.

MPLS–TP defines a profile of MPLS targeted at transport applications and networks. This profile specifies the MPLS characteristics and extensions required to meet the transport requirements.

Note MPLS–TP supports only point–to–point Layer 2 VPN service in this release. The point–to–point Layer 2 VPN service is called Virtual Private Wire Service (VPWS). MPLS–TP supports only static pseudowires in this release.

Key Features

The key features of MPLS–TP are as follows:

- Connection–oriented.
- Carries Layer 3 and Layer 2 services.
- Runs over IEEE Ethernet PHYs, OTN, WDM and so on.
- Static and bidirectional label-switched path (LSP) provisioning.
- OAM functions similar to those available in traditional optical transport networks such as SONET or SDH are provided. These OAM functions belong to the MPLS–TP data plane and are independent from the control plane.
- Fault propagation through Bidirectional Fault Detection (BFD), Link Down Indication (LDI), and Lockout Request (LKR) messages.
- 1:1 revertive path protection.
- IP–less provisioning of tunnels.
- Network provisioning through CTC.
- Traffic switchover time from working LSP to protect LSP and vice versa is up to 50 milliseconds.

Planes in MPLS–TP

The three planes in MPLS–TP perform the following functions:

Plane	Functions
Control plane through CTC	• Constraint-based path computation • Primary and backup LSPs definition • Auto-discovery of existing tunnels • Fault management
Data plane	Forwards data packets
Management plane	Configuration

The control plane is decoupled from the data plane such that the failures in the control plane do not affect the data plane and vice versa.

Restrictions

The following restrictions apply to MPLS–TP:

- Penultimate hop popping is not supported. Only ultimate hop popping is supported, because the label mappings are configured at the MPLS–TP end points.
- MPLS–TP link numbers are not configured on the interfaces for which Multiprotocol Label Switching Traffic Engineering (MPLS-TE) is enabled and vice versa.
- IPv6 addressing is not supported.

Understanding MPLS–TP Operations, Administration, and Maintenance

Several Operations, Administration, and Maintenance (OAM) protocols and messages support the provisioning and maintenance of MPLS–TP tunnels and bidirectional LSPs. The OAM messages are used for fault management, connection verification, continuity check, and other functions. The timers can be configured for each OAM message.

The following OAM messages are forwarded along the specified LSP:

- OAM fault management—Link Down Indication (LDI) and Lockout Request (LKR) messages
- OAM connection verification—ping and traceroute messages
- OAM continuity check—Bidirectional Fault Detection (BFD) messages. min_tx and min_rx are 4 milliseconds.

The following messages are forwarded along the specified pseudowire:

- Static pseudowire OAM messages
- Pseudowire ping and traceroute messages
- Pseudowire BFD messages. min_tx and min_rx are 50 milliseconds.

LDI and LKR Messages

The LDI messages are generated at midpoint nodes when a link failure is detected. The LKR messages are sent from a midpoint node to the reachable endpoint when an interface is administratively shut. When a **lockout** command is configured on either the working or the protect LSP, an LDI message is sent from the local endpoint to the remote endpoint.

LSP Ping and Trace Messages

For MPLS–TP connectivity verification, **ping mpls tp** and **trace mpls tp** commands can be used to specify that the echo requests must be sent along the working LSP or the protect LSP, or the locked out working or protect LSP.

BFD Messages

BFD sessions running on MPLS-TP LSPs can be configured. These sessions run on both the working LSP and the protect LSP. BFD provides continuity check for MPLS–TP LSPs to detect forwarding failures between two adjacent routers. When BFD is enabled on an MPLS–TP tunnel interface, the MPLS–TP client creates separate BFD sessions for working and protect LSPs. A single set of BFD timers is configured on the tunnel that applies to both the working and protect LSPs.

Multiprotocol Label Switching Transport Profile Configuration Procedures

The following procedures can be performed using Cisco IOS commands to configure MPLS–TP:

- DLP-J95 Configure Global Settings for Multiprotocol Label Switching Transport Profile Using Cisco IOS Commands, on page 287
- DLP-J103 Specify Static Label Range Using Cisco IOS Commands, on page 291
- DLP-J97 Create and Configure BFD Templates Using Cisco IOS Commands, on page 293
- DLP-J99 Configure an MPLS–TP Link Using Cisco IOS Commands, on page 298
- DLP-J226 Configure an MPLS–TP Link Without IP Addresses Using Cisco IOS Commands, on page 300
- DLP-J101 Create a Static OAM Class Using Cisco IOS Commands, on page 303
- DLP-J105 Configure Tunnel Midpoints Using Cisco IOS Commands, on page 309
- DLP–J106 Configure Tunnel Endpoints Using Cisco IOS Commands, on page 312

The following procedures can be performed using CTC to configure MPLS–TP:

- DLP-J96 Configure Global Settings for Multiprotocol Label Switching Transport Profile Using CTC, on page 289
- DLP-J104 Specify Static Label Range Using CTC, on page 292
- DLP-J98 Create and Configure BFD Templates Using CTC, on page 295
- DLP-J100 Configure an MPLS–TP Link Number Using CTC, on page 301
- DLP-J102 Create a Static OAM Class Using CTC, on page 304

• DLP-J107 Create an MPLS–TP Tunnel Using CTC, on page 316
• DLP-J208 Edit MPLS–TP Tunnel Attributes Using CTC, on page 319

NTP-J36 Configure Global Settings for Multiprotocol Label Switching Transport Profile

Purpose	This procedure configures the global settings for MPLS–TP.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J95 Configure Global Settings for Multiprotocol Label Switching Transport Profile Using Cisco IOS Commands, on page 287
- DLP-J96 Configure Global Settings for Multiprotocol Label Switching Transport Profile Using CTC, on page 289

Stop. You have completed this procedure.

DLP-J95 Configure Global Settings for Multiprotocol Label Switching Transport Profile Using Cisco IOS Commands

Purpose	This procedure configures the global settings for MPLS–TP using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls tp** **Example:** Router(config)# mpls tp	Enters MPLS–TP configuration mode, from where you can configure MPLS–TP parameters for the router.
Step 4	**router-id** *ip-address* **Example:** Router(config-mpls-tp)#mpls label range 4001 8000 static 16 4000 **Example:** Router(config-mpls-tp)# router-id 209.165.200.225	Specifies the default MPLS–TP router ID. This address is used as the source node ID for all the MPLS–TP tunnels configured on the router. Configure MPLS label range before configuring router ID.
Step 5	**global-id** *number* **Example:** Router(config-mpls-tp)# global-id 1	Specifies the default global ID used for all the endpoints and midpoints. The valid range is from 0 to 2147483647. The default value is 0.
Step 6	**fault-oam refresh-timer** *seconds* **Example:** Router(config-mpls-tp)# fault-oam refresh-timer 10	Specifies the maximum time between successive fault OAM messages specified in seconds. The valid range is from 1 to 255. The default value is 20.
Step 7	**wtr-timer** *seconds* **Example:** Router(config-mpls-tp)# wtr-timer 25	Specifies the wait-to-restore (WTR) timer. This timer controls the length of time to wait before reverting to the original working path following the repair of a fault on the original working path. The valid range is from 0 to 2147483647. **Note** For CPT 50 in ring mode, configure the wait-to-restore (WTR) timer to 60 seconds. In other cases, configure the wait-to-restore (WTR) timer to 30 seconds.

	Command or Action	Purpose
Step 8	**exit** **Example:** Router(config-mpls-tp)# exit	Returns the router to global configuration mode.
Step 9	Return to your originating procedure (NTP). **Example:** —	

Example: Configure Global Settings for MPLS–TP

The following example shows how to configure the global settings for MPLS–TP using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# mpls tp
Router(config-mpls-tp)# router-id 209.165.200.225
Router(config-mpls-tp)# global-id 1
Router(config-mpls-tp)# fault-oam refresh-timer 10
Router(config-mpls-tp)# wtr-timer 25
Router(config-mpls-tp)# exit
```

DLP-J96 Configure Global Settings for Multiprotocol Label Switching Transport Profile Using CTC

Purpose	This procedure configures the global settings for MPLS–TP using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to configure the global settings for MPLS–TP.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Provisioning** tab.

Step 5 From the left pane, click **MPLS TP**.

Step 6 Click the **Global Settings** tab.

Step 7 Enter the router IP address in the Node ID field. This IP address need not be the loopback IP address.

Step 8 In the TP Fault OAM area, enter the number of seconds in the Refresh Timer field to specify how often the static OAM packets must be sent out.

Step 9 Click **Apply** to save the configuration.

Step 10 Return to your originating procedure (NTP).

NTP-J40 Specify Static Label Range

Purpose	This procedure specifies the static label range.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J103 Specify Static Label Range Using Cisco IOS Commands, on page 291
- DLP-J104 Specify Static Label Range Using CTC, on page 292

Stop. You have completed this procedure.

DLP-J103 Specify Static Label Range Using Cisco IOS Commands

Purpose	This procedure specifies the static label range using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

You must specify the static label range before provisioning the MPLS–TP tunnel.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls label range** *dyn-min-value dyn-max-value* **static** *static-min-value static-max-value* **Example:** Router(config)# mpls label range 1000 8000 static 16 999	Specifies the static label range that applies to both the pseudowire and MPLS–TP tunnel. The valid range of static and dynamic labels is from 16 to 8000. The dynamic label range is automatically calculated based on the values specified in the static label range.
Step 4	Return to your originating procedure (NTP). **Example:** —	

Example: Specify Static Label Range

The following example shows how to specify the static label range using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# mpls label range 1000 8000 static 16 999
```

DLP-J104 Specify Static Label Range Using CTC

Purpose	This procedure specifies the static label range using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

You must specify the static label range before provisioning the MPLS–TE or MPLS–TP tunnel.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to specify the static label range.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Provisioning** tab.

Step 5 From the left pane, click **Label Range**.

Step 6 In the MPLS Static Label Range area, enter the minimum label value in the Min Label field.

Step 7 Enter the maximum label value in the Max Label field.
The static label range specified in the static label applies to both the pseudowire and MPLS–TP tunnel. The valid range of static and dynamic labels is from 16 to 8000. You do not need to specify the values for dynamic labels. The dynamic label range is automatically calculated by CTC based on the values specified in the static label range. For example, if you choose 100 to 1000 for static labels, the dynamic label range is set to 1001 to 8000.

Step 8 Click **Apply** to specify the static label range.

Step 9 Return to your originating procedure (NTP).
To support the TDM interoperability, CTC allocates two unique labels to each TDM SFP, if provisioned in CTC mode. These two unique labels take the static label space of CPT. If TDM SFP is provisioned in IOS mode, unique labels will not be assigned.

Prior to 9.701, TDM SFP default labels value were 16 & 16.

Understanding Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) provides a low–overhead, short–duration method of detecting failures in the forwarding path between two adjacent routers, including interfaces, data links, and forwarding planes.

BFD is a fault detection protocol that is enabled at the interface level. The BFD asynchronous mode, which depends on sending of BFD control packets between two systems to activate and maintain BFD neighbor sessions between routers, is supported. Therefore, to create a BFD session, BFD must be configured on both systems (or BFD peers). When BFD is enabled on the interfaces, a BFD session is created, BFD timers are negotiated, and the BFD peers begin to send BFD control packets to each other at the negotiated interval.

BFD provides continuity check for MPLS–TP LSPs to detect forwarding failures between two adjacent routers. When BFD is enabled on the MPLS–TP tunnel interface, MPLS–TP client creates separate BFD sessions for working and protect LSPs. A single set of BFD timers is configured on the tunnel that applies to both the working and protect LSPs.

NTP-J37 Configure BFD Templates

Purpose	This procedure creates and configures BFD templates.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J97 Create and Configure BFD Templates Using Cisco IOS Commands, on page 293
- DLP-J98 Create and Configure BFD Templates Using CTC, on page 295

Stop. You have completed this procedure.

DLP-J97 Create and Configure BFD Templates Using Cisco IOS Commands

Purpose	This procedure creates and configures a BFD template using Cisco IOS commands.

Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**bfd-template single-hop** *template-name* **Example:** Router(config)# bfd-template single-hop bfdtemplate1	Creates a BFD template and enters BFD configuration mode. The **bfd-template** command allows you to create a BFD template and enters BFD configuration mode. The template can be used to specify a set of BFD interval values. You can then invoke the BFD template when you set up the MPLS–TP tunnel.
Step 4	**interval microseconds {both** *microseconds* | **min-tx** *microseconds* **min-rx** *microseconds*} [**multiplier** *multiplier-value*] **Example:** Router(config-bfd)# interval microseconds both 3300 multiplier 3	Configures the transmit and receive intervals in microseconds between BFD packets, and specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that a peer is unavailable. The valid range for min-tx and min-rx is from 3300 to 999000 microseconds. The valid range for multiplier is from 2 to 50.
Step 5	**interval {both** *milliseconds* | **min-tx** *milliseconds* **min-rx** *milliseconds*} [**multiplier** *multiplier-value*] **Example:** Router(config-bfd)# interval both 120 multiplier 3	Configures the transmit and receive intervals in milliseconds between BFD packets, and specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that a peer is unavailable.
Step 6	**exit** **Example:**	Exits BFD configuration mode and returns the router to global configuration mode.

	Command or Action	Purpose
	Router(config-bfd)# exit	
Step 7	Return to your originating procedure (NTP). **Example:** —	

Example: Create and Configure BFD Templates

The following example shows how to create and configure a BFD template using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# bfd-template single-hop bfdtemplate1
Router(config-bfd)# interval microseconds both 3300 multiplier 3
Router(config-bfd)# exit
```

DLP-J98 Create and Configure BFD Templates Using CTC

Purpose	This procedure creates and configures a BFD template using CTC. You need to enable BFD on both the source and destination nodes of the MPLS–TP tunnel.
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 NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to create and configure a BFD template.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Provisioning** tab.

Step 5 From the left pane, click **MPLS TP**.

Step 6 Click the **BFD Template** tab.

Step 7 Click **Create**. The **Create BFD Template** dialog box appears.

Step 8 Enter the name of the BFD template in the Name field.
The **Single Hop** check box is checked and cannot be changed.

Step 9 Specify the time unit in milliseconds or microseconds.

Step 10 To specify the same interval for transmit and receive between BFD packets:

a) Check the **Use Single Value** check box.

b) Enter the interval between BFD packets in the Interval Value field. The range is from 4 to 999 milliseconds.

Step 11 To specify different intervals for transmit and receive between BDF packets:

a) Enter the transmit interval between BFD packets in the Min_Tx Interval field. The range is from 4 to 999 milliseconds.

b) Enter the receive interval between BFD packets in the Min_Rx Interval field. The range is from 4 to 999 milliseconds.

Step 12 Enter the number of consecutive BFD control packets that must be missed before BFD declares that a peer is unavailable in the Multiplier field.

Step 13 Click **OK** to create and configure a BFD template.

Step 14 Return to your originating procedure (NTP).

Understanding Multiprotocol Label Switching Transport Profile Link Numbers

The MPLS–TP link numbers are configured only on the physical interfaces. Only one MPLS–TP link number can be configured for each interface. The user-assigned link numbers must be unique within the router. The **show mpls tp link-number** command shows all the configured links on the router.

The MPLS–TP link numbers are not assigned to bundled interfaces and virtual interfaces.

The MPLS–TP link numbers can be configured either using the next hop IP address or the MAC address. The valid range of MPLS–TP link number is from 1 to 10000.

Note For Release 9.7, the valid range of MPLS-TP link number is from 1 to 1000.

When you configure a MPLS–TP link using an IP address for the next hop, you use the following commands, where 209.165.200.226 is the IP address of the next hop router:

```
interface TenGigabitEthernet4/1
ip address 209.165.200.225 255.255.255.0
mpls tp link 1 ipv4 209.165.200.226
```

MPLS-TP over Ethernet Without IP Addressing

Transport networks usually do not use IP addresses. You can configure MPLS–TP with links that do not require IP addresses. Instead, Ethernet MAC addresses are used to establish MPLS adjacency between the nodes on Ethernet links. MPLS–TP uses IP only to determine the MAC address of the next hop device through Address Resolution Protocol (ARP).

When you configure a MPLS–TP link without an IP address, you use the following commands:

```
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# medium p2p
Router(config-if)# mpls tp link 1
```

You can use these commands whether the interface has an IP address or not. However, the commands are primarily used when the router and its neighbor router do not have IP addresses.

The **medium p2p** command changes an interface that allows multiple connections to a point-to-point interface. This command allows the router to send and receive all the MPLS-TP packets using a common multicast MAC address knowing that it is communicating with only one other device.

An interface that is natively point-to-point, such as serial, does not require the **medium p2p** command.

Alternatively, you can configure the unicast MAC address of the next-hop device as follows:

```
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# medium p2p
Router(config-if)# mpls tp link 1 tx-mac 0000.0c00.1234
```

You can also configure to transmit and receive on some other multicast address as follows:

```
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# medium p2p
Router(config-if)# mpls tp link 1 tx-mac 0100.0c99.8877 rx-mac 0100.0c99.8877
```

Note When a MPLS–TP link is configured without an IP address on an Ethernet interface, Cisco uses an IEEE Bridge Group MAC address (0180.c200.0000) for communication by default.

NTP-J38 Configure an MPLS–TP Link

Purpose	This procedure configures an MPLS-TP link number on a physical interface.
Tools/Equipment	None
Prerequisite Procedures	None

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

Procedure

Perform any of the following procedures as needed:

- DLP-J99 Configure an MPLS–TP Link Using Cisco IOS Commands, on page 298
- DLP-J226 Configure an MPLS–TP Link Without IP Addresses Using Cisco IOS Commands, on page 300
- DLP-J100 Configure an MPLS–TP Link Number Using CTC, on page 301

Stop. You have completed this procedure.

DLP-J99 Configure an MPLS–TP Link Using Cisco IOS Commands

Purpose	This procedure configures an MPLS-TP link number on a physical interface using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**ip address** *ip-address mask-value* **Example:** Router(config-if)# ip address 209.165.200.225 255.255.255.0	Assigns an IP network address and network mask to the interface.
Step 5	**ip rsvp bandwidth** *value* **Example:** Router(config-if)# ip rsvp bandwidth 100	Enables Resource Reservation Protocol (RSVP) for IP on this interface. The valid range is from 1 to 10000000 kpbs. If you configure non-zero bandwidth for the MPLS–TP tunnel or at a midpoint LSP, ensure that the interface to which the output link is attached has enough available bandwidth. For example, if three tunnel LSPs run over link 1 and each LSP was assigned 1000 with the **tp bandwidth** command, the interface associated with link 1 needs bandwidth of 3000 with the **ip rsvp bandwidth** command.
Step 6	**mpls tp link** *link-num* {**ipv4** *nexthop-ip-address* | **tx-mac** *mac-address* } **Example:** Router(config-if)# mpls tp link 1 ipv4 209.165.200.226	Configures the MPLS–TP link either with the IPv4 address of the next hop router or using a per-interface transmit multicast MAC address. The *link-num* is a number assigned to the link. It must be unique to the device. Only one link number can be assigned per interface. The valid range is from 1 to 10000. **Note** For Release 9.7, the valid range is from 1 to 1000.
Step 7	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
Step 8	Return to your originating procedure (NTP). **Example:** —	

DLP-J226 Configure an MPLS–TP Link Without IP Addresses Using Cisco IOS Commands

Purpose	This procedure configures an MPLS-TP link without IP addresses using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**medium p2p** **Example:** Router(config-if)# medium p2p	Changes an interface that allows multiple connections to a point-to-point interface. This command allows the router to send and receive all the MPLS–TP packets using a common multicast MAC address knowing that it is communicating with only one other device.
Step 5	**mpls tp link** *link-num* {**ipv4** *ip-address* | **tx-mac** *mac-address* **rx-mac** *mac-address*} **Example:** Router(config-if)# mpls tp link 1 tx-mac 0000.0c00.1234	Configures an MPLS–TP link without the IP address. The **tx-mac** keyword is available on Ethernet interfaces, but the interface must be point-to-point to configure the value of **tx-mac** as a multicast MAC address. The **rx-mac** keyword is available only when the **tx-mac** keyword is used and only when the interface is point-to-point.

	Command or Action	Purpose
Step 6	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
Step 7	Return to your originating procedure (NTP). **Example:** —	

Example: Configure MPLS–TP Link Numbers Without IP Addresses

The following example shows how to create an MPLS–TP link without an IP address using Cisco IOS commands:

```
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# medium p2p
Router(config-if)# mpls tp link 1
```

The following example shows how to configure the unicast MAC address of the next-hop device using Cisco IOS commands:

```
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# medium p2p
Router(config-if)# mpls tp link 1 tx-mac 0000.0c00.1234
```

Th following example shows how to configure the transmit and receive parameters for a different multicast address using Cisco IOS commands:

```
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# medium p2p
Router(config-if)# mpls tp link 1 tx-mac 0100.0c99.8877 rx-mac 0100.0c99.8877
```

DLP-J100 Configure an MPLS–TP Link Number Using CTC

Purpose	This procedure configures an MPLS–TP link number on a physical interface, using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to configure an MPLS-TP link number.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Provisioning** tab.

Step 5 From the left pane, click **MPLS TP**.

Step 6 Click the **Link Config** tab.

Step 7 Click **Create**. The **Create Link** dialog box appears.

Step 8 From the Slot drop-down list, choose a slot to configure the MPLS–TP link.

Step 9 From the Port drop-list, choose a port.

Step 10 Enter a link number in the Link Number field.

Step 11 To configure the link with the IP address:

a) Check the **Arp** check box.

b) Enter the next hop IP address in the Next Hop IP field.

Note The next hop IP address must be in the same subnet as the IP address of the interface.

Step 12 To configure the MPLS-TP link number with the MAC address, complete one of the following options:

a) Check the **P2P Link** check box.
In the Tx–Mac area, enter the unicast or multicast transmit MAC address in the Mac Address field.

In the Rx–Mac area, enter the unicast or multicast receive MAC address in the Mac Address field.

b) Check the **P2P Link** check box.
In the Tx–Mac area, enter the unicast or multicast transmit MAC address in the Mac Address field.

Step 13 Click **OK** to create the MPLS–TP link.

Step 14 Return to your originating procedure (NTP).

NTP-J39 Create a Static OAM Class

Purpose	This procedure creates a static OAM class.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J101 Create a Static OAM Class Using Cisco IOS Commands, on page 303
- DLP-J102 Create a Static OAM Class Using CTC, on page 304

Stop. You have completed this procedure.

DLP-J101 Create a Static OAM Class Using Cisco IOS Commands

Purpose	This procedure creates a static OAM class using Cisco IOS commands. You must create a static OAM class for static pseudowire OAM that specifies the OAM timeout refresh intervals.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**pseudowire-static-oam class** *class-name* **Example:** Router(config)# pseudowire-static-oam class oam-class1	Specifies the name of the static OAM class.

	Command or Action	Purpose
Step 4	**timeout refresh send** *seconds* **Example:** Router(config-st-pw-oam-class)# timeout refresh send 20	Specifies how often the static OAM packets must be sent out. The valid range is from 1 to 4095 seconds. The default value is 30 seconds.
Step 5	**exit** **Example:** Router(config-st-pw-oam-class)# exit	Returns the router to global configuration mode.
Step 6	Return to your originating procedure (NTP). **Example:** —	

Example: Create a Static OAM Class

The following example shows how to create a static OAM class using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# pseudowire-static-oam class oam-class1
Router(config-st-pw-oam-class)# timeout refresh send 20
Router(config-st-pw-oam-class)# exit
```

DLP-J102 Create a Static OAM Class Using CTC

Purpose	This procedure creates a static OAM class using CTC. You must create a static OAM class for static pseudowire OAM that specifies the OAM timeout refresh intervals.
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 NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to create a static OAM class.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Provisioning** tab.

Step 5 From the left pane, click **MPLS TP**.

Step 6 Click the **Static OAM Class** tab.

Step 7 Click **Create**. The **Create Static OAM Class** dialog box appears.

Step 8 Enter the name of static OAM class in the Name field.

Step 9 Enter the number of seconds in the Refresh Send field to specify how often the static OAM packets must be sent out.

Step 10 Click **OK** to create a static OAM class.

Step 11 Return to your originating procedure (NTP).

NTP-J67 Create a Provisionable Patchcord Using CTC

Purpose	This procedure creates a Provisionable Patchcord (PPC), also called a virtual link, using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note PPCs can be created only between ports of the same size (1GE-1GE or 10GE-10GE) for Client/Trunk to Client/Trunk (layer 2) PPCs.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to create a provisionable patchcord.

Step 2 In the node view (single-shelf mode), click the **Provisioning > Comm Channels > PPC** tabs. Alternatively, in network view, click the **Provisioning > Provisionable Patchcord (PPC)** tabs.
PPCs can be created in either node or network view. However, if you create the PPC in node view, the PPC origination ports will be restricted to the cards installed on the node. Therefore, choose node view only if you know that the PPC origination port resides on a card installed in the node.

Step 3 Click **Create**. The PPC Attributes screen of the PPC Creation wizard appears.

Step 4 Choose the Client/Trunk to Client/Trunk (L2) link type.
This link type creates a PPC between two NNI client or trunk ports.

Step 5 Click **Next**.

Step 6 In the PPC Origination screen of the wizard, specify the following:

- From the Node drop-down list, choose the node where the PPC will originate.
- From the Slot drop-down list, choose the slot where the PPC will originate.
- From the Port drop-down list, choose the port where the PPC will originate.

The ID field displays the ID automatically assigned to the PPC.

Step 7 Click **Next**.

Step 8 In the PPC Termination screen of the wizard, specify the following:

- From the Node drop-down list, choose the node where the PPC will terminate.
- From the Slot drop-down list, choose the slot where the PPC will terminate.
- From the Port drop-down list, choose the port where the PPC will terminate.

The ID field displays the ID automatically assigned to the PPC.

Step 9 Click **Next**.

Step 10 In the PPCs ID page, review the PPC information. If the PPC information is correct, click **Finish**. If you need to make corrections, click **Back** and return to the wizard page where you want to change the information.
Stop. You have completed this procedure.

Understanding Multiprotocol Label Switching Transport Profile Tunnels

An MPLS–TP tunnel consists of a pair of unidirectional tunnels providing a bidirectional LSP. Each unidirectional tunnel can be protected with a protect LSP that activates automatically upon failure. MPLS–TP tunnels are provisioned manually at their endpoints across the network.

Tunnel Identifiers

MPLS–TP tunnel identifiers uniquely identify an MPLS–TP tunnel within the network. The tunnel identifier consists of a global identifier, a node identifier, and a tunnel number for each endpoint of the MPLS–TP LSP.

The node identifier is an IP address for an interface on the endpoint router. The tunnel number is the tunnel–tp number assigned when the tunnel–tp virtual interface is created on the endpoint router.

Tunnel Source

The tunnel source is the MPLS–TP node identifier of the endpoint router that is configured. This tunnel source can be specified to override the router-id configured in the global MPLS-TP configuration.

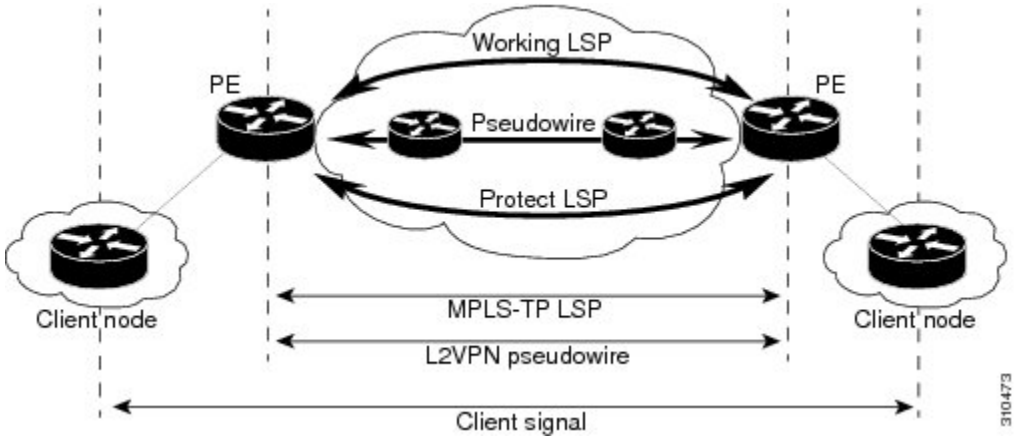
Tunnel Destination

The tunnel destination is the MPLS–TP node identifier of the remote endpoint router. The destination tunnel number is the virtual interface number assigned to the remote tunnel interface when it is provisioned. This destination tunnel number can be optionally configured. If the destination tunnel number is not configured, it defaults to the local tunnel number.

Understanding MPLS–TP LSPs

MPLS–TP LSPs are bidirectional and corouted and are comprised of two unidirectional LSPs that are supported by the MPLS forwarding infrastructure. The static and bidirectional MPLS–TP LSPs can be configured either through CTC or Cisco IOS commands. The LSPs are configured and managed without a control plane. The MPLS–TP LSPs have a fixed path. The statically defined LSP does not require an Interior Gateway Protocol (IGP).

Figure 52: MPLS–TP LSP



MPLS–TP LSPs are not supported over a Link Aggregation Group (LAG). The static pseudowire is the only traffic carried over MPLS–TP LSPs in this release.

LSP Path Protection

MPLS–TP LSPs support 1:1 revertive path protection. The working and protect LSPs can be configured as part of configuring MPLS–TP tunnels. The working LSP is the primary LSP used to route the traffic. The

protect LSP is a backup for the working LSP. When the working LSP fails, the traffic is switched to the protect LSP until the working LSP is restored, at which time the forwarding reverts to the working LSP.

LSP Number

The LSP number is assigned when the MPLS–TP LSP is configured. The default value of the LSP number is 0 for the working LSP and 1 for the protect LSP. You can edit LSP numbers.

LSP Ping and Trace

The LSP **ping** and **trace** commands are supported on MPLS–TP bidirectional LSPs and pseudowires.

LSP Lockout

The working LSP or protect LSP can be locked out. Only one LSP must be locked out at a time. When the LSP is currently locked out, the **lockout** command is not available in the other LSP configuration submode. The lockout of a working or protect LSP is cleared using the **no lockout** command.

When the LSP is locked out, the user traffic is not forwarded over the locked out LSP. However, the OAM traffic and BFD traffic is forwarded over the locked out LSP.

Because an MPLS-TP tunnel is statically configured, the possibility exists that the working LSP could be locked out at one MPLS-TP tunnel endpoint and the protect LSP could be locked out at the other MPLS-TP tunnel endpoint. If this occurs, the MPLS-TP tunnel is deadlocked and non-functional until the lockout configuration is changed at one of the endpoints.

LSP Shutdown

When the LSP is shut down, the LDI messages, user traffic, and OAM traffic are not sent.

Tunnel Midpoints and Endpoints

Tunnel LSPs, whether endpoint or midpoint, use the same identifying information. However, it is entered differently.

- At the midpoint, all the information for the LSP is specified with the **mpls tp lsp** command, which enters the submode for configuring forward and reverse information for forwarding.
- At the midpoint, determining which end is source and which end is destination is arbitrary. That is, if you are configuring a tunnel between your router and a coworker's router, your router is the source. However, your coworker considers his or her router to be the source. At the midpoint, either router could be considered the source. At the midpoint, the forward direction is from source to destination, and the reverse direction is from destination to source.
- At the endpoint, the source information comes either from the global router ID or from locally configured information using the **tp source** command after you enter the command **interface tunnel-tp** *number* command, where *number* is the source tunnel number.
- At the endpoint, the remote information (destination) is configured using the **tp destination** command after you enter the command **interface tunnel-tp** *number*. The **tp destination** command includes the destination node ID, optionally the global ID, and optionally the destination tunnel number. If you do not specify the destination tunnel number, the source tunnel number is used.
- At the endpoint, the LSP number is configured in working-lsp or protect-lsp submode. The default value is 0 for the working LSP and 1 for the protect LSP.

NTP-J41 Configure an MPLS-TP Tunnel

Purpose	This procedure configures an MPLS–TP tunnel.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J105 Configure Tunnel Midpoints Using Cisco IOS Commands, on page 309
- DLP–J106 Configure Tunnel Endpoints Using Cisco IOS Commands, on page 312
- DLP-J107 Create an MPLS–TP Tunnel Using CTC, on page 316
- DLP-J208 Edit MPLS–TP Tunnel Attributes Using CTC, on page 319

Stop. You have completed this procedure.

DLP-J105 Configure Tunnel Midpoints Using Cisco IOS Commands

Purpose	This procedure configures the midpoints for the MPLS–TP tunnel.
Tools/Equipment	None
Prerequisite Procedures	• DLP-J95 Configure Global Settings for Multiprotocol Label Switching Transport Profile Using Cisco IOS Commands, on page 287 • DLP-J99 Configure an MPLS–TP Link Using Cisco IOS Commands, on page 298 • DLP-J103 Specify Static Label Range Using Cisco IOS Commands, on page 291
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls tp lsp source** *ip-address* [**global-id** *number*] **tunnel-tp** *tunnelnumber* **lsp** {*lspnumber* | **working** | **protect**} **destination** *ip-address* [**global-id** *number*] **tunnel-tp** *tunnelnumber* **Example:** Router(config)# mpls tp lsp source 209.165.200.225 tunnel-tp 15 lsp 0 destination 209.165.200.226 tunnel-tp 20	Configures the source and destination parameters of the MPLS–TP tunnel. The source and destination parameters may be specified in a different order at different midpoints of an MPLS–TP tunnel. The default value of source and destination global–id is 0. The LSP number defined for one of the endpoints can uniquely identify an MPLS–TP LSP.
Step 4	**forward–lsp** **Example:** Router(config-mpls-tp-lsp)# forward–lsp	Enters the configuration mode of the forward LSP.
Step 5	**bandwidth** *number* **Example:** Router(config-mpls-tp-lsp-forw)# bandwidth 100	Configures the bandwidth for the forward LSP. The forward LSP refers to the unidirectional LSP going from the source to the destination.
Step 6	**in–label** *locallabelnumber* **out-label** *outlabelnumber* **out-link** *outlinknumber* **Example:** Router(config-mpls-tp-lsp-forw)# in-label 200 out-label 300 out-link 2	Assigns an incoming label (local label), outgoing label, and outgoing link to the forward LSP. The values for the incoming label must be within the static label range that is defined. The outgoing label must be a valid and unreserved MPLS label.
Step 7	**exit** **Example:** Router(config-mpls-tp-lsp-forw)# exit	Exits the configuration mode of the forward LSP.

	Command or Action	Purpose
Step 8	**reverse–lsp** **Example:** Router(config-mpls-tp-lsp)# reverse–lsp	Enters the configuration mode of the reverse LSP.
Step 9	**bandwidth** *number* **Example:** Router(config-mpls-tp-lsp-rev)# bandwidth 100	Configures the bandwidth for the reverse LSP. The reverse LSP refers to the unidirectional LSP going from the destination to the source.
Step 10	**in–label** *locallabelnumber* **out-label** *outlabelnumber* **out-link** *out-tp-link* **Example:** Router(config-mpls-tp-lsp-rev)# in-label 201 out-label 301 out-link 4	Assigns an incoming label (local label), outgoing label, and outgoing link to the reverse LSP. The values for the incoming label must be within the static label range that is defined. The outgoing label must be a valid and unreserved MPLS label.
Step 11	**exit** **Example:** Router(config-mpls-tp-lsp-rev)# exit	Exits the configuration mode of the reverse LSP.
Step 12	**exit** **Example:** Router(config-mpls-tp-lsp)# exit	Exits the LSP configuration mode.
Step 13	Return to your originating procedure (NTP). **Example:** —	

Example: Configuring Tunnel Midpoints

The following example shows how to configure the midpoints of the MPLS–TP tunnel using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# mpls label range 1000 8000 static 16 999
Router(config)# bfd bfd-tp-template

Router(config)# mpls tp
Router(config-mpls-tp)# router-id 2.2.2.2
Router(config-mpls-tp)# exit

Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# mpls tp link 1 ipv4 11.10.10.15
Router(config-if)# exit
Router(config)# interface TenGigabitEthernet4/2
Router(config-if)# mpls tp link 1 ipv4 11.10.10.16
```

```
Router(config-if)# exit


Router(config)# mpls tp lsp source 1.1.1.1 tunnel-tp 10 lsp working destination 3.3.3.3
tunnel-tp 30
Router(config-mpls-tp-lsp)# forward-lsp
Router(config-mpls-tp-lsp-forw)# bandwidth 1000
Router(config-mpls-tp-lsp-forw)# in-label 200 out-label 300 out-link 2
Router(config-mpls-tp-lsp-forw)# exit
Router(config-mpls-tp-lsp)# reverse-lsp
Router(config-mpls-tp-lsp-rev)# in-label 250 out-label 100 out-link 1
Router(config-mpls-tp-lsp-rev)# exit
Router(config-mpls-tp-lsp)# exit
Router(config-mpls-tp)# exit

Router(config)# mpls tp lsp source 1.1.1.1 tunnel-tp 10 lsp protect destination 3.3.3.3
tunnel-tp 30
Router(config-mpls-tp-lsp)# forward-lsp
Router(config-mpls-tp-lsp-forw)# bandwidth 1000
Router(config-mpls-tp-lsp-forw)# in-label 201 out-label 301 out-link 4
Router(config-mpls-tp-lsp-forw)# exit
Router(config-mpls-tp-lsp)# reverse-lsp
Router(config-mpls-tp-lsp-rev)# in-label 251 out-label 101 out-link 3
Router(config-mpls-tp-lsp-rev)# exit
Router(config-mpls-tp-lsp)# exit
Router(config-mpls-tp)# exit
```

DLP–J106 Configure Tunnel Endpoints Using Cisco IOS Commands

Purpose	This procedure configures the endpoints for MPLS–TP tunnels. The MPLS–TP tunnel is provisioned as a virtual interface.
Tools/Equipment	None
Prerequisite Procedures	• DLP-J95 Configure Global Settings for Multiprotocol Label Switching Transport Profile Using Cisco IOS Commands, on page 287 • DLP-J97 Create and Configure BFD Templates Using Cisco IOS Commands, on page 293 • DLP-J99 Configure an MPLS–TP Link Using Cisco IOS Commands, on page 298 • DLP-J103 Specify Static Label Range Using Cisco IOS Commands, on page 291
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface tunnel–tp** *tunnelnumber* **Example:** Router(config)# interface tp–tunnel 30	Enters the interface configuration mode and configures the parameters of the tunnel.
Step 4	**description** *tunnel-description* **Example:** Router(config–if)# description firsttunnel	Provides a description for the tunnel. The description is used only when displaying information about the MPLS–TP tunnel.
Step 5	**bandwidth tx** *number* [**rx** number] **Example:** Router(config–if)# bandwidth tx 1000	Configures the bandwidth for the MPLS–TP tunnel. The transmit and receive bandwidth provisioned for the working LSP are the same as that of the protect LSP.
Step 6	**tp source** *ip-address* [**global-id** *number*] **Example:** Router(config–if)# tp source 209.165.200.225	Configures the MPLS–TP tunnel source IP address. The source IP address is the ID of the endpoint router that is configured. The **global-id** is the default global ID used for all midpoints and endpoints. The default value of the **global–id** is 0. The valid range is from 0 to 2147483647.
Step 7	**tp destination** *ip-address* [**tunnel-tp** *number*] [**global-id** *number*] **Example:** Router(config–if)# tp destination 209.165.200.226	Configures the MPLS–TP tunnel destination IP address. The **tunnel-tp** is the tunnel–TP number of the MPLS–TP tunnel destination. If the tunnel–TP number is not specified, the number assigned to the local tunnel is used. The **global-id** is the default global ID used for the endpoint. The default value of the global–id is 0. The valid range is from 0 to 2147483647.
Step 8	**bfd** *bfdtemplatename* **Example:** Router(config–if)# bfd bfd1	Configures a BFD template for the MPLS–TP tunnel. The BFD configuration template used for the working LSP is the same as that of the protect LSP.

	Command or Action	Purpose
Step 9	**working-lsp** **Example:** Router(config–if)# working-lsp	Enters the configuration mode of the working LSP.
Step 10	**out-label** *outlabelnumber* **out-link** *out-tp-link* **Example:** Router(config–if–working)# out–label 250 out–link 1	Assigns an outgoing label and outgoing link to the working LSP. The outgoing label must be a valid and unreserved MPLS label. The working LSP is the primary LSP that is used to route traffic.
Step 11	**in–label** *locallabelnumber* **Example:** Router(config–if–working)# in–label 10	Assigns an incoming label (local label) to the working LSP. The values for the incoming label must be within the static label range (16 to 8000).
Step 12	**lsp–num** *number* **Example:** Router(config–if–working)# lsp–num 0	Configures the LSP number for the working LSP. The default LSP number for the working LSP is 0. The range is 0 and above. The local and remote LSP numbers must match.
Step 13	**lockout** **Example:** Router(config–if–working)# lockout	(Optional) Locks out the working LSP.
Step 14	**protect-lsp** **Example:** Router(config–if)# protect-lsp	Enters the configuration mode of the protect LSP.
Step 15	**out-label** *outlabelnumber* **out-link** *out-tp-link* **Example:** Router(config–if–protect)# out–label 251 out–link 2	Assigns an outgoing label and outgoing link to the protect LSP. The outgoing label must be a valid and unreserved MPLS label. A protect LSP is a backup for a working LSP. If the working LSP fails, the traffic is switched to the protect LSP until the working LSP is restored, when forwarding reverts to the working LSP.
Step 16	**in–label** *locallabelnumber* **Example:** Router(config–if–protect)# in–label 20	Assigns an incoming label (local label) to the protect LSP. The values for the incoming label must be within the static label range that is defined.
Step 17	**lsp–num** *number* **Example:** Router(config–if–protect)# lsp–num 1	Configures the LSP number for the protect LSP. The default LSP number for the protect LSP is 1. The range is 1 and above. The local and remote LSP numbers must match.

	Command or Action	Purpose
Step 18	**lockout** **Example:** Router(config–if–protect)# lockout	Locks out the protect LSP.
Step 19	**shutdown** **Example:** Router(config–if)# shutdown	Performs an administrative shut down of the MPLS–TP tunnel.
Step 20	Return to your originating procedure (NTP).	

Example: Configuring Tunnel Endpoints

The following example shows how to configure one of the endpoints of the MPLS–TP tunnel using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# mpls label range 1000 8000 static 16 999
Router(config)# bfd bfd-tp-template

Router(config)# mpls tp
Router(config-mpls-tp)# router-id 1.1.1.1
Router(config-mpls-tp)# exit

Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# mpls tp link 1 ipv4 11.10.10.15
Router(config-if)# exit
Router(config)# interface TenGigabitEthernet4/2
Router(config-if)# mpls tp link 1 ipv4 11.10.10.16
Router(config-if)# exit

Router(config)# interface tunnel-tp 10
Router(config-if)# description MPLS-TP tunnel connecting ABC customer A PE routers
Router(config–if)# bandwidth  tx 1000

Router(config-if)# no ip address
Router(config-if)# no keepalive
Router(config-if)# tp destination 3.3.3.3 tunnel-tp 30
Router(config-if)# bfd  bfd-tp-template

Router(config-if)# working-lsp
Router(config-if-working)# out-label 200 out-link 1
Router(config-if-working)# in-label 100
Router(config-if-working)# lsp-number 0
Router(config-if-working)# exit

Router(config-if)# protect-lsp
Router(config-if-protect)# out-label 201 out-link 2
Router(config-if-protect)# in-label 101
Router(config-if-protect)# lsp-number 1
Router(config-if-protect)# exit
Router(config-if)# exit
```

The following example shows how to configure another endpoint of the MPLS–TP tunnel using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# mpls label range 1000 8000 static 16 999
Router(config)# bfd bfd-tp-template

Router(config)# mpls tp
Router(config-mpls-tp)# router-id 2.2.2.2
Router(config-mpls-tp)# exit

Router(config)# interface TenGigabitEthernet4/3
Router(config-if)# mpls tp link 1 ipv4 11.10.11.17
Router(config-if)# exit
Router(config)# interface TenGigabitEthernet4/4
Router(config-if)# mpls tp link 1 ipv4 11.10.11.18
Router(config-if)# exit

Router(config)# interface tunnel-tp 30
Router(config-if)# description  MPLS-TP tunnel connecting ABC customer A PE routers
Router(config-if)# bandwidth  tx 1500

Router(config-if)# no ip address
Router(config-if)# no keepalive
Router(config-if)# tp destination 1.1.1.1 tunnel-tp 10
Router(config-if)# bfd  bfd-tp-template

Router(config-if)# working-lsp
Router(config-if-working)# out-label 250 out-link  1 in-label 300
Router(config-if-working)# lsp-number 2
Router(config-if-working)# exit

Router(config-if)# protect-lsp
Router(config-if-protect)# out-label 251 out-link 2 in-label 301
Router(config-if-working)# lsp-number 3
Router(config-if-protect)# exit
Router(config-if)# exit
```

DLP-J107 Create an MPLS–TP Tunnel Using CTC

Purpose	This procedure creates an MPLS–TP tunnel using CTC.
Tools/Equipment	None

Prerequisite Procedures	• DLP-J96 Configure Global Settings for Multiprotocol Label Switching Transport Profile Using CTC, on page 289 • DLP-J98 Create and Configure BFD Templates Using CTC, on page 295 • DLP-J100 Configure an MPLS–TP Link Number Using CTC, on page 301 • DLP-J104 Specify Static Label Range Using CTC, on page 292 • NTP-J67 Create a Provisionable Patchcord Using CTC, on page 305
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You cannot create an MPLS–TE tunnel and an MPLS–TP tunnel on the same interface.

Note The layer 2 services on CPT can be created on top of layer 2 PPCs or OCHTrails.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to create an MPLS–TP tunnel.

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

Step 3 Click the **Layer2+** tab.

Step 4 In the left pane, click **Circuits**.

Step 5 Click the **MPLS TP Tunnels** tab.

Step 6 Click **Create**. The Circuit Creation wizard appears.

Step 7 In the Circuit Attributes screen of the wizard:

a) Enter the name of the tunnel that you want to create, in the Name field.

b) Enter the description of the tunnel in the Description field.
The type of the tunnel is MPLS_TP and cannot be changed. The tunnel is always created as a bidirectional tunnel.

c) Check the **Protection** check box to create a protected tunnel.

d) From the Admin State drop–down list, choose **UP** or **DOWN** . The default value is UP.

e) Enter the bandwidth of the MPLS–TP tunnel in Kbps (default), Mbps, or Gbps and click **Next**.

Step 8 In the Source screen of the wizard, specify the parameters for one endpoint:

a) Check the RING ID check box.
Note This check box is enabled only if the service state of the ring is enabled.

b) From the RING ID drop–down list, choose a ring .
Note This drop down list is enabled only if the RING ID check box is checked.

c) From the Slot/CPT50 drop-down list, choose a slot or CPT 50.
Note If you select the RING ID check box, a list of available CPT 50s is displayed. Otherwise, a list of available slots is displayed.

d) From the Attach BFD drop-down list, choose a BFD template to attach to this endpoint.
Note It is recommended that the same BFD template be attached for the endpoints.

e) Enter the unique tunnel number for this endpoint in the Tunnel Number field.

f) Enter the LSP number for the working LSP in the Working LSP Number field. The default value is 0.

g) Enter the LSP number for the protect LSP in the Protect LSP Number field. The default value is 1. Click **Next.**

Step 9 In the Destination screen of the wizard, specify the parameters for another endpoint. Repeat the previous step to do this.

Step 10 In the TP Tunnel Circuit Routing Preferences screen of the wizard, specify the routing preferences for the tunnel:

a) For constraint–based routing, check the **Using Required Nodes/Spans** check box. The **Route Automatically** check box is set by default and cannot be changed.

b) Specify the diversity constraints by choosing **Nodal Diversity Required**, **Nodal Diversity Desired**, or **Link Diversity Only**.

- Nodal Diversity Required—Ensures that the primary and alternate paths within path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.

  Node diversity is not applicable if the source and destination are directly connected with fiber diverse path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

c) Click **Next**.

Step 11 In the TP Tunnel Circuit Routing Constraints screen of the wizard, the route of the MPLS–TP tunnel is displayed.

a) In the route, choose the nodes appropriately to include or exclude in the MPLS–TP tunnel.

b) Click **Next**.

Step 12 In the TP Tunnel Circuit Label Preview screen of the wizard:

a) Change the local label and outgoing label for working LSP and protect LSP as appropriate.

b) Click **Apply**.

c) Click **Finish** to create an MPLS–TP tunnel.

It is not recommended to delete the MPLS–TP tunnel in Partial state. For example, the tunnel is in Partial state due to missing intermediate LSP information. If you delete this Partial tunnel, you cannot delete the LSP information on the intermediate node and reuse the tunnel bandwidth.

When you change the PPC paths of a tunnel in Discovered state, you cannot delete the LSP information on the intermediate node. For example, consider a tunnel that spans three nodes A, B, and C. The PPC links from A to B and B to C are deleted and a direct PPC link is created from A to C. In this case, the LSP information on the intermediate node B cannot be deleted.

Step 13 Return to your originating procedure (NTP).
In order to achieve better TP switchover in rings, It is recommended to set WTR timer not less than 30sec in a Single Home ring and 60sec in a Dual Home ring.

DLP-J208 Edit MPLS–TP Tunnel Attributes Using CTC

Purpose	This procedure edits MPLS–TP tunnel attributes using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J107 Create an MPLS–TP Tunnel Using CTC, on page 316
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to edit an MPLS–TP tunnel.

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

Step 3 Click the **Layer2+** tab.

Step 4 From the left pane, click **Circuits**.

Step 5 Click the **MPLS TP Tunnels** tab.

Step 6 Choose a tunnel to edit and click **Edit**. The Edit Circuit screen appears.

Step 7 In the General tab, modify the name, description of the MPLS–TP tunnel as required.

Note The following points are applicable, If you query the tunnel after editing the name.

- The query window will display two tunnels, one from the endpoints and the other from the midpoints.
- Both the tunnels should be selected for service discovery.

Step 8 In the LSPs tab, edit, add, or remove the LSPs:

a) To edit an LSP:

1. Choose an LSP to edit.
2. From the Node drop-down list, choose a node.
3. Click **Edit LSP**.
4. Modify the values in the Local Label and Out Label fields as appropriate.
5. Click **Apply**.

b) To add an LSP:

1. Click **Add LSP**. The Add LSP Members wizard appears.
2. In the Circuit Attributes screen of the wizard, enter the LSP number in the LSP Number field and click **Next**.
3. In the Routing and Member Preferences screen of the wizard, check the **Using Required Nodes/Spans** check box for constraint–based routing. The **Route Automatically** check box is set by default and cannot be changed.
4. Specify the diversity constraints by choosing **Nodal Diversity Required**, **Nodal Diversity Desired**, or **Link Diversity Only** and click **Next**.
5. In the Constraints for Automatic Routing screen of the wizard, choose the nodes appropriately to include or exclude and click **Next**.
6. In the Circuit Label Preview screen of the wizard, enter the local label and outgoing label for the working LSP and protect LSP as appropriate.
7. Click **Apply**.
8. Click **Finish** to add an LSP.

c) To delete an LSP:

1. Choose an LSP to delete.
2. Click **Delete LSP**. The Delete LSP dialog box appears.
3. Click **OK** in the Delete LSP dialog box.

Step 9 In the BFD tab, choose an appropriate BFD template from the BFD Template field and click **Apply**.

Step 10 In the Lockout tab, choose a node from the Endpoint field.

Step 11 From the Switch State drop–down list, choose **LOCKOUT** or **CLEAR**
The Lockout option specifies that the locked out LSP do not carry traffic. Only one LSP can be locked out at a time. The Lockout option can be applied only when there are two LSPs. The Clear option clears the lockout condition.

Step 12 In the State tab, choose UP or DOWN from the Target Circuit Admin State drop-down list and click **Apply**.

Step 13 Return to your originating procedure (NTP).

DLP-J368 Query an MPLS-TP Circuit Using CTC

Purpose	This procedure allows you to discover the MPLS-TP services using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J107 Create an MPLS–TP Tunnel Using CTC, on page 316
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note When the discovered nodes are disconnected, the circuits move to Partial state. When the disconnected nodes become online in CTC, re-query the circuits to move the circuits to Discovered state.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to query for an MPLS-TP circuit.

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

Step 3 Click the **Layer2+** tab.

Step 4 From the left pane, click **Carrier Ethernet**.

Step 5 Click **Query**. The L2 Services Query dialog box appears.

Step 6 From the Existing/New Query drop-down list, choose an existing query or a new query.

Step 7 In the Equipment Termination area, choose **Port** or **Query Group**.

Step 8 If you choose Port, specify the following:

a) Click **Port**. The Port/Channel Group Selection dialog box appears.
b) Choose the node, card, and port/channel group and click **OK**.
c) Close the Port/Channel Group Selection dialog box.

Step 9 If you choose Query Group, specify the following:

a) Click **Query Group**. The User Query Group Chooser dialog box appears.
b) From the Group drop-down list, choose a query group.
c) Add the nodes that can be grouped for the query from the Available Nodes area to the Grouped Nodes area.
d) Click **Save** to save the query group and close the User Query Group Chooser dialog box.

Step 10 In the L2 Services Query dialog box, click **Save**. The Store a Set of Query Criteria dialog box appears.

Step 11 Enter the query name in the Name field and click **Save** to save the query.

Step 12 In the L2 Services Query dialog box, click **Run Query**.

The results of the query appear in the Service Query Results area.

Step 13 Click **Discover All** to discover all the MPLS-TP services, click **Discover Selected** to discover the selected MPLS-TP services or click **Delete** to delete the midpoint nodes of the MPLS-TP services.

Note If a CPT50 in a ring is not discovered by CTC then the services on that CPT50 in a ring, are not manageable by CTC, i.e. user cannot query, view, edit, create or delete the service on that CPT50 in a ring. In the above state, the services passing through such a CPT50 will be displayed as PARTIAL at CTC though the actual traffic might not be affected depending on the type of failure.

A CPT50 in a ring can be unreachable in CTC due to one or more of the following reasons:

1. Link failure. CPT50 is failed or not ready for configuration.
2. Topo-Mis-Config alarm present in the ring.
3. Disabled ring state.
4. Ring ports are shut.

Some of the above conditions can be verified from the Show Actual Topology.

Close the L2 Services Query dialog box. The discovered MPLS-TP services appear in the Carrier Ethernet Circuits area.

Step 14 Return to your originating procedure (NTP).

NTP-J107 Perform ping and traceroute Operations on Services Using CTC

Purpose	This procedure performs ping and traceroute operations on services using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to perform ping and traceroute operations.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Maintenance** tab.

Step 4 In the left pane, click **OAM**.

Step 5 From the Service drop-down list, choose **TP Tunnel**, **TE Tunnel**, **Pseudowire**.

Step 6 From the Command drop-down list, choose **Ping** or **Traceroute**.

Step 7 If you choose TP Tunnel as the service, complete the following:

a) Enter the tunnel ID in the Tunnel No field.

b) From the LSP drop-down list, choose **Active**, **Working**, or **Protect**.

Step 8 If you choose TE Tunnel as the service, complete the following:

a) Enter the tunnel ID in the Tunnel No field.

Step 9 If you choose Pseudowire as the service, complete the following:

a) Enter the IP address in the IP field.

b) Enter the virtual circuit ID in the VC ID field.

Step 10 Click **Execute** to run the OAM operation for the specified service.
Stop. You have completed this procedure.

MPLS–TP Show Commands

This section describes several show commands that can be used with MPLS–TP tunnels.

Display MPLS–TP Tunnel Summary

This command displays a count of the configured tunnels, midpoint LSPs, and the global configuration parameters.

```
Router# show mpls tp summary
```

```
Endpoints: 4      Midpoints: 3
ICC:
Router Id: 3.3.3.3
Global Id: 0
Path protection mode:  1:1 revertive
Fault OAM timer: 0
```

Display Link Number Information

This command provides information about the MPLS–TP link numbers. It displays the mappings between link numbers and physical interfaces and next hop addresses when appropriate.

```
Router# show mpls tp link-numbers
```

```
Link Number     Interface               Next Hop
 1              Ethernet0/0             1.2.3.4
 2              Ethernet1/0             2.3.4.5
 3              Ethernet0/3             fcce.c1cc.cc01
```

Display MPLS–TP Tunnel Information

This command displays the tunnel information of MPLS–TP tunnels.

```
Router# show mpls tp tunnel-tp
```

```
Tunnel    Peer node-id::tun  Working/   Local  Outgoing  Outgoing  Oper
Number                       Protect    Label  Label     Interface State

   5       4.4.4.4::5           w        100     110        Et0/0    up
   6       6.6.6.6::7           w        200     210        Et0/0    up
```

Display MPLS–TP Tunnel Information with LSPs

This command displays the tunnel information of MPLS–TP tunnels with LSPs.

```
Router# show mpls tp tunnel-tp lsps
```

```
Tunnel  Peer node-id::tun  Working/  Local Outgoing Outgoing  Oper
Number                     Protect   Label Label    Interface State

   5       4.4.4.4::5          w       100     110     Et0/0    up
           LSP: working                100     110     Et0/0    up active

           LSP: protect                120     130     Et1/0    up standby



   6       6.6.6.6::7          w       200     210     Et0/0    up
           LSP: working                200     210     Et0/0    up active

           LSP: protect                220     230     Et1/0    up standby
```

Display Detailed MPLS–TP Tunnel Information

This command displays detailed tunnel information of MPLS–TP tunnels.

```
Router# show mpls tp tunnel-tp detail
```

```
MPLS-TP Tunnels:
  MPLS-TP tunnel 5:
      source global id  0 : node id 3.3.3.3 : tunnel 5
      dest global id  0 : node id 4.4.4.4 : tunnel 5
      description:  this is test tunnel 5
      UMC: tunnel5    ICC: ATT
      Admin: up           Oper: up
      bandwidth transmit     1400, receive     1500
```

```
     BFD template:  bfd-template-5
     working-lsp: active      lsp num 0
     protect-lsp: standby      lsp num 1
  MPLS-TP tunnel 6:
     source global id  0 : node id 3.3.3.3 : tunnel 6
     dest global id  0 : node id 6.6.6.6 : tunnel 7
     description:  this is test tunnel  6
     Admin: up           Oper: up
     bandwidth transmit     1600, receive     1700
     BFD template:
     working-lsp: active      lsp num 0
     protect-lsp: standby      lsp num 1
  MPLS-TP tunnel 65530:
     source global id  0 : node id 123.123.123.123 : tunnel 65530
     dest global id  0 : node id 124.124.124.124 : tunnel 65530
     description:  this is test tunnel  65530
     UMC: big_id
     Admin: up           Oper: up
     bandwidth transmit     1600, receive     1700
     BFD template:
     working-lsp: active      lsp num 0
     protect-lsp: standby      lsp num 1
```

Display Detailed MPLS–TP Tunnel Information with LSPs

This command displays detailed tunnel information of MPLS–TP tunnels with LSPs.

```
Router# show mpls tp tunnel-tp lsps detail
```

```
MPLS-TP Tunnels:
  MPLS-TP tunnel 5:
     source global id  0 : node id 3.3.3.3 : tunnel 5
     dest global id  0 : node id 4.4.4.4 : tunnel 5
     description:  this is test tunnel 5
     UMC: tunnel5    ICC: ATT
     Admin: up           Oper: up
     bandwidth transmit     1400, receive     1500
     BFD template:  bfd-template-5
     working-lsp: active      lsp num 0
        0::3.3.3.3::5::0::4.4.4.4::5::0
        local label 100    local label table 0    outgoing label   110
        outgoing tp-link 1   interface Et0/0
        UMC: working-5
     protect-lsp: standby      lsp num 1
        0::3.3.3.3::5::0::4.4.4.4::5::1
        local label 120    local label table 0    outgoing label   130
        outgoing tp-link 2   interface Et1/0
  MPLS-TP tunnel 6:
     source global id  0 : node id 3.3.3.3 : tunnel 6
     dest global id  0 : node id 6.6.6.6 : tunnel 7
     description:  this is test tunnel  6
     Admin: up           Oper: up
     bandwidth transmit     1600, receive     1700
     BFD template:
     working-lsp: active      lsp num 0
        0::3.3.3.3::6::0::6.6.6.6::7::0
        local label 200    local label table 0    outgoing label   210
```

```
        outgoing tp-link 1   interface Et0/0
    protect-lsp: standby      lsp num 1
       0::3.3.3.3::6::0::6.6.6.6::7::1
       local label 220    local label table 0    outgoing label   230
       outgoing tp-link 2   interface Et1/0
       UMC: protect-6
 MPLS-TP tunnel 65530:
    source global id  0 : node id 123.123.123.123 : tunnel 65530
    dest global id  0 : node id 124.124.124.124 : tunnel 65530
    description:  this is test tunnel  65530
    UMC: big_id
    Admin: up           Oper: up
    bandwidth transmit     1600, receive     1700
    BFD template:
    working-lsp: active      lsp num 0
       0::123.123.123.123::65530::0::124.124.124.124::65530::0
       local label 300    local label table 0    outgoing label   310
       outgoing tp-link 1   interface Et0/0
    protect-lsp: standby      lsp num 1
       0::123.123.123.123::65530::0::124.124.124.124::65530::1
       local label 320    local label table 0    outgoing label   330
       outgoing tp-link 2   interface Et1/0
```

Display MPLS–TP Tunnel Information for a Single Tunnel

This command displays the tunnel information for a single MPLS–TP tunnel.

```
Router# show mpls tp tunnel-tp tunnelnumber
```

```
Tunnel    Peer node-id::tun  Working/   Local  Outgoing  Outgoing  Oper
Number                        Protect    Label  Label     Interface State

   5       4.4.4.4::5           w        100     110        Et0/0    up
```

Display MPLS–TP Tunnel Information for a Single Tunnel with LSPs

This command displays the tunnel information for a single MPLS–TP tunnel with LSPs.

```
Router# show mpls tp tunnel-tp tunnelnumber lsps
```

```
Tunnel  Peer node-id::tun  Working/  Local Outgoing Outgoing  Oper
Number                     Protect   Label Label    Interface State

   5       4.4.4.4::5          w       100     110     Et0/0    up
           LSP: working                100     110     Et0/0    up active

           LSP: protect               120     130     Et1/0    up standby



   6       6.6.6.6::7          w       200     210     Et0/0    up
           LSP: working                200     210     Et0/0    up active

           LSP: protect               220     230     Et1/0    up standby
```

Display Detailed MPLS–TP Tunnel Information for a Single Tunnel

This command displays the detailed tunnel information for a single MPLS–TP tunnel.

```
Router# show mpls tp tunnel-tp tunnelnumber detail
```

```
MPLS-TP Tunnels:
  MPLS-TP tunnel 5:
      source global id  0 : node id 3.3.3.3 : tunnel 5
      dest global id  0 : node id 4.4.4.4 : tunnel 5
      description:  this is test tunnel 5
      UMC: tunnel5    ICC: ATT
      Admin: up           Oper: up
      bandwidth transmit     1400, receive     1500
      BFD template:  bfd-template-5
      working-lsp: active      lsp num 0
      protect-lsp: standby      lsp num 1
```

Display Detailed MPLS–TP Tunnel Information for a Single Tunnel with LSPs

This command displays the detailed tunnel information for a single MPLS–TP tunnel with LSPs.

```
Router# show mpls tp tunnel-tp tunnelnumber lsps detail
```

```
MPLS-TP Tunnels:
  MPLS-TP tunnel 5:
      source global id  0 : node id 3.3.3.3 : tunnel 5
      dest global id  0 : node id 4.4.4.4 : tunnel 5
      description:  this is test tunnel 5
      UMC: tunnel5    ICC: ATT
      Admin: up           Oper: up
      bandwidth transmit     1400, receive     1500
      BFD template:  bfd-template-5
      working-lsp: active      lsp num 0
         0::3.3.3.3::5::0::4.4.4.4::5::0
         local label 100    local label table 0    outgoing label   110
         outgoing tp-link 1   interface Et0/0
         UMC: working-5
      protect-lsp: standby      lsp num 1
         0::3.3.3.3::5::0::4.4.4.4::5::1
         local label 120    local label table 0    outgoing label   130
         outgoing tp-link 2   interface Et1/0
```

Display LSP Information

This command displays information for all the MPLS–TP LSPs (midpoint and endpoint LSPs) configured on this router.

```
Router# show mpls tp lsps
```

```
MPLS-TP Endpoint LSPs:
LSP Identifier                      Local  Outgoing  Outgoing  Oper   Role
                                    Label  Label     Interface State
0::3.3.3.3::5::0::4.4.4.4::5::0     100    110       Et0/0     up   active
0::3.3.3.3::5::0::4.4.4.4::5::1     120    130       Et1/0     up   standby
```

```
0::3.3.3.3::6::0::6.6.6.6::7::0    200    210        Et0/0     up   active
0::3.3.3.3::6::0::6.6.6.6::7::1    220    230        Et1/0     up   standby

MPLS-TP Midpoint LSPs:
LSP Identifier                     LSP  Local Outgoing  Outgoing
                                        Label Label     Interface
0::1.1.1.1::1::0::6.6.6.6::1::0    forw  150   151        Et0/0
                                   rev   152   153        Et1/0
0::1.1.1.1::9::0::9.9.9.9::9::0    forw  160   161        Et0/0
                                   rev   162   163        Et1/0
```

Display Midpoint LSP Information

This command displays information for the midpoint LSP.

```
Router# show mpls tp lsps midpoints
```

```
MPLS-TP Midpoint LSPs:
LSP Identifier                     LSP  Local Outgoing  Outgoing
                                        Label Label     Interface
0::1.1.1.1::1::0::6.6.6.6::1::0    forw  150   151        Et0/0
                                   rev   152   153        Et1/0
0::1.1.1.1::9::0::9.9.9.9::9::0    forw  160   161        Et0/0
                                   rev   162   163        Et1/0
```

Display Endpoint LSP Information

This command displays information for the endpoint LSP.

```
Router# show mpls tp lsps endpoints
```

```
MPLS-TP Endpoint LSPs:
LSP Identifier                     Local  Outgoing  Outgoing  Oper   Role
                                   Label  Label     Interface State
0::3.3.3.3::5::0::4.4.4.4::5::0    100    110        Et0/0     up   active
0::3.3.3.3::5::0::4.4.4.4::5::1    120    130        Et1/0     up   standby
0::3.3.3.3::6::0::6.6.6.6::7::0    200    210        Et0/0     up   active
0::3.3.3.3::6::0::6.6.6.6::7::1    220    230        Et1/0     up   standby
```

Display Detailed LSP Information

This command displays detailed LSP information.

```
Router# show mpls tp lsps detail
```

```
MPLS-TP Endpoint LSPs:
   0::3.3.3.3::5::0::4.4.4.4::5::0
   local label 100    local label table 0    outgoing label   110
   outgoing tp-link 1   interface Et0/0
   UMC: working-5
   0::3.3.3.3::5::0::4.4.4.4::5::1
   local label 120    local label table 0    outgoing label   130
   outgoing tp-link 2   interface Et1/0
   0::3.3.3.3::6::0::6.6.6.6::7::0
   local label 200    local label table 0    outgoing label   210
```

```
   outgoing tp-link 1   interface Et0/0
   0::3.3.3.3::6::0::6.6.6.6::7::1
   local label 220    local label table 0    outgoing label   230
   outgoing tp-link 2   interface Et1/0
   UMC: protect-6
   0::123.123.123.123::65530::0::124.124.124.124::65530::0
   local label 300    local label table 0    outgoing label   310
   outgoing tp-link 1   interface Et0/0
   0::123.123.123.123::65530::0::124.124.124.124::65530::1
   local label 320    local label table 0    outgoing label   330
   outgoing tp-link 2   interface Et1/0

MPLS-TP Midpoint LSPs:
   0::1.1.1.1::1::0::6.6.6.6::1::0
      source global id  0 : node id 1.1.1.1 : tunnel 1
      dest global id  0 : node id 6.6.6.6 : tunnel 1
      lsp    working
      UMC: midpoint_1_2    ICC: ATT
      forward-lsp:  local label 150   outgoing label   151
                    outgoing tp-link 1   interface Et0/0
      bandwidth  1122
      reverse-lsp:  local label 152   outgoing label   153
                    outgoing tp-link 2   inteface Et1/0
         bandwidth  2211
   0::1.1.1.1::9::0::9.9.9.9::9::0
      source global id  0 : node id 1.1.1.1 : tunnel 9
      dest global id  0 : node id 9.9.9.9 : tunnel 9
      lsp    working
      forward-lsp:  local label 160   outgoing label   161
                    outgoing tp-link 1   interface Et0/0
      bandwidth  0
      reverse-lsp:  local label 162   outgoing label   163
                    outgoing tp-link 2   inteface Et1/0
         bandwidth  0
   0::2.2.2.2::2::0::9.9.9.9::2::0
      source global id  0 : node id 2.2.2.2 : tunnel 2
      dest global id  0 : node id 9.9.9.9 : tunnel 2
      lsp    working
      forward-lsp:  local label 170   outgoing label   171
                    outgoing tp-link 1   interface Et0/0
      bandwidth  0
      reverse-lsp:  local label 172   outgoing label   173
                    outgoing tp-link 2   inteface Et1/0
         bandwidth  0
```

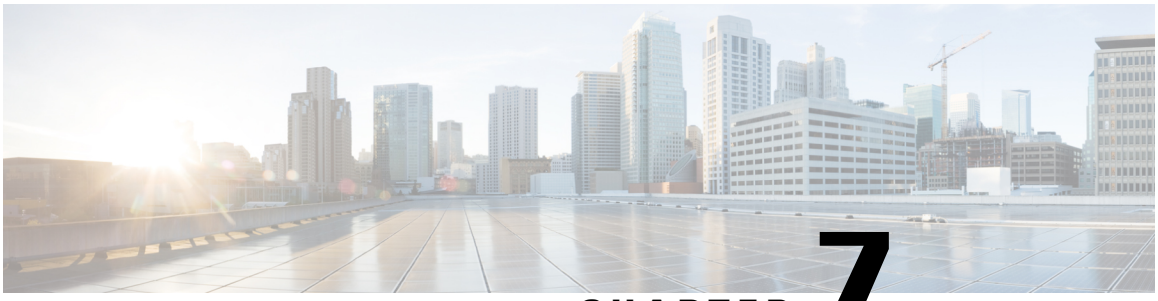
Display Matching LSP Information

This command displays information for the MPLS–TP LSPs that match the specified filter value. The filter value can be node-id, global-id, tunnel number, or lsp number. The specified filter value is applied to each source and destination LSP identifier.

```
Router# show mpls tp lsps 6.6.6.6
```

```
MPLS-TP Endpoint LSPs:
LSP Identifier                    Local  Outgoing  Outgoing  Oper   Role
                                  Label  Label     Interface State
0::3.3.3.3::6::0::6.6.6.6::7::0    200    210       Et0/0     up   active
```

```
0::3.3.3.3::6::0::6.6.6.6::7::1    220    230        Et1/0     up   standby

MPLS-TP Midpoint LSPs:
LSP Identifier                     LSP  Local Outgoing  Outgoing
                                        Label Label     Interface
0::1.1.1.1::1::0::6.6.6.6::1::0    forw  150   151        Et0/0
                                   rev   152   153        Et1/0
```



CHAPTER 7

Configuring Pseudowire

This chapter describes static and dynamic pseudowires. This chapter also describes the configuration procedures of pseudowires.

Understanding Any Transport over MPLS

Any Transport over MPLS (AToM) feature provides the following capabilities:

- Transport data link layer (Layer 2) packets over an MPLS backbone.
- Enable service providers to connect customer sites with existing Layer 2 networks by using a single, integrated, packet–based network infrastructure — an MPLS network. Instead of using separate networks with network management environments, service providers can deliver Layer 2 connections over an MPLS backbone.
- Provide a common framework to encapsulate and transport supported Layer 2 traffic types over an MPLS network core.

Note CPT supports only Ethernet over MPLS as the transport type under AToM in this release.

Prerequisites

Before configuring AToM, ensure that the network is configured as follows:

- Configure IP routing in the core so that the provider edge (PE) routers can reach each other via IP.
- Configure MPLS in the core so that a Label Switched Path (LSP) exists between the PE routers.
- Enable Cisco Express Forwarding or distributed Cisco Express Forwarding before configuring any Layer 2 circuits.
- Configure a loopback interface for originating and terminating Layer 2 traffic. Ensure that the PE routers can access the loopback interface of the other router.

Restrictions

The following restrictions pertain to Ethernet over MPLS feature under AToM:

- Configure the Label Distribution Protocol (LDP) router ID on all the PE routers to be a loopback address with a /32 mask. Otherwise, some configurations might not function properly.
- Ethernet over MPLS supports VLAN packets that conform to the IEEE 802.1Q standard. The 802.1Q specification establishes a standard method for inserting VLAN membership information into Ethernet frames. The Inter–Switch Link (ISL) protocol is not supported between the PE and CE routers.
- The AToM control word is supported. However, if the peer PE does not support a control word, the control word is disabled. This negotiation is done by LDP label binding.
- Ethernet packets with hardware–level cyclic redundancy check (CRC) errors, framing errors, and runt packets are discarded on input.

Benefits

The following list explains some of the benefits of enabling Layer 2 packets to be sent in the MPLS network:

- AToM adheres to the standards developed for transporting Layer 2 packets over MPLS. This benefits the service provider that wants to incorporate industry–standard methodologies in the network. Other Layer 2 solutions are proprietary, which can limit the ability of the service provider to expand the network and can force the service provider to use the equipment of only one vendor.
- Upgrading to AToM is transparent to the customer. Because the service provider network is separate from the customer network, the service provider can upgrade to AToM without disruption of service to the customer. The customers assume that they are using a traditional Layer 2 backbone.

How AToM Transports Layer 2 Packets

AToM encapsulates Layer 2 frames at the ingress PE and sends them to a corresponding PE at the other end of a pseudowire, which is a connection between the two PE routers. The egress PE removes the encapsulation and sends out the Layer 2 frame.

The successful transmission of the Layer 2 frames between PE routers is due to the configuration of the PE routers. Set up the connection, called a pseudowire, between the routers. Pseudowire is the emulation of services over the MPLS network.

Specify the following information on each PE router:

- The type of Layer 2 data that is transported across the pseudowire, such as Ethernet.
- The IP address of the loopback interface of the peer PE router, which enables the PE routers to communicate.
- A unique combination of peer PE IP address and Virtual Circuit ID (VC ID) that identifies the pseudowire.

Understanding Ethernet over MPLS

You can configure Ethernet over MPLS in the following modes:

- Ethernet over MPLS in VLAN mode
- Ethernet over MPLS in Port mode
- Ethernet over MPLS in VLAN ID Rewrite mode

Ethernet over MPLS in VLAN Mode

A VLAN is a switched network that is logically segmented by functions, project teams, or applications regardless of the physical location of users. Ethernet over MPLS allows you to connect two VLAN networks that are in different locations. You can configure the PE routers at each end of the MPLS backbone and add a point-to-point VC. Only the two PE routers at the ingress and egress points of the MPLS backbone are aware of the VCs dedicated to transporting Layer 2 VLAN traffic. All other routers do not have table entries for those VCs. Ethernet over MPLS in VLAN mode transports Ethernet traffic from a source 802.1Q VLAN to a destination 802.1Q VLAN over a core MPLS network.

Note You must configure Ethernet over MPLS (VLAN mode) on the Ethernet Flow Points (EFPs).

Ethernet over MPLS in Port Mode

Port mode allows a frame coming into an interface to be packed into an MPLS packet and transported over the MPLS backbone to an egress interface. The entire Ethernet frame is transported as a single packet. You can configure port mode xconnect by using EFP mode with encapsulation default. You can then specify the destination address and the VC ID. Each interface is associated with one unique pseudowire VC label.

When configuring Ethernet over MPLS in port mode, use the following guidelines:

- The pseudowire VC type is set to Ethernet.
- The Port mode and VLAN mode are mutually exclusive. If you enable a main interface for port-to-port transport, you cannot enter commands on the EFP.

Ethernet over MPLS in VLAN ID Rewrite Mode

The VLAN ID rewrite mode enables you to use VLAN interfaces with different VLAN IDs at both ends of the tunnel.

NTP-J29 Configure Ethernet over MPLS

Purpose	This procedure configures Ethernet over MPLS using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None

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

Procedure

Perform any of the following procedures as needed:

- DLP-J84 Configure Ethernet over MPLS in VLAN Mode Using Cisco IOS Commands, on page 334
- DLP-J85 Configure Ethernet over MPLS in Port Mode Using Cisco IOS Commands, on page 335
- DLP-J86 Configure Ethernet over MPLS with VLAN ID Rewrite Using Cisco IOS Commands, on page 337
- DLP-J87 Configure MTU for Ethernet over MPLS Using Cisco IOS Commands, on page 339

Stop. You have completed this procedure.

DLP-J84 Configure Ethernet over MPLS in VLAN Mode Using Cisco IOS Commands

Purpose	This procedure configures Ethernet over MPLS in VLAN mode using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note You must configure Ethernet over MPLS in VLAN mode on the EFPs.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	Router> enable	
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**serviceinstance** *serviceinstanceid* **ethernet** **Example:** Router(config-if)# serviceinstance 100 ethernet	Specifies the service instance to configure and enters service instance configuration mode. Ensure that the EFPs between the CE and PE routers that are running Ethernet over MPLS are in the same subnet.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** Router(config-if-srv)# encapsulation dot1q 100	Enables the EFP to accept 802.1Q VLAN packets.
Step 6	**xconnect** *peer-router-id vcid* **encapsulation mpls** **Example:** Router(config-if-srv)# xconnect 10.0.0.1 123 encapsulation mpls	Binds the attachment circuit to a pseudowire VC.
Step 7	Return to your originating procedure (NTP).	—

DLP-J85 Configure Ethernet over MPLS in Port Mode Using Cisco IOS Commands

Purpose	This procedure configures Ethernet over MPLS in port mode using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**service instance** *serviceinstanceid* **ethernet** **Example:** Router(config-if)# service instance 100 ethernet	Specifies the service instance and enters service instance configuration mode. Ensure that the EFPs between the CE and PE routers that are running Ethernet over MPLS are in the same subnet.
Step 5	**encapsulation default** **Example:** Router(config-if-srv)# encapsulation default	Enables the EFP to accept all the packets (tagged and untagged).
Step 6	**xconnect** *peer-router-id vcid* **encapsulation mpls** **Example:** Router(config-if-srv)# xconnect 10.0.0.1 123 encapsulation mpls	Binds the attachment circuit to a pseudowire VC. The syntax for this command is the same as for all other Layer 2 transports.
Step 7	**exit** **Example:** Router(config-if-srv)# exit	Exits service instance configuration mode.
Step 8	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode.
Step 9	Return to your originating procedure (NTP).	—

DLP-J86 Configure Ethernet over MPLS with VLAN ID Rewrite Using Cisco IOS Commands

Purpose	This procedure configures Ethernet over MPLS with VLAN ID rewrite using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

The VLAN ID rewrite feature enables you to use VLAN interfaces with different VLAN IDs at both ends of the tunnel.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**service instance** *id* **ethernet** **Example:** Router(config-if)# service instance 100 ethernet	Configures an Ethernet service instance on an interface and enters service instance configuration mode. • Ensure that the EFPs between the CE and PE routers that are running Ethernet over MPLS are in the same subnet.
Step 5	**encapsulation dot1q** *vlan-id* **Example:**	Enables the EFP to accept 802.1Q VLAN packets.

	Command or Action	Purpose
	Router(config-if-srv)# encapsulation dot1q 100	
Step 6	**rewrite ingress tag push** | **pop** | **translate** **Example:** Router(config-if-srv)# rewrite ingress tag push dot1q 20	Specifies the rewrite operation to be applied on the frame ingress to the service instance.
Step 7	**xconnect** *peer-router-id vcid* **encapsulation mpls** **Example:** Router(config-if-srv)# xconnect 10.0.0.1 123 encapsulation mpls	Binds the attachment circuit to a pseudowire VC and enters cross–connect configuration mode.
Step 8	**exit** **Example:** Router(config-if-srv-xconn)# exit	Exits cross–connect configuration mode.
Step 9	**exit** **Example:** Router(config-if-srv)# exit	Exits service instance configuration mode.
Step 10	**exit** **Example:** Router(config)# exit	Exits global configuration mode.
Step 11	Return to your originating procedure (NTP).	—

Example: Configure Ethernet over MPLS with VLAN ID Rewrite

The following example shows how to configure VLAN ID rewrite on peer PE routers.

PE1:

```
interface TenGigabitEthernet4/1
encapsulation dot1Q 2
no ip directed-broadcast
no cdp enable
rewrite ingress tag push dot1q 20
xconnect 10.5.5.5 2 encapsulation mpls
```

PE2:

```
interface TenGigabitEthernet4/2
encapsulation dot1Q 3
no ip directed-broadcast
no cdp enable
```

```
rewrite ingress tag push dot1q 30
xconnect 10.3.3.3 2 encapsulation mpls
```

DLP-J87 Configure MTU for Ethernet over MPLS Using Cisco IOS Commands

Purpose	This procedure configures MTU for Ethernet over MPLS using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface and enters interface configuration mode.
Step 4	**mtu** *mtu-value* **Example:** Router(config-if)# mtu 2000	Specifies the MTU value for the interface. The MTU value specified at the interface level can be inherited by a EFP.
Step 5	**service instance** *serviceinstanceid* **ethernet** **Example:** Router(config-if)# service instance 100 ethernet	Specifies the service instance and enters service instance configuration mode. Ensure the EFP on the adjoining CE router is on the same VLAN as this PE router.
Step 6	**encapsulation dot1q** *vlan-id* **Example:**	Enables the EFP to accept 802.1Q VLAN packets. The EFPs between the CE and PE routers that are

	Command or Action	Purpose
	Router(config-if-srv)# encapsulation dot1q 100	running Ethernet over MPLS must be in the same subnet.
Step 7	**xconnect** *peer-router-id vcid* **encapsulation mpls** **Example:** Router(config-if-srv)# xconnect 10.0.0.1 123 encapsulation mpls	Binds the attachment circuit to a pseudowire VC.
Step 8	**end** **Example:** Router(config-if-srv)# end	Exits the cross-connect service instance configuration mode and returns to global configuration mode.
Step 9	**show mpls l2transport binding** **Example:** Router# show mpls l2transport binding	Displays the MTU values assigned to the local and remote interfaces.
Step 10	Return to your originating procedure (NTP).	—

Understanding L2VPN Pseudowire

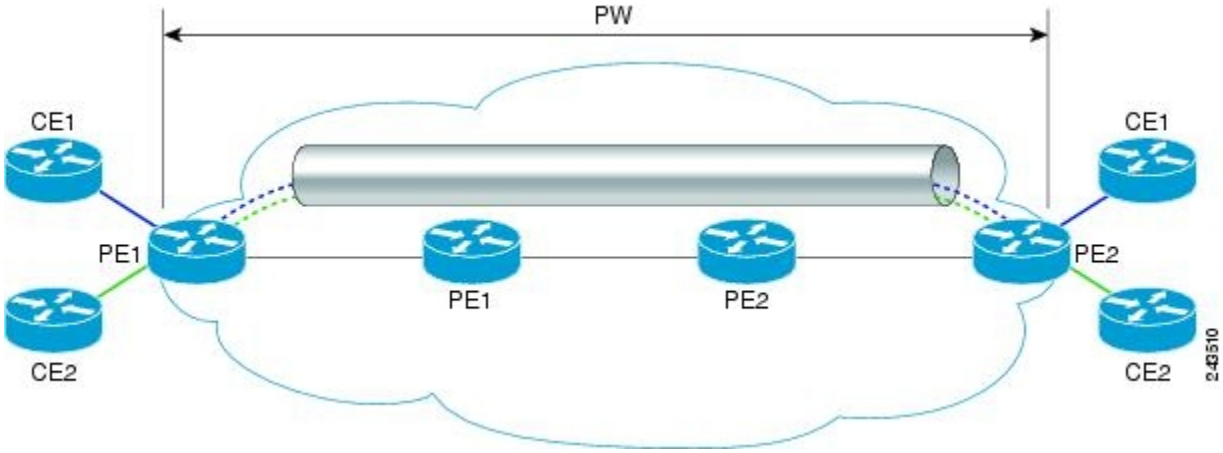
supports the forwarding of the Ethernet frames coming from the customer networks under AToM. The technique used to transport such a frame is called a pseudowire that is the emulation of a native service over the MPLS network.

Note You can create static and dynamic pseudowires. The static pseudowire can carry traffic over LDP, MPLS-TE tunnels, and MPLS-TP tunnels. The dynamic pseudowire can carry traffic over LDP and MPLS–TE tunnels.

An L2VPN pseudowire is a tunnel established between the two PE routers across the core carrying the Layer 2 payload encapsulated as MPLS data, as shown in Figure 53: An L2VPN Pseudowire, on page 341. This helps the carriers migrate from Layer 2 networks such as Ethernet over MPLS to an MPLS core. In the L2VPN pseudowire shown in Figure 54: A Multisegment Pseudowire, on page 341, the pseudowires between the two

PE routers are located within the same autonomous system. The routers PE1 and PE2 are called terminating PE routers (T-PEs). The attachment circuits (AC) are bound to the pseudowire on these PE routers.

Figure 53: An L2VPN Pseudowire



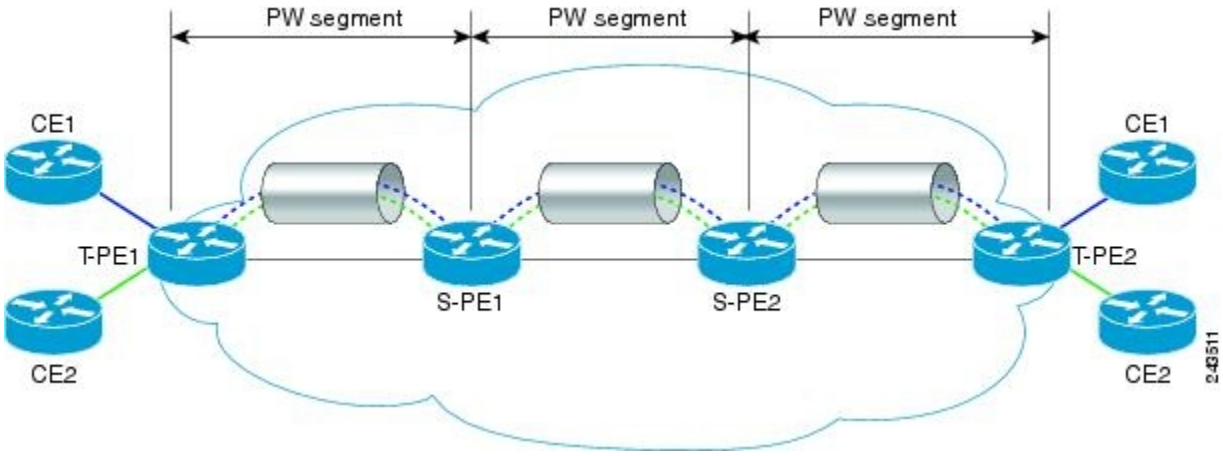
Dual homed pseudowire is a pseudowire protected circuit where the destination point is split on two different nodes.

Understanding L2VPN Multisegment Pseudowire

An L2VPN multisegment pseudowire is a set of two or more pseudowire segments that function as a single pseudowire. It is also known as stitched pseudowire. The multisegment pseudowires span multiple cores or autonomous systems of the same or different carrier networks. An L2VPN multisegment pseudowire can include up to 254 pseudowire segments.

The end routers are called terminating PE routers (T-PEs), and the switching routers are called S-PE routers. The S-PE router terminates the tunnels of the preceding and succeeding pseudowire segments in a multisegment pseudowire. The S-PE router can switch the control and data planes of the preceding and succeeding pseudowire segments of the multisegment pseudowire. A multisegment pseudowire is declared to be up when all the single-segment pseudowires are up.

Figure 54: A Multisegment Pseudowire



You can create both static segments and dynamic segments for a multisegment pseudowire. When you enable the control word on one segment, ensure that the control word is enabled on the other segments as well.

See Static and Dynamic Multisegment Pseudowires for MPLS–TP, on page 345 for information on multisegment pseudowires for MPLS–TP.

Restrictions for L2VPN Multisegment Pseudowires

- Only MPLS Layer 2 pseudowires are supported.
- The L2VPN Pseudowire Stitching feature is supported for pseudowires advertised with FEC 128. FEC 129 is not supported.
- The S-PE router is limited to 1600 pseudowires.

Supported Pseudowire Combinations

The following table lists the types of tunnels that are supported for static and dynamic single segment pseudowires.

Pseudowire Type	LDP	MPLS-TE Tunnel	MPLS-TP Tunnel with IP Address	MPLS-TP Tunnel without IP Address
Static	Yes	Yes	Yes	Yes
Dynamic	Yes	Yes	No	No

The following table lists the OAM protocols supported for static and dynamic single segment pseudowires.

Pseudowire Type	Targeted LDP	Static OAM	BFD over VCCV	BFD over VCCV with AC Status Signaling
Static pseudowire over MPLS-TP	No	Yes	Yes	Yes
Static pseudowire over LDP	No	Yes	Yes	Yes
Static pseudowire over MPLS-TE	No	Yes	Yes	Yes
Dynamic pseudowire over LDP	Yes	No	Yes	No
Dynamic pseudowire over MPLS-TE	Yes	No	Yes	No

The following table lists the OAM protocols supported for static and dynamic multisegment pseudowires.

Pseudowire Type	Targeted LDP	Static OAM	BFD over VCCV	BFD over VCCV with AC Status Signaling
Static-Static	No	Yes	Yes	Yes

Pseudowire Type	Targeted LDP	Static OAM	BFD over VCCV	BFD over VCCV with AC Status Signaling
Static-Dynamic	Yes	Yes	Yes	Yes
Dynamic-Dynamic	Yes	Not applicable	Yes	Not applicable

Note CPT shall support CESoP and SAToP interoperability to external world (e.g. Cisco 7600, Cisco ASR9000) over static pseudowire, if TDM SFP is provisioned.

Rewrite Operations on Pseudowire

The following tables list the rewrite operations supported on pseudowire.

Table 11: Ingress Rewrite Operations on Pseudowire

EFP Encapsulation	Incoming Encapsulation Type	Ingress Rewrite Operation	Outgoing Encapsulation Type	Pseudowire Type
encapsulation dot1q *vlan id*	0x8100	• No rewrite • Pop 1 symmetric • Push 1 symmetric • 1:1 translate symmetric	0x8100	Ethernet and VLAN
encapsulation dot1q *vlan id*	0x8100	• 1:1 translate symmetric e-type • Push 1 symmetric	0x8100	Ethernet
encapsulation dot1q *vlan id*	0x8100	• No rewrite	Not applicable	Ethernet and VLAN
encapsulation dot1q *vlan id*	0x8100	• Pop 1 symmetric	any	Ethernet and VLAN
encapsulation dot1q *vlan id*	0x8100	• Push 1 symmetric	any	Ethernet
encapsulation dot1q *vlan id*	0x8100	• 1:1 translate	any	Ethernet

EFP Encapsulation	Incoming Encapsulation Type	Ingress Rewrite Operation	Outgoing Encapsulation Type	Pseudowire Type
encapsulation dot1q any	0x8100	• No rewrite	Not applicable	Ethernet and VLAN
encapsulation dot1q any	0x8100	• Push 1 symmetric	0x8100	Ethernet and VLAN
encapsulation dot1q any	0x8100	• No rewrite	Not applicable	Ethernet
encapsulation untagged	0x8100	• No rewrite • Push 1 symmetric	0x8100	Ethernet and VLAN
encapsulation untagged	0x8100	• Push 1 symmetric	0x8100	Ethernet
encapsulation default	Not applicable	• No rewrite	Not applicable	Ethernet and VLAN
encapsulation default	Not applicable	• Push 1 symmetric	0x8100	Ethernet and VLAN
encapsulation default	Not applicable	• Push 1 symmetric	0x8100	Ethernet
encapsulation double tagged	0x8100 and second 0x8100	• Pop 1 symmetric	0x8100	Ethernet and VLAN
encapsulation double tagged	0x8100 and second 0x8100	• 1:1 translate symmetric	0x8100 and second 0x8100	Ethernet and VLAN
encapsulation double tagged	0x8100 and second 0x8100	• 1:1 translate symmetric	0x8100	Ethernet
encapsulation double tagged	0x8100 and second 0x8100	• 1:1 translate symmetric	any	Ethernet
encapsulation double tagged	0x8100 and second 0x8100	• Pop 1 symmetric	0x8100	Ethernet and VLAN

EFP Encapsulation	Incoming Encapsulation Type	Ingress Rewrite Operation	Outgoing Encapsulation Type	Pseudowire Type
encapsulation double tagged	0x8100 and second 0x8100	• Pop 2 symmetric	0x8100 and second 0x8100	Ethernet
encapsulation dot1q range	0x8100	• No rewrite	Not applicable	Ethernet and VLAN
encapsulation dot1q range	0x8100	• Push 1 symmetric	0x8100	VLAN
encapsulation dot1q range	0x8100	• Push 1 symmetric	0x8100	Ethernet
encapsulation dot1ad any/range	0x8100	• No rewrite	0x8100	Ethernet and VLAN
encapsulation dot1ad any/range	0x8100	• Push 1 symmetric	any	Ethernet

Static and Dynamic Multisegment Pseudowires for MPLS–TP

MPLS-TP supports the following combinations of static and dynamic multisegment pseudowires:

- Static-static
- Static-dynamic
- Dynamic-static

MPLS–TP: Pseudowire Redundancy for Static and Dynamic Multisegment Pseudowires

MPLS-TP supports pseudowire redundancy for the following combinations of static and dynamic pseudowires:

- Static pseudowire with a static backup pseudowire
- Static pseudowire with a dynamic backup pseudowire
- Dynamic pseudowire with a static backup pseudowire

MPLS–TP: OAM Status for Static and Dynamic Multisegment Pseudowires

With static pseudowires, status notifications can be provided by BFD over VCCV or static pseudowire OAM protocol. However, BFD over VCCV sends only attachment circuit status code notifications. Hop-by-hop notifications of other pseudowire status codes are not supported. Therefore, static pseudowire OAM protocol is preferred. You can acquire per pseudowire OAM for attachment circuit/pseudowire notification over VCCV channel with or without the control word.

NTP-J30 Create a Pseudowire Class

Purpose	This procedure creates a pseudowire class.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J88 Create a Pseudowire Class Using Cisco IOS Commands, on page 346
- DLP-J89 Create a Pseudowire Class Using CTC, on page 348

Stop. You have completed this procedure.

DLP-J88 Create a Pseudowire Class Using Cisco IOS Commands

Purpose	This procedure creates a pseudowire class using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	• DLP-J97 Create and Configure BFD Templates Using Cisco IOS Commands, on page 293 • NTP-J35 Configure BFD Control Channel over VCCV Using Cisco IOS Commands, on page 379
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

When you create the pseudowire class, you specify the parameters of the pseudowire, such as the use of control word, preferred path, OAM class, and VCCV BFD template.

Note To create a pseudowire for TDM SFP, pseudowire class should not have control-word, sequencing, OAM, BFDoVCC, Dynamic tunnel and Dynamic Protocol attributes.

Note The Pseudowire-class shall not be deleted if it is in **use.**

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**pseudowire-class** *class-name* **Example:** Router(config)# pseudowire-class class1	Creates a pseudowire class with a name that you specify and enters pseudowire class configuration mode.
Step 4	**encapsulation** *type* **Example:** Router(config-pw-class)# encapsulation mpls	Specifies that MPLS is used as the encapsulation type for tunneling Layer 2 traffic over a pseudowire. You must specify MPLS encapsulation as part of the **xconnect** command or as part of a pseudowire class for the Virtual Circuits to work properly.
Step 5	**control-word** **Example:** Router(config-pw-class)# control-word	Enables the control word in a dynamic pseudowire connection.
Step 6	**protocol** {**ldp** | **none**} **Example:** Router(config-pw-class)# protocol ldp	Specifies the signaling protocol to be used to manage the pseudowires created from this pseudowire class.
Step 7	**preferred-path** {**interface tunnel** *tunnel-number* | **peer** {*ip-address* | *host-name*}} [**disable-fallback**] **Example:** Router(config-pw-class)# preferred-path interface tunnel 1 disable-fallback	Specifies the MPLS–TP or MPLS–TE tunnel path that must be used by the pseudowire. **Note** If multiple MPLS-TP tunnels are exist between same pair of nodes, configure the preferred path using the MPLS-TP tunnel having highest cost. The Tunnel cost shall not exceed 110.

	Command or Action	Purpose
Step 8	**status protocol notification static** *class-name* **Example:** Router(config-pw-class)# status protocol notification static oam-class1	Specifies a static OAM class.
Step 9	**vccv bfd template** *name* [**udp** | **raw-bfd**] **Example:** Router(config-pw-class)# vccv bfd template bfdtemplate1 raw-bfd	Enables BFD over VCCV for a pseudowire class.
Step 10	**exit** **Example:** Router(config-pw-class)# exit	Returns the router to the global configuration mode.
Step 11	—	Return to your originating procedure (NTP).

Example: Create a Pseudowire Class

The following example creates a pseudowire class using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# pseudowire-class class1
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# control-word
Router(config-pw-class)# protocol ldp
Router(config-pw-class)# preferred-path interface tunnel 1 disable-fallback
Router(config-pw-class)# status protocol notification static oam-class1
Router(config-pw-class)# vccv bfd template bfdtemplate1 raw-bfd
Router(config-pw-class)# exit
```

DLP-J89 Create a Pseudowire Class Using CTC

Purpose	This procedure creates a pseudowire class using CTC.
Tools/Equipment	None
Prerequisite Procedures	• DLP-J102 Create a Static OAM Class Using CTC, on page 304 • DLP-J98 Create and Configure BFD Templates Using CTC, on page 295
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note To create a pseudowire for TDM SFP, pseudowire class should not have control-word, sequencing, OAM, BFDoVCC, Dynamic tunnel and Dynamic Protocol attributes.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to create a pseudowire class.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Provisioning** tab.

Step 5 From the left pane, click **Pseudowire Class**.

Step 6 Click **Create**. The **Create Pseudowire Class** dialog box appears.

Step 7 Enter the name of the pseudowire class in the Name field.
The encapsulation type for tunneling Layer 2 traffic over a pseudowire is set to MPLS and cannot be changed.

Step 8 From the Interworking drop-down list, choose **VLAN** or **Ethernet**.
The Interworking option enables the translation between the different Layer 2 encapsulations.

Note If a pseudowire is to be created with same encapsulation at both the ends, create pseudowire class with interworking as "NONE", else with interworking as VLAN or Ethernet .

Step 9 If unchecked, check the **Control Word** check box to enable the control word in a dynamic pseudowire connection.

Step 10 Check the **Master Redundancy** check box to place the pseudowire redundancy group on this node in master mode.

Step 11 In the Preferred Path area, specify the MPLS–TP or MPLS–TE tunnel path that must be used by the pseudowire.

a) Check the **Enable** check box to enable the preferred path.
b) Choose **TP** or **TE** as the tunnel type for the preferred path.
c) Enter the tunnel ID in the Tunnel ID field.

Note If multiple MPLS-TP tunnels are exist between the same pair of nodes, configure the preferred path using the MPLS-TP tunnel having highest cost.

d) Check the **Disable Fallback** check box to disable the router from using the default path when the preferred path is unreachable.

Step 12 In the Protocol area, choose **LDP** or **NONE** to specify the signaling protocol to be used to manage the pseudowires created from this pseudowire class.

Note LDP cannot be enabled simultaneously if the Static OAM is enabled or vica versa.

Step 13 In the Sequencing area, specify the direction in which the sequencing of packets in a pseudowire is enabled.

a) Check the **Enable** check box to enable sequencing.
b) From the Sequencing drop-down list, choose **Transmit**, **Receive**, or **Both**.

- **Transmit—**This option updates the sequence number field in the headers of packets sent over the pseudowire according to the data encapsulation method that is used.
- **Receive—**This option keeps the sequence number field in the headers of packets received over the pseudowire. The packets that are not received in sequence are dropped.
- **Both—**This option enables both the transmit and receive options.

c) Enter a value in the Resync field. The Resync field is enabled when the protocol is chosen as **LDP**.

Step 14 In the BFDoVCCV area, enable BFD over VCCV for a pseudowire class.

a) Check the **Enable** check box to enable BFD over VCCV.
b) From the BFD Template drop-down list, choose a BFD template.
c) Check the **AC Status Signalling** check box to enable end-to-end attachment circuit status code notification using BFDoVCCV.

Step 15 In the Status OAM area:

a) Check the **Enable** check box to enable static OAM.
b) From the OAM Class drop-down list, choose a static OAM class.

Step 16 Click **OK** to create a pseudowire class.

Step 17 Return to your originating procedure (NTP).

NTP-J31 Configure a Pseudowire

Purpose	This procedure configures a pseudowire.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J90 Create a Pseudowire Using Cisco IOS Commands, on page 351
- DLP-J91 Create a Pseudowire Using CTC, on page 359
- DLP-J223 Edit a Pseudowire Using CTC, on page 363
- DLP-J92 Configure L2VPN Multisegment Pseudowires Using Cisco IOS Commands, on page 353

- DLP-J227 Configure Static-to-Static Multisegment Pseudowires for MPLS-TP Using Cisco IOS Commands, on page 355
- DLP-J228 Configure Static-to-Dynamic Multisegment Pseudowires for MPLS-TP Using Cisco IOS Commands, on page 357
- DLP-J93 Perform ping mpls and trace mpls Operations on L2VPN Multisegment Pseudowires Using Cisco IOS Commands, on page 365
- DLP-J94 Configure L2VPN Pseudowire Preferential Forwarding Using Cisco IOS Commands, on page 367

Stop. You have completed this procedure.

DLP-J90 Create a Pseudowire Using Cisco IOS Commands

Purpose	This procedure creates a static and dynamic pseudowire using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	• DLP-J88 Create a Pseudowire Class Using Cisco IOS Commands, on page 346 • DLP-J163 Create a MPLS-TE Tunnel Using Cisco IOS Commands, on page 267 or DLP–J106 Configure Tunnel Endpoints Using Cisco IOS Commands, on page 312 or Configure LDP.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

The successful transmission of the Layer 2 frames between the provider edge routers is due to the configuration of the PE routers. You set up the connection, called a pseudowire, between the routers.

Note Do not set labels to create a dynamic pseudowire.

Note If a VPWS is provisioned between two nodes where one node is running CPT version 9.7.0.2 or higher and the other node is running an older version than 9.702, before provisioning the pseudowire, edit the TDM SFP labels to the default values.

Note If a TDM SFP is used in a CPT 50 in IOS mode, shut both the ends of VPWS configured on a TDM interface in order to stop the traffic.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**xconnect** *peer-ip-address vcid* **encapsulation mpls pw-class** *pw-class-name* [**sequencing** {**transmit** | **receive** | **both**}] **Example:** Router(config-if)# xconnect 10.131.191.252 100 encapsulation mpls pw-class class1	Binds an attachment circuit to a pseudowire and configures a static pseudowire.
Step 5	**mpls label** *local-pseudowire-label remote-pseudowire-label* **Example:** Router(config-if-xconn)# mpls label 100 150	Sets the local and remote labels for the static pseudowire. Do not set labels to create a dynamic pseudowire. • The label must be an unused static label within the static label range configured using the **mpls label** command. • The **mpls label** command checks the validity of the label entered and displays an error message if it is not valid. The label supplied for the *remote-pseudowire-label* argument must be the value of the peer PE's local pseudowire label.
Step 6	**mpls control-word** **Example:**	Enables the MPLS control word. If you enable inclusion of the control word, it must be enabled on both ends of the connection for the circuit to work properly.

	Command or Action	Purpose
	Router(config-if-xconn)# no mpls control-word	
Step 7	**exit** **Example:** Router(config-if-xconn)# exit	Returns the router to interface configuration mode.
Step 8	**exit** **Example:** Router(config-if)# exit	Returns the router to global configuration mode. **Note** In scaled configuration, if shut or no shut operation performed on the core ports that have huge number of pseudowires configured, the CPT 50 may reboot due to high CPU utilization.
Step 9	Return to your originating procedure (NTP).	—

Example: Create a Pseudowire

The following example creates a static pseudowire using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# xconnect 10.131.191.251 100 encapsulation mpls pw-class class1
Router(config-if-xconn)# mpls label 100 150
Router(config-if-xconn)# no mpls control-word
Router(config-if-xconn)# exit
Router(config-if)# exit
```

DLP-J92 Configure L2VPN Multisegment Pseudowires Using Cisco IOS Commands

Purpose	This procedure configures L2VPN multisegment pseudowires using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	• DLP-J88 Create a Pseudowire Class Using Cisco IOS Commands, on page 346 • DLP-J163 Create a MPLS-TE Tunnel Using Cisco IOS Commands, on page 267 or DLP–J106 Configure Tunnel Endpoints Using Cisco IOS Commands, on page 312 or Configure LDP.

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**mpls label protocol ldp** **Example:** Router(config)# mpls label protocol ldp	Configures the use of LDP on all the interfaces.
Step 4	**mpls ldp router-id** *interface* **force** **Example:** Router(config)# mpls ldp router-id loopback0 force	Specifies the preferred interface for determining the LDP router ID.
Step 5	**pseudowire-class** *name* **Example:** Router(config)# pseudowire-class atom	Establishes a pseudowire class with a name that you specify, and enters pseudowire class configuration mode. Ensure that the interworking and control word are the same.
Step 6	**encapsulation mpls** **Example:** Router(config-pw-class)# encapsulation mpls	Specifies the tunneling encapsulation. For MPLS L2VPNs, the encapsulation type is mpls.
Step 7	**switching tlv** **Example:** Router(config-pw-class)# switching tlv	(Optional) Enables the advertisement of the switching point type, length, value (TLV) in label binding. This command is enabled by default.
Step 8	**exit** **Example:** Router(config-pw-class)# exit	Exits pseudowire class configuration mode.

	Command or Action	Purpose
Step 9	**l2 vfi** *name* **point-to-point** **Example:** Router(config)# l2 vfi atomtunnel point-to-point	Creates a point-to-point Layer 2 virtual forwarding interface (VFI) and enters VFI configuration mode.
Step 10	**description** *string* **Example:** Router(config-vfi)# description segment1	Provides a description of the switching PE router for a multisegment pseudowire.
Step 11	**neighbor** *ip-address vcid* {**encapsulation mpls** | **pw-class** *pw-class-name*} **Example:** Router(config-vfi)# neighbor 10.0.0.1 100 pw-class mpls	Sets up an emulated VC. Specify the IP address and the VC ID of the peer router. Also, specify the pseudowire class to use for the emulated VC. **Note** Only two **neighbor** commands are allowed for each **l2 vfi point-to-point** command.
Step 12	exit **Example:** Router(config-vfi)# exit	Returns to global configuration mode.
Step 13	Return to your originating procedure (NTP).	—

DLP-J227 Configure Static-to-Static Multisegment Pseudowires for MPLS-TP Using Cisco IOS Commands

Purpose	This procedure configures static-to-static multisegment pseudowires for MPLS–TP using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**l2 vfi** *name* **point-to-point** **Example:** Router(config)# l2 vfi atomtunnel point-to-point	Creates a point-to-point Layer 2 virtual forwarding interface (VFI) and enters VFI configuration mode.
Step 4	**neighbor** *ip-address vc-id* {**encapsulation mpls** | **pw-class** *pw-class-name*} **Example:** Router(config-vfi)# neighbor 10.0.0.1 100 pw-class mpls	Sets up an emulated VC. Specify the IP address and the VC ID of the peer router. Also, specify the pseudowire class to use for the emulated VC.
Step 5	**mpls label** *local-pseudowire-label remote-pseudowire-label* **Example:** Router(config-vfi-neighbor)# mpls label 100 150	Sets the local and remote labels for a static pseudowire.
Step 6	**mpls control-word** **Example:** Router(config-vfi-neighbor)# mpls control-word	Enables the MPLS control word. **Note** Repeat steps 4, 5, and 6 for another static pseudowire.
Step 7	**exit** **Example:** Router(config-vfi-neighbor)# exit	Exits VFI neighbor configuration mode.
Step 8	Return to your originating procedure (NTP). **Example:** —	

DLP-J228ConfigureStatic-to-DynamicMultisegmentPseudowiresforMPLS-TP Using Cisco IOS Commands

Purpose	This procedure configures static-to-dynamic multisegment pseudowires for MPLS–TP using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note When you configure static-to-dynamic pseudowires, you configure the static pseudowire class with the **protocol none** command.

Procedure

	Command or Action	Purpose
Step 1	Configure the static pseudowire. **Example:** **1** enable **2** configure terminal **3** pseudowire-class *class-name* **4** mpls control-word **5** protocol none **6** exit	Configures the static pseudowire.
Step 2	Configure the dynamic pseudowire. **Example:** **1** enable **2** configure terminal **3** pseudowire-class *class-name* **4** mpls control-word	Configures the dynamic pseudowire using ldp protocol.

	Command or Action	Purpose
Step 3	**enable** **Example:** Router> enable	Enables privileged EXEC mode. Perform the following steps to configure the static-to-dynamic multisegment pseudowire. • Enter your password if prompted.
Step 4	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 5	**l2 vfi** *name* **point-to-point** **Example:** Router(config)# l2 vfi atomtunnel point-to-point	Creates a point-to-point Layer 2 virtual forwarding interface (VFI) and enters VFI configuration mode.
Step 6	**neighbor** *ip-address vc-id* {**encapsulation mpls** | **pw-class** *pw-class-name*} **Example:** Router(config-vfi)# neighbor 10.0.0.1 100 pw-class mpls	Sets up an emulated VC. Specify the IP address and the VC ID of the peer router. Also, specify the pseudowire class to use for the emulated VC.
Step 7	**mpls label** *local-pseudowire-label remote-pseudowire-label* **Example:** Router(config-vfi-neighbor)# mpls label 100 150	Sets the local and remote labels for a static pseudowire.
Step 8	**mpls control-word** **Example:** Router(config-vfi-neighbor)# mpls control-word	Enables the MPLS control word.
Step 9	**local interface** *pseudowire-type* **Example:** Router(config-vfi-neighbor)# local interface 5	Specifies the pseudowire type when configuring static to dynamic pseudowires.
Step 10	**tlv template** *template-name* **Example:** Router(config-vfi-neighbor-interface)# tlv template net	Specifies a TLV template to use as part of the local interface configuration.
Step 11	**exit** **Example:** Router(config-vfi-neighbor-interface)# exit	Exits VFI neighbor interface configuration mode.
Step 12	Return to your originating procedure (NTP).	

Example: Configure Static-to-Dynamic Multisegment Pseudowires for MPLS-TP

The following example shows how to configure a TLV template:

```
Router(config)#pseudowire-tlv template tlv-template-name
Router(config-pw-tlv-template)#tlv mtu-value 1 4 dec 1500
Router(config-pw-tlv-template)#tlv vccv-flags C 4 hexstr 0108
Router(config-pw-tlv-template)#exit
```

The following example shows how to configure VFI at an SPE node:

```
Router(config)#l2 vfi vfi::1 point-to-point
Router(config-vfi)#neighbor 3.3.3.3 1 pw-class PW_LDP_VPWS
Router(config-vfi)#neighbor 1.1.1.1 1 pw-class PW_TP_1_VPWS
Router(config-vfi-neighbor)#mpls label 17 17
Router(config-vfi-neighbor)#local interface 5
Router(config-vfi-neighbor-interface)#tlv template tlv-template-name
Router(config-vfi-neighbor-interface)#exit
Router(config-vfi-neighbor)#exit
```

DLP-J91 Create a Pseudowire Using CTC

Purpose	This procedure allows you to do the following: • Create a pseudowire • Create a multisegment pseudowire • Create a backup pseudowire
Tools/Equipment	None
Prerequisite Procedures	• DLP-J89 Create a Pseudowire Class Using CTC, on page 348 • DLP–J166 Create an MPLS–TE Tunnel Using CTC, on page 274 or DLP-J107 Create an MPLS–TP Tunnel Using CTC, on page 316 or Configure LDP.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

The pseudowire configuration can be EVC VLAN–based or EVC port–based. CPT supports only Ethernet over MPLS as the transport type for pseudowire.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to create a pseudowire.

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

Step 3 Click the **Layer2+** tab.

Step 4 From the left pane, click **Circuits**.

Step 5 Click the **Pseudowire** tab.

Step 6 Click **Create**. The Circuit Creation wizard appears.

Step 7 In the AC Global Attributes area of the Circuit Attributes screen, specify the global attributes as follows:

a) Enter the name of the pseudowire that you want to create in the PW Name field.
b) Enter the description of the pseudowire in the PW Description field.
c) From the Admin State drop-down list, choose **UP** or **DOWN**. The default value is UP.
d) Enter the bandwidth value in Kbps, Mbps (default), or Gbps in the Bandwidth field.

Step 8 In the Redundancy area of the Circuit Attributes screen, specify the following to create a redundant pseudowire:

a) Check the **Enabled** check box to enable pseudowire redundancy.
b) Check the **Dual Homed Peer** check box to create a special case of pseudowire protection. In this case, there is an additional end point (T-PE3) for the pseudowire apart from T-PE1 and T-PE2.
c) Check the **Provision working go & return on primary path** check box to enable the user to configure working go and return path of a pseudowire on primary path. For example, if this checkbox is unchecked, a pseudowire A is primary pseudowire and pseudowire B is backup pseudowire on T-PE1 node, pseudowire A must be backup pseudowire and pseudowire B must be primary pseudowire on T-PE2 node.
d) Enter the delay timer in seconds in the Enable Delay field to specify how long the backup pseudowire must wait to take over after the primary pseudowire goes down. The range is from 0 to 180 seconds.
e) Enter the delay timer in seconds in the Disable Delay field to specify how long the primary pseudowire must wait after it becomes active to take over from the backup pseudowire. The range is from 0 to 180 seconds.
f) Click the **Never** radio button to specify that the primary pseudowire never takes over from the backup pseudowire.
g) Click **Next**.
The T-PE1 screen appears. Terminating Provider Edge (T-PE1) represents one of the end points of the pseudowire.

Step 9 To choose a non CPT source node for the pseudowire, complete the following steps:

a) Check the **Unmanaged Node** check box.
At least one node (T-PE or S-PE node) in the pseudowire must be a CPT node. The other nodes can be unmanaged nodes.
b) Enter the router IP address in the Router ID field.
c) Enter the VC ID in the VC ID field.

Step 10 To choose a CPT source node for the pseudowire, choose the CPT node from the Node drop-down list. The Router ID field is automatically populated.

Note If a VPWS is provisioned between two nodes where one node is running CPT version 9.7.0.2 and the other node is running older version. Before provisioning the pseudowire, set the TDM SFP labels to the default value.

Step 11 In the AC End Point area of the T-PE1 screen, identify the attachment circuit (AC) with the exact end point of the CPT node as follows:

The attachment circuit is the physical or virtual circuit attaching a CE to a PE.

a) If you want to choose a port or CPT 50 to serve as an end point for the pseudowire, complete the following:

1. Check the RING ID check box.
   Note This check box is enabled only if the service state of the ring is enabled.
2. From the RING ID drop-down list, choose a ring.
   Note This drop down list is enabled only if the RING ID check box is checked.
3. From the Slot/CPT 50 drop-down list, choose a slot or CPT 50.
   Note If you select the RING ID check box, a list of available CPT 50 is displayed. Otherwise, a list of available ports is displayed.
4. From the Port drop-down list, choose a port.

b) If you want to choose a channel group to serve as an end point for the pseudowire, complete the following:

1. Check the **CHGRP** check box.
2. From the CHGRP drop-down list, choose a channel group to serve as an end point.
3. Click **Manual Load Balancing** to configure manual load balancing on the ports of the channel group.
   The Manual Load Balancing dialog box appears.
4. From the Primary Loadbalanced Link list, choose a port.
5. Click **Apply**.

Step 12 In the AC Attributes area of the T-PE1 screen, specify the following:

a) From the AC Type drop-down list, choose **EVC Port Based** or **EVC VLAN Based**.
b) (For EVC VLAN Based AC Type) Click the **EFP Configuration** link. The EFP Configuration dialog box appears.
c) (For EVC VLAN Based AC Type) In the Outer VLAN Configuration area, choose the type of VLAN tagging:

- Double Tagged
- Single Tagged
- Untagged
- Default
- Any

d) (For EVC VLAN Based AC Type) From the TPID drop-down list, choose a TPID—dot1q, dot1ad, 0x9100, or 0x9200.
e) (For EVC VLAN Based AC Type) Enter a VLAN tag in the VLAN Tag field.
f) (For EVC VLAN Based AC Type) In the Inner VLAN Configuration area, enter the TPID and VLAN tag.
g) (For EVC VLAN Based AC Type) In the Rewrite Ingress Operation area, choose the rewrite operation:

- PUSH 1
- PUSH 2

- POP 1
- POP 2
- TRANSLATE 1-to-1
- TRANSLATE 1-to-2
- TRANSLATE 2-to-1
- TRANSLATE 2-to-2

See Rewrite Operations on Pseudowire, on page 343 to determine the supported ingress rewrite operations on pseudowire.

h) (For EVC VLAN Based AC Type) From the Outer VLAN TPID drop-down list, choose a TPID—dot1q, dot1ad, 0x9100, or 0x9200.
i) (For EVC VLAN Based AC Type) Enter the outer VLAN tag in the Outer VLAN Tag field.
j) Check the **Symmetric** check box to enable symmetric rewrite operations.
k) (For EVC VLAN Based AC Type) Enter the inner VLAN TPID in the Inner VLAN TPID field.
l) (For EVC VLAN Based AC Type) Enter the inner VLAN tag in the Inner VLAN Tag field.
m) (For EVC VLAN Based AC Type) In the Enable Statistics area, check the **Ingress** and **Egress** check boxes as needed.
n) (For EVC VLAN Based AC Type) Click **OK** to save this EFP configuration.
o) (For EVC Port Based and EVC VLAN Based AC Types) Click the **QoS Configuration** link. The QoS Configuration dialog box appears.
p) (For EVC Port Based and EVC VLAN Based AC Types) Specify the table map, ingress policy, and egress policy and click **OK**.

Step 13 In the PW Attributes area of the T-PE1 screen, specify the following:

a) From the PW class drop-down list, choose a pseudowire class.
b) Enter the VC ID used by the pseudowire in the VC ID field.
c) Check the **Static** check box to specify that the pseudowire segment starting from T-PE1 is static. Otherwise, the pseudowire segment is dynamic.
d) (For static pseudowire segment) Enter an unused static label in the Local Label field.

Step 14 In the Backup PW Attributes area of the T-PE1 screen, specify the following:

a) From the PW class drop-down list, choose a PW class for the backup pseudowire.
b) Enter the VC ID used by the backup pseudowire in the VC ID field.
c) Check the **Static** checkbox to specify that the backup pseudowire segment starting from T-PE1 is static. Otherwise, the backup pseudowire segment is dynamic.
d) (For static backup pseudowire segment) Enter an unused static label in the Local Label field.
e) Click **Next**.
The T-PE2 screen appears. T-PE2 represents one of the end points of the pseudowire.

Step 15 From the Node drop-down list, choose the destination node for the pseudowire.
You can choose a CPT or non CPT node as the destination node similar to the source node.

Step 16 Specify all the values in the T-PE2 screen similar to the previous T-PE1 screen.

Step 17 If you had checked the **Dual Homed Peer** check box in the Circuit Attributes screen, an additional screen appears to specify the settings for T-PE3.

Step 18 Click **Next**.
The PW Protected Circuit Path screen appears.

Step 19 In the PW Protected Circuit Path screen, specify the following for Switch Provider Edge (SPE) nodes to create a multisegment pseudowire.

Note Do not set the pseudowire class with the interworking at SPE nodes while creating a multisegment pseudowire. Setting this would corrupt the Label table.

a) Click the **SPEs Working** tab.
b) Select a node from the network map and click **Add**. The Add node dialog box appears.
c) From the Node drop-down list, choose a node and click **Apply**.
d) Enter the Neighbor ID and VC ID in the respective fields.
e) From the PW class drop-down list, choose a pseudowire class.
f) Check the **Static** check box to specify that the pseudowire segment is static. Otherwise, the pseudowire segment is dynamic.
g) (For static pseudowire segment) Enter an unused static label in the Local Label field.
h) Click the **Advanced Configuration** link. The **Advanced Configuration** link is enabled only when you stitch dynamic segment to static segment and vice versa.
The AC Advanced Configuration dialog box appears.
i) Specify the MTU, Requested VLAN, Interface Description, and VCCV Flags in the respective fields and click **OK**. You can specify a value from 64 to 9600 for MTU. The default value is 1500.
The MTU and Interface Description fields are applicable to dynamic segments. The Requested VLAN field is applicable to the static segment.

Note The MTU of a pseudowire can not be greater than the MTU of the LAG on which this pseudowire is configured.

Step 20 Click the **SPEs Backup** tab and specify all the values similar to the **SPEs Working** tab.

Step 21 Click **Finish** to create a pseudowire.

Note You cannot create a pseudowire successfully, if the TDM pluggable is already configured on the port and the pseudowire class has any of these configurations:

- TP as tunnel type
- Sequencing enabled
- BFD over VCCV enabled
- LDP as protocol
- Status OAM enabled

Note In scaled configuration, if shut or no shut operation performed on the core ports that have huge number of pseudowires configured, the CPT 50 may reboot due to high CPU utilization.

Step 22 Return to your originating procedure (NTP).

DLP-J223 Edit a Pseudowire Using CTC

Purpose	This procedure edits a pseudowire using CTC.
Tools/Equipment	None
Prerequisite Procedures	• DLP-J91 Create a Pseudowire Using CTC, on page 359

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

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to edit a pseudowire.

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

Step 3 Click the **Layer2+** tab.

Step 4 Click **Pseudo Wire**.

Step 5 From the list of pseudowires, select a pseudowire to edit.

Step 6 Click **Edit**. The **Edit Circuit** screen appears.

Step 7 In the General tab, modify the following attributes of the pseudowire as required and click **Apply**:

- Description

Step 8 In the T-PE Nodes tab, view the details of the terminating provider edge nodes that are the end points of this pseudowire.

a) In the PW Attributes area, view the attributes of this pseudowire.

Step 9 Click the **EFP Configuration**tab and view the configurations of the EFPs associated with this pseudowire. Edit the VLAN configuration for EFPs:

a) From the EFP drop-down list, choose an EFP to view its configuration.

b) From the EFP State drop-down list, choose UP or Down to change the up or down status of EFP.

c) In the Outer VLAN Configuration area, choose the type of VLAN tagging:

- Double Tagged
- Single Tagged
- Untagged
- Default
- Any

Note The VLAN tagging type chosen for Ethernet Private Line and Ethernet Private LAN is Default. Do not change this option for the source EFP.

d) Enter a VLAN tag in the VLAN Tag field. For example, enter 10,20,30-50 without white spaces in the VLAN Tag field.

e) In the Inner VLAN Configuration area, enter the VLAN tag. You cannot enter VLAN range for inner VLANs. The inner VLAN TPID cannot be changed.

f) In the Rewrite Ingress Operation area, choose the rewrite operation:

- PUSH 1
- PUSH 2
- POP 1

- POP 2
- TRANSLATE 1-to-1
- TRANSLATE 1-to-2
- TRANSLATE 2-to-1
- TRANSLATE 2-to-2

g) Enter the outer VLAN tag in the Outer VLAN Tag field. The Outer VLAN TPID cannot be changed.
h) Enter the inner VLAN tag in the Inner VLAN Tag field. The Inner VLAN TPID is dot1q and cannot be changed.
i) Click **Apply** to apply this configuration to the selected EFP
You Cannot edit the VLAN configurations of the EFP for VPWS if the following services are present.

- QOS
- Span
- CFM
- Y1731

Step 10 In the State tab, complete the following:
a) View the circuit status and service state of the pseudowire.
b) From the Target PW Admin State drop-down list, choose UP or DOWN to change the administrative state of the pseudowire.
c) Click **Apply**.

Step 11 In the QoS tab, modify the table map, ingress policy, and egress policy of the pseudowire as required and click **Apply**.

Step 12 Close the **Edit Circuit** screen.

Note You can not create a pseudowire on the channel group port on which destination port of a span is already configured.

Note In scaled configuration, if shut or no shut operation performed on the core ports that have huge number of pseudowires configured, the CPT 50 may reboot due to high CPU utilization.

Step 13 Return to your originating procedure (NTP).

DLP-J93 Perform ping mpls and trace mpls Operations on L2VPN Multisegment Pseudowires Using Cisco IOS Commands

Purpose	Use the **ping mpls** and **trace mpls** commands to verify that all the segments of the MPLS multisegment pseudowire are operating.
Tools/Equipment	None
Prerequisite Procedures	None

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

You can use the **ping mpls** command to verify connectivity at the following pseudowire points:

- From one end of the pseudowire to the other
- From one of the pseudowires to a specific segment
- The segment between two adjacent S-PE routers

You can use the **trace mpls** command to verify connectivity at the following pseudowire points:

- From one end of the pseudowire to the other
- From one of the pseudowires to a specific segment
- The segment between two adjacent S-PE routers
- A range of segments

Note Enable **l2 router-id IP address** command for static pseudowire ping operation to work. It is recommended to set up the router-id to the loopback0 IP address. This IP address must be the same IP address that is used in the **mpls ldp router-id** LDP command.

Note The ping and trace operation for multisegment pseudowires that have one or more static pseudowire segments is not supported.

Note The ping for multisegment pseudowires on TDM interfaces over MPLS-TP tunnels is not supported.

Procedure

	Command or Action	Purpose
Step 1	**ping mpls pseudowire** *destination-address vc-id* [**segment** *segment-number*] **Example:** Router# ping mpls pseudowire 10.10.10.9 220 1 reply mode control-channel	Performs a ping operation. • *destination-address* is the address of the S-PE router, which is the end of the segment from the direction of the source. • *vc-id* is the VC ID of the segment from the source to the next PE router. • *segment-number* is optional and specifies the segment you want to ping.

	Command or Action	Purpose
Step 2	**trace mpls pseudowire** *destination-address vc-id* **segment** *segment-number* [*segment-number*] **Example:** Router# trace mpls pseudowire 10.10.10.9 220 segment reply mode control-channel	Performs a trace operation. • *destination-address* is the address of the next S-PE router from the origin of the trace. • *vc-id* is the VC ID of the segment from which the trace command is issued. • *segment-number* indicates the segment on which the trace operation acts. If you enter the two segment numbers, the **traceroute** operation performs a trace on that range of routers.
Step 3	Return to your originating procedure (NTP).	—

DLP-J94 Configure L2VPN Pseudowire Preferential Forwarding Using Cisco IOS Commands

Purpose	This procedure configures L2VPN pseudowire preferential forwarding using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**pseudowire-class** *class-name* **Example:** Router(config)# pseudowire-class atom	Establishes a pseudowire class with a name that you specify, and enters pseudowire class configuration mode.
Step 4	**encapsulation mpls** **Example:** Router(config-pw)# encapsulation mpls	Specifies the tunneling encapsulation. For AToM, the encapsulation type is mpls.
Step 5	**status redundancy** {*master* | *slave*} **Example:** Router(config-pw)# status redundancy master	Specifies the pseudowire as the master or slave. This enables the L2VPN Pseudowire Preferential Forwarding feature to display the status of the active and backup pseudowires. By default, the PE router is in slave mode. **Note** One pseudowire must be the master and the other must be assigned the slave. You cannot configure both the pseudowires as master or slave • Status redundancy master must be configured on one of the end of pseudowire class if both the ends of the pseudowire has a backup configuration. • Status redundancy master shall be configured on the end of that pseudowire class which has the backup configuration in case of dual-homed pseudowire. .
Step 6	**interworking** {*ethernet* | *vlan*} **Example:** Router(config-pw)# interworking vlan	(Optional) Enables the translation between the different Layer 2 encapsulations.
Step 7	**exit** **Example:** Router(config-pw)# exit	Returns to global configuration mode.
Step 8	Return to your originating procedure (NTP).	—

Example: Configure L2VPN Pseudowire Preferential Forwarding

The following example shows how to configure a PE router with the L2VPN Pseudowire Preferential Forwarding feature:

```
mpls ldp graceful-restart
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp advertise-labels
!
pseudowire-class mpls
 encapsulation mpls
 status redundancy master

interface TenGigabitEthernet4/1
 service instance 1 ethernet
 encapsulation dot1q 10
  xconnect 1.1.1.1 123 encapsulation mpls
   backup peer 1.1.1.2 123
end
```

Understanding L2VPN Pseudowire Redundancy

The L2VPN Pseudowire Redundancy feature enables you to set up backup pseudowires.

The L2VPN Pseudowire Redundancy feature lets you configure the network to detect a failure in the network and reroute the Layer 2 (L2) service to another end point that can continue to provide the service. This feature provides the ability to recover from a failure either of the remote PE router or of the link between the PE and CE routers.

The L2VPN Pseudowire Redundancy feature enables you to configure a backup pseudowire if the primary pseudowire fails. When the primary pseudowire fails, the PE router can switch to the backup pseudowire. You can have the primary pseudowire resume operation after it comes up.

Note The static pseudowire can be backed up by the dynamic pseudowire and vice versa.

Prerequisites

The L2VPN Pseudowire Redundancy feature requires the following mechanisms to detect a failure in the network:

- LSP ping/traceroute and Any Transport over MPLS Virtual Circuit Connection Verification (AToM VCCV)
- Operation, Administration, and Maintenance (OAM)

Restrictions

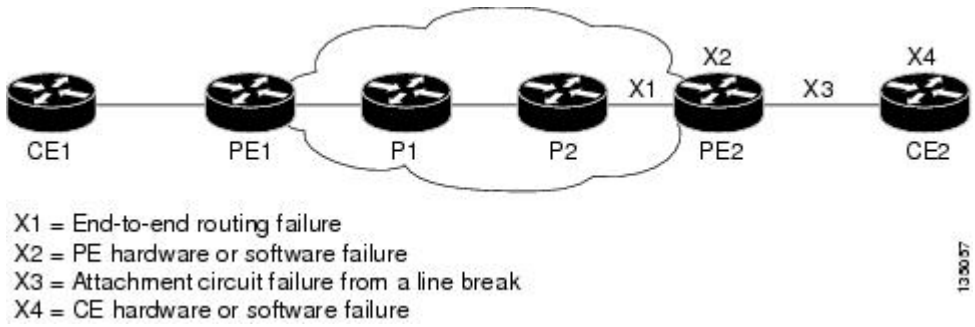
- The primary and backup pseudowires must run the same type of transport service. The primary and backup pseudowires must be configured with AToM.
- Only static, on-box provisioning is supported.
- If you use L2VPN Pseudowire Redundancy with L2VPN Interworking, the interworking method must be the same for the primary and backup pseudowires.

- Setting the experimental (EXP) bit on the MPLS pseudowire is supported.
- Different pseudowire encapsulation types on the MPLS pseudowire are not supported.
- The ability to have the backup pseudowire fully operational at the same time that the primary pseudowire is operational is not supported. The backup pseudowire becomes active only after the primary pseudowire fails.
- The AToM VCCV feature is supported only on the active pseudowire. The AToM VCCV feature is used for fault detection, isolation, and verification at both ends of the pseudowire.
- More than one backup pseudowire is not supported.

Pseudowire Redundancy

L2VPNs can provide pseudowire resiliency through their routing protocols. When connectivity between end-to-end PE routers fails, an alternative path to the directed LDP session and the user data can take over. However, there are some parts of the network where this rerouting mechanism does not protect against interruptions in service. Figure 55: Points of Potential Failure in an L2VPN Network, on page 370 shows those parts of the network that are vulnerable to an interruption in service.

Figure 55: Points of Potential Failure in an L2VPN Network



The L2VPN Pseudowire Redundancy feature provides the ability to ensure that the CE2 router in Figure 55: Points of Potential Failure in an L2VPN Network, on page 370 can always maintain network connectivity, even if one or all the failures in the figure occur.

Note In this release, a pseudowire can be protected by only one backup pseudowire.

You can configure the network with redundant pseudowires and redundant network elements, which are shown in Figure 56: L2VPN Network with Redundant PWs and Attachment Circuits, on page 371, Figure 57: L2VPN Network with Redundant PWs, Attachment Circuits, and CE Routers, on page 371, and Figure 58: L2VPN Network with Redundant PWs, Attachment Circuits, CE Routers, and PE Routers, on page 371.

Figure 56: L2VPN Network with Redundant PWs and Attachment Circuits, on page 371 shows a network with redundant pseudowires and redundant attachment circuits.

Figure 56: L2VPN Network with Redundant PWs and Attachment Circuits

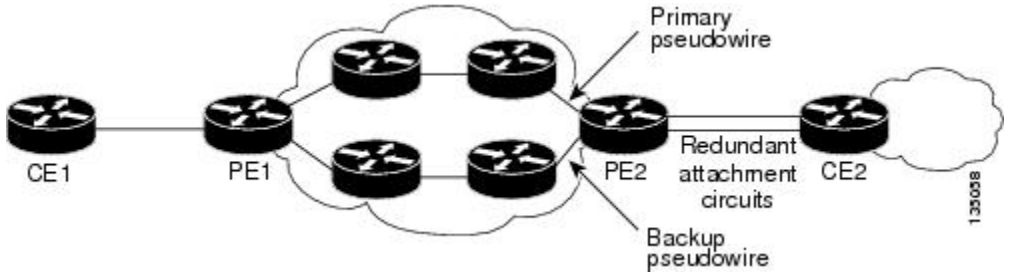


Figure 57: L2VPN Network with Redundant PWs, Attachment Circuits, and CE Routers, on page 371 shows a network with redundant pseudowires, attachment circuits, and CE routers.

Figure 57: L2VPN Network with Redundant PWs, Attachment Circuits, and CE Routers

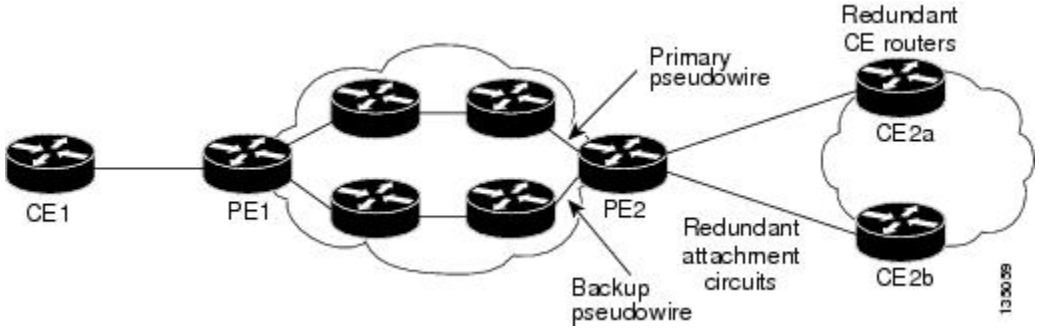
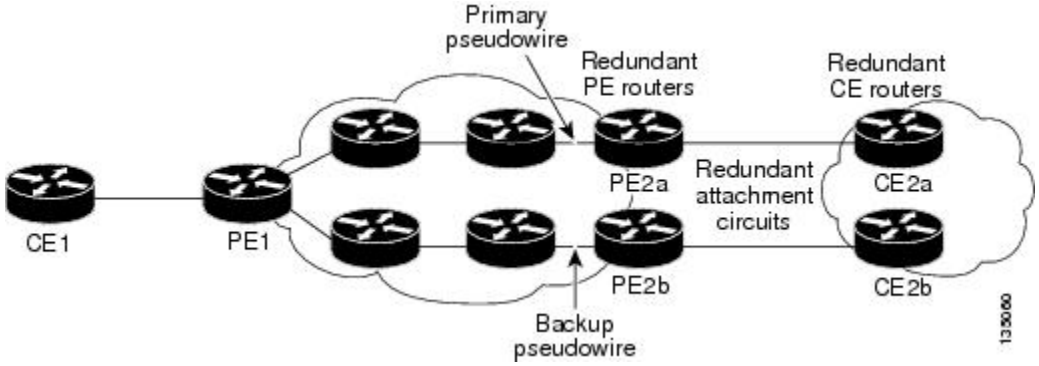


Figure 58: L2VPN Network with Redundant PWs, Attachment Circuits, CE Routers, and PE Routers, on page 371 shows a network with redundant pseudowires, attachment circuits, CE routers, and PE routers.

Figure 58: L2VPN Network with Redundant PWs, Attachment Circuits, CE Routers, and PE Routers



NTP-J32 Configure the Pseudowire Redundancy Using Cisco IOS Commands

Purpose	This procedure configures the L2VPN pseudowire redundancy feature using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**service instance** *serviceinstanceid* **ethernet** **Example:** Router(config-if)# service instance 100 ethernet	Specifies the service instance and enters service instance configuration mode. Ensure that the EFP on the adjoining CE router is on the same VLAN as this PE router.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** Router(config-if-srv)# encapsulation dot1q 100	Enables the EFP to accept 802.1Q VLAN packets. The EFPs between the CE and PE routers that are running Ethernet over MPLS must be in the same subnet.
Step 6	**xconnect** *peer-router-id vcid* {**encapsulation mpls** | **pw-class** *pw-class-name*}	Binds the attachment circuit to a pseudowire VC and enters xconnect configuration mode.

	Command or Action	Purpose
	Example: Router(config-if-srv)# xconnect 10.0.0.1 123 pw-class atom	
Step 7	**backup peer** *peer-router-ip-addr vcid* [**pw-class** *pw-class-name*] **Example:** Router(config-if-srv-xconn)# backup peer 10.0.0.3 125 pw-class atom	Specifies a redundant peer for the pseudowire VC. The pseudowire class name must match the name you specified when you created the pseudowire class, but you can use a different pw-class in the **backup peer** command than the name that you used in the primary **xconnect** command.
Step 8	**backup delay** *enable-delay* {*disable-delay* | **never**} **Example:** Router(config-if-srv-xconn)# backup delay 5 never	Specifies the period, in seconds, the backup pseudowire VC must wait to take over after the primary pseudowire VC goes down. The range is from 0 to 180 seconds. If you specify the **never** keyword, the primary pseudowire VC never takes over from the backup pseudowire VC. **Note** The range for backup delay for a redundant multi-segment pseudowire (protected MSPW) is from 0 to 60.
Step 9	**exit** **Example:** Router(config-if-srv-xconn)# exit	Returns to service instance configuration mode.
Step 10	**exit** **Example:** Router(config-if-srv)# exit	Returns to global configuration mode.
Step 11	Return to your originating procedure (NTP).	—

Examples

The following example shows an Ethernet attachment circuit cross-connect with L2VPN IP interworking and a backup pseudowire:

```
Router> enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# xconnect 10.0.0.1 123 pw-class mpls-ip
Router(config-if-srv-xconn)# backup peer 10.0.0.3 125 pw-class mpls-ip
```

Understanding MPLS Pseudowire Status Signaling

The MPLS Pseudowire Status Signaling feature enables you to configure the router to send the pseudowire status to a peer router, even when the attachment circuit (AC) is down. The MPLS Pseudowire Status Signaling feature enables the AC status to be sent to the peer through LDP. The pseudowire status messages are sent in label advertisement and label notification messages if the peer router also supports the MPLS Pseudowire Status Signaling feature.

Restrictions

- Both peer routers must support the ability to send and receive pseudowire status messages in label advertisement and label notification messages. If both peer routers do not support pseudowire status messages, it is recommended that you disable the messages with the **no status** command.
- This feature is not integrated with AToM Virtual Circuit Connection Verification (VCCV).

NTP-J33 Configure MPLS Pseudowire Status Signaling Using Cisco IOS Commands

Purpose	This procedure configures MPLS pseudowire status signaling using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Use this procedure to enable the router to send pseudowire status to a peer router even when the attachment circuit is down. If both routers do not support pseudowire status messages, then disable the messages with the **no status** command.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	Router# configure terminal	
Step 3	**pseudowire-class** *class-name* **Example:** Router(config)# pseudowire-class atom	Establishes a pseudowire class with a name that you specify and enters pseudowire class configuration mode.
Step 4	**status** **Example:** Router(config-pw)# status	(Optional) Enables the router to send pseudowire status messages to the peer router through label advertisement and label notification messages. By default, the status messages are enabled. This step is included only if status messages have been disabled. If both routers do not support pseudowire status messages, then disable the messages with the **no status** command.
Step 5	**encapsulation mpls** **Example:** Router(config-pw)# encapsulation mpls	Specifies the tunneling encapsulation.
Step 6	**exit** **Example:** Router(config-pw)# exit	Exits pseudowire class configuration mode.
Step 7	**exit** **Example:** Router(config)# exit	Exits global configuration mode.
Step 8	**show mpls l2transport vc detail** **Example:** Router# show mpls l2transport vc detail	Validates that pseudowire messages can be sent and received.
Step 9	Return to your originating procedure (NTP).	—

Example: Configure MPLS Pseudowire Status Signaling

The following example shows how to configure the MPLS Pseudowire Status Signaling feature using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# pseudowire-class atom
Router(config-pw)# status
Router(config-pw)# encapsulation mpls
Router(config-pw)# exit
Router(config)# exit
```

Understanding L2VPN Pseudowire Stitching

L2VPN Pseudowire Stitching defines a static or dynamically configured set of two or more pseudowire segments that behave and function as a single point-to-point pseudowire. L2VPN Pseudowire Stitching enables L2VPN pseudowires to extend across two separate MPLS networks or across an inter-AS boundary, as shown in Figure 59: L2VPN Pseudowire Stitching in an Intra-AS Topology, on page 376 and Figure 60: L2VPN Pseudowire Stitching in an Inter-AS Topology, on page 376.

L2VPN Pseudowire Stitching connects two or more contiguous pseudowire segments to form an end-to-end multihop pseudowire. This end-to-end pseudowire functions as a single point-to-point pseudowire.

As shown in Figure 60: L2VPN Pseudowire Stitching in an Inter-AS Topology, on page 376, L2VPN Pseudowire Stitching enables you to keep the IP addresses of the edge PE routers private across inter-AS boundaries. You can use the IP address of the Autonomous System Boundary Routers (ASBRs) and treat them as pseudowire aggregation (PE-agg) routers. The ASBRs join the pseudowires of the two domains.

Figure 59: L2VPN Pseudowire Stitching in an Intra-AS Topology

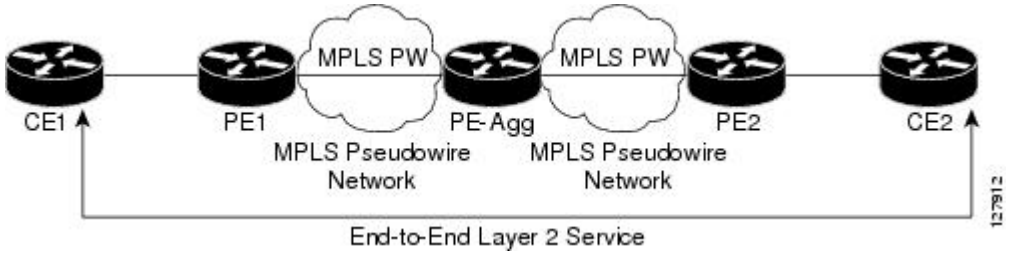
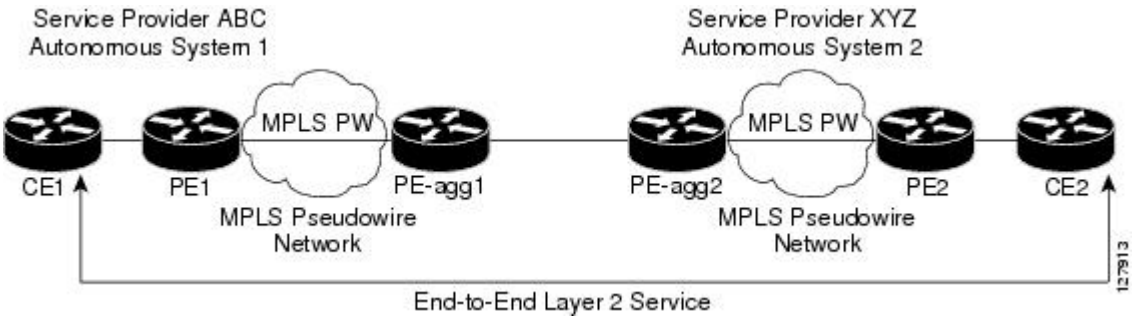


Figure 60: L2VPN Pseudowire Stitching in an Inter-AS Topology



Restrictions for L2VPN Pseudowire Stitching

- L2VPN Pseudowire Stitching is supported with AToM.
- Only static, on-box provisioning is supported.
- Sequencing numbers in AToM packets are not processed by L2VPN Pseudowire Stitching. The feature passes the sequencing data through the cross-connect packet paths, a process that is called transparent sequencing. The end point PE to CE connections enforce the sequencing.
- You can ping the adjacent next-hop PE router. End-to-end LSP pings are not supported.

- Do not configure IP or Ethernet interworking on a router where L2VPN Pseudowire Stitching is enabled. Instead, configure interworking on the routers at the edge PEs of the network.
- The control word negotiation results must match. If either segment does not negotiate the control word, the control word is disabled for both segments.
- AToM Graceful Restart is negotiated independently on each pseudowire segment. If there is a transient loss of the LDP session between two AToM PE routers, packets continue to flow.
- Per-pseudowire QoS is not supported. The TE tunnel selection is supported.
- Attachment circuit interworking is not supported.

NTP-J34 Configure the Pseudowire Stitching Using Cisco IOS Commands

Purpose	This procedure configures L2VPN Pseudowire Stitching on each of the PE routers.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

This procedure assumes that you have configured the basic AToM L2VPNs.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**l2 vfi** *name* **point-to-point** **Example:** Router(config)# l2 vfi atomtunnel point-to-point	Creates a point-to-point Layer 2 VFI and enters VFI configuration mode.
Step 4	**neighbor** *ip-address vcid* [**encapsulation mpls** | **pw-class** *pw-class-name*]	Configures an emulated VC. • Specify the IP address and the VC ID of the remote router.

	Command or Action	Purpose
	Example: Router(config-vfi)# neighbor 10.0.0.1 100 pw-class mpls	• Specify the pseudowire class to use for the emulated VC. **Note** Only two **neighbor** commands are allowed for each **l2 vfi point-to-point** command.
Step 5	**exit** **Example:** Router(config-vfi)# exit	Exits VFI configuration mode.
Step 6	**exit** **Example:** Router(config)# exit	Exits global configuration mode.
Step 7	**show mpls l2transport vc** [**vcid** [*vc-id* | *vc-id-min vc-id-max*]] [**interface** *name* [*local-circuit-id*]] [**destination** *ip-address* | *name*] [**detail**] **Example:** Router# show mpls l2transport vc	Verifies that the L2VPN Pseudowire Stitching session has been established.
Step 8	**show vfi** [*vfi-name*] **Example:** Router# show vfi atomtunnel	Verifies that a point-to-point VFI has been established.
Step 9	**ping** [*protocol*] [**tag**] {*host-name* | *system-address*} **Example:** Router# ping 10.1.1.1	Verifies end-to-end connectivity when this command is issued from the CE routers.
Step 10	Return to your originating procedure (NTP).	—

Understanding BFD Control Channel over VCCV

MPLS pseudowires enable Layer 2 traffic to be carried over an IP/MPLS core network. The Bidirectional Forwarding Detection (BFD) control channel over Virtual Circuit Connection Verification (VCCV) feature provides OAM functions for MPLS pseudowires.

You can enable BFD control channel over VCCV feature using the NTP-J35 Configure BFD Control Channel over VCCV Using Cisco IOS Commands, on page 379 or DLP-J89 Create a Pseudowire Class Using CTC, on page 348.

Note This feature provides support only for VCCV type 1. VCCV type 1 is in-band VCCV and can be used only for MPLS pseudowires that use a control word.

The BFD protocol can be used to provide OAM functionality to the MPLS protocol. The VCCV provides a control channel associated with the pseudowire to provide OAM functions over that pseudowire. BFD can use the VCCV control channel as a pseudowire fault mechanism to detect data plane failures. BFD can also use the VCCV control channel to carry the fault status of an attachment circuit (AC).

MPLS pseudowires can dynamically signal or statically configure virtual circuit (VC) labels. In dynamically signaled pseudowires, the control channel (CC) types and connection verification (CV) types are also signaled. In statically configured pseudowires, the CC and CV types must be configured on both ends of the pseudowire.

The CC types define whether VCCV packets are in-band or out-of-band for the pseudowire. The CV types define whether BFD monitoring is required for the pseudowire. If BFD monitoring is required for the pseudowire, the CV types also define how the BFD packets are encapsulated and whether BFD provides status signaling functionality.

Any protocol that requires BFD monitoring must register with BFD as a client. For example, the the Xconnect protocol registers as a BFD client, and BFD assigns a client ID to Xconnect. The Xconnect uses this client ID to create the BFD sessions that monitor the pseudowire.

BFD can detect forwarding failures (end-to-end) in the pseudowire path. When BFD detects a failure in the pseudowire forwarding path, it notifies the Xconnect client that created the session. In addition, BFD can signal the status in any concatenated path or AC, to the remote device where the BFD session is terminated.

Restrictions of BFD Control Channel over VCCV

- The BFD Control Channel over VCCV feature supports only VCCV type 1 without IP/User Datagram Protocol (UDP) encapsulation.
- Any Transport over Multiprotocol Label Switching (AToM) is the only transport protocol supported by the BFD Control Channel over VCCV.
- Layer 2 Transport Protocol version 3 (L2TPv3) is not supported.
- Pseudowire redundancy is not supported.

NTP-J35 Configure BFD Control Channel over VCCV Using Cisco IOS Commands

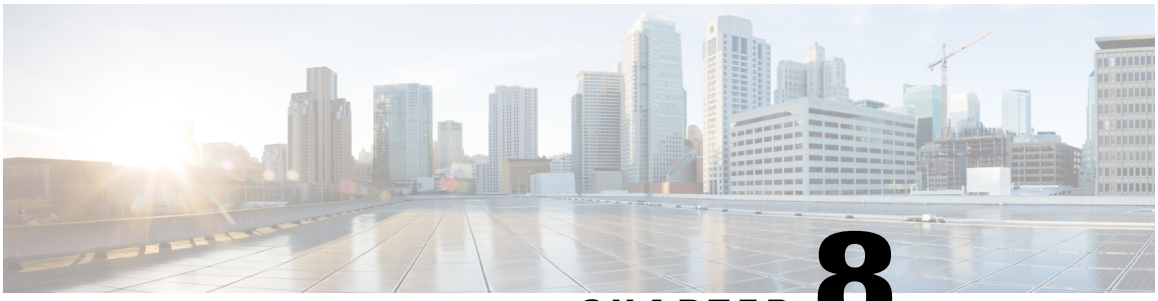
Purpose	This procedure configures VCCV BFD to run on pseudowires.
Tools/Equipment	None
Prerequisite Procedures	• DLP-J97 Create and Configure BFD Templates Using Cisco IOS Commands, on page 293 • DLP-J88 Create a Pseudowire Class Using Cisco IOS Commands, on page 346
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**pseudowire-class** *name* **Example:** Router(config)# pseudowire-class vccv-bfd1	Specifies the name of the pseudowire class and enters pseudowire class configuration mode.
Step 4	**encapsulation mpls** **Example:** Router(config-pw-class)# encapsulation mpls	Specifies that the MPLS is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire. You must specify MPLS encapsulation as part of the **xconnect** command or as part of a pseudowire class for the virtual circuits to work properly.
Step 5	**protocol** {**ldp** | **none**} **Example:** Router(config-pw-class)# protocol none	Specifies that no signaling is configured and that manually configured sessions are used. To configure static pseudowires, you must specify the **none** keyword.
Step 6	**vccv** {**control-word** | **router-alert** | **ttl**} **Example:** Router(config-pw-class)# vccv control-word	Sets the MPLS pseudowire control channel (CC) type. For MPLS pseudowires that use a connection verification (CV) type that does not include IP/UDP headers, you must set the CC type to CC type 1: pseudowire control word.
Step 7	**vccv bfd template** *name* **{udp** | **raw-bfd**} **Example:** Router(config-pw-class)# vccv bfd template bfdtemplate1 raw-bfd	Enables BFD over VCCV for the pseudowire class.
Step 8	**vccv bfd status signaling** **Example:**	Enables status signaling for BFD over VCCV.

	Command or Action	Purpose
	Router(config-pw-class)# vccv bfd status signaling	
Step 9	**exit** **Example:** Router(config-pw-class)# exit	Exits pseudowire class configuration mode and returns to global configuration mode.
Step 10	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 11	**service instance** *serviceinstanceid* **ethernet** **Example:** Router(config-if)# service instance 100 ethernet	Specifies the service instance and enters service instance configuration mode.
Step 12	**encapsulation dot1q** *vlan-id* **Example:** Router(config-if-srv)# encapsulation dot1q 100	Enables the Ethernet Flow Point (EFP) to accept 802.1Q VLAN packets.
Step 13	**xconnect** *peer-ip-address vc-id* {**encapsulation mpls** [**manual**] | **pw-class** *pw-class-name* } [**pw-class** *pw-class-name*] [**sequencing** {**transmit** | **receive** | **both**}] **Example:** Router(config-if-srv)# xconnect 10.0.0.7 100 pw-class vccv-bfd1	Binds an attachment circuit (AC) to a pseudowire, configures a static pseudowire, and specifies the pseudowire class.
Step 14	Return to your originating procedure (NTP). **Example:** —	



CHAPTER 8

Configuring Virtual Private LAN Services

This chapter describes Virtual Private LAN Services (VPLS). This chapter also describes procedures to configure VPLS.

Virtual Private LAN Services

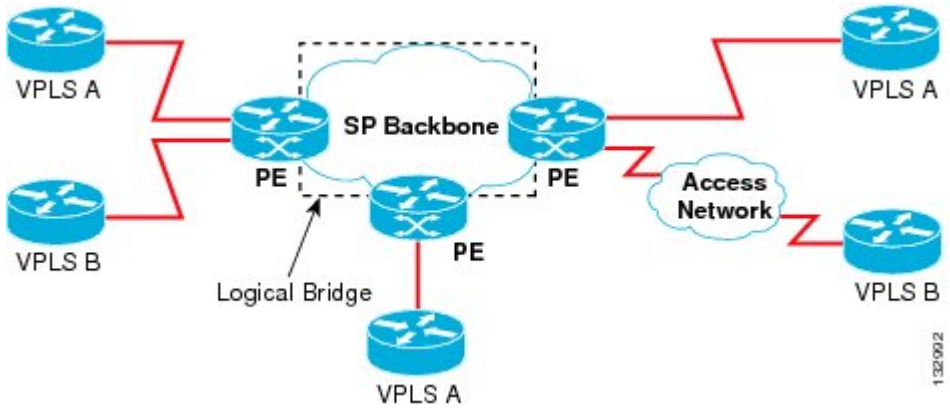
Virtual Private LAN Services (VPLS) is a multipoint Layer 2 VPN (L2VPN) technology that allows multiple sites to be connected over a simulated Ethernet broadcast domain, which is supported across a provider-provisioned IP/MPLS network. In other words, VPLS delivers multipoint Layer 2 connectivity over a Layer 3 network architecture. VPLS evolved as a logical extension of Ethernet over MPLS (EoMPLS), which was developed to enable point-to-point Ethernet-based L2VPN services.

At a basic level, VPLS can be defined as a group of Virtual Switch Instances (VSIs) that are interconnected using EoMPLS circuits to form a single, logical bridge. In concept, a VSI is similar to the bridging function found in IEEE 802.1q bridges where a frame is switched based on the destination MAC and membership in a Layer 2 VPN (a virtual LAN or VLAN). If the destination address is unknown, or is a broadcast or multicast address, the frame is flooded to all ports associated with the VSI, where a port, in the context of VPLS, is an EoMPLS virtual circuit (VC) pseudowire.

VPLS uses the provider core to join multiple attachment circuits together to simulate a virtual bridge that connects the multiple attachment circuits together. From a user-perspective, there is no topology for VPLS.

All of the customer edge (CE) devices appear to connect to a logical bridge emulated by the provider core. See the figure below:

Figure 61: Virtual Private LAN Services



With VPLS, all CE devices participating in a single VPLS instance appear to be on the same LAN; therefore, each CE device can communicate directly with one another in a multipoint topology, without requiring a full mesh of point-to-point circuits at the CE device. In a VPLS network, CE and provider edge (PE) devices are not routing peers, so there is no need for service providers to provision customer IP routers; this is a significant advantage over MPLS L3 VPN services. Compared to traditional LAN switching technologies, VPLS is also more flexible in its geographic scaling, so that CE sites may be within the same metropolitan domain, or may be geographically dispersed on a regional or national basis.

VPLS using Label Distribution Protocol (LDP) Signaling is supported. To enable VPLS over a network, a full-mesh or ring configuration with bridge-domains (pseudowires or Ethernet Flow Points (EFPs)) must be established using the Label Distribution Protocol (LDP). Dynamic pseudowires over LDP signalled, Static Pseudowire, Traffic Engineering (TE), or Transport Profile (TP) label switched path is supported in this release.

VPLS can be enabled on these configurations:

- Full-mesh
- Ring

Full-Mesh Configuration

The full-mesh configuration requires a full mesh of label-switched paths (LSPs) tunnels between all the PEs that participate in the VPLS. The tunnel label switched paths are required only for TE and TP configurations and not for LDP. With a full-mesh configuration, signaling overhead and packet replication requirements for each provisioned VC on a PE can be high.

To set up a VPLS, a virtual forwarding instance (VFI) must be created on each participating PE router. The VFI specifies the VPN ID of a VPLS domain, the addresses of other PE routers in the domain, and the type of tunnel signaling and encapsulation mechanism for each peer PE router.

The set of VFIs formed by the interconnection of the emulated VCs is called a *VPLS instance*; it is the VPLS instance that forms the logic bridge over a packet-switched network (PSN). The VPLS instance is assigned a unique VPN ID.

The PE routers use the VFI to establish a full-mesh LSP of emulated VCs to all the other PE routers in the VPLS instance. PE routers obtain the membership of a VPLS instance.

The full-mesh configuration allows the PE router to maintain a single broadcast domain. The CE devices view the VPLS instance as an emulated LAN.

To avoid the problem of a packet looping in the provider core, the PE devices enforce a *split-horizon* principle for the emulated VCs. That means if a packet is received on an emulated VC, it is not forwarded on any other emulated VC.

After the VFI has been defined, it needs to be bound to a bridge-domain to the CE device.

The packet forwarding decision is made by looking up the Layer 2 VFI of a particular VPLS domain.

A VPLS instance on a particular PE router receives Ethernet frames that enter on specific physical or logical ports and populates a MAC table similarly to how an Ethernet switch works. The PE router can use the MAC address to switch those frames into the appropriate LSP to be delivered to another PE router at a remote site.

If the MAC address is not in the MAC address table, the PE router replicates the Ethernet frame and floods it to all logical ports associated with that VPLS instance, except the ingress port where it just entered. The PE router updates the MAC table as it receives packets on specific ports and removes addresses that are not used for specific periods.

Ring Configuration

Ring configuration reduces both signaling and replication overhead, and also the bandwidth utilization for multicast traffic. Ring VPLS has an interconnection of PEs in a ring fashion. The main difference between ring and mesh VPLS is that in mesh VPLS, split horizon is enabled between the core PWs, and in a ring VPLS, split horizon is disabled. To prevent the consequential loop, at least one span in the ring is deprived of the PW configuration, that is, in a ring formed from X number of PEs, there will be (X-1) PWs with split horizon disabled.

Comparison of Mesh VPLS with Ring VPLS

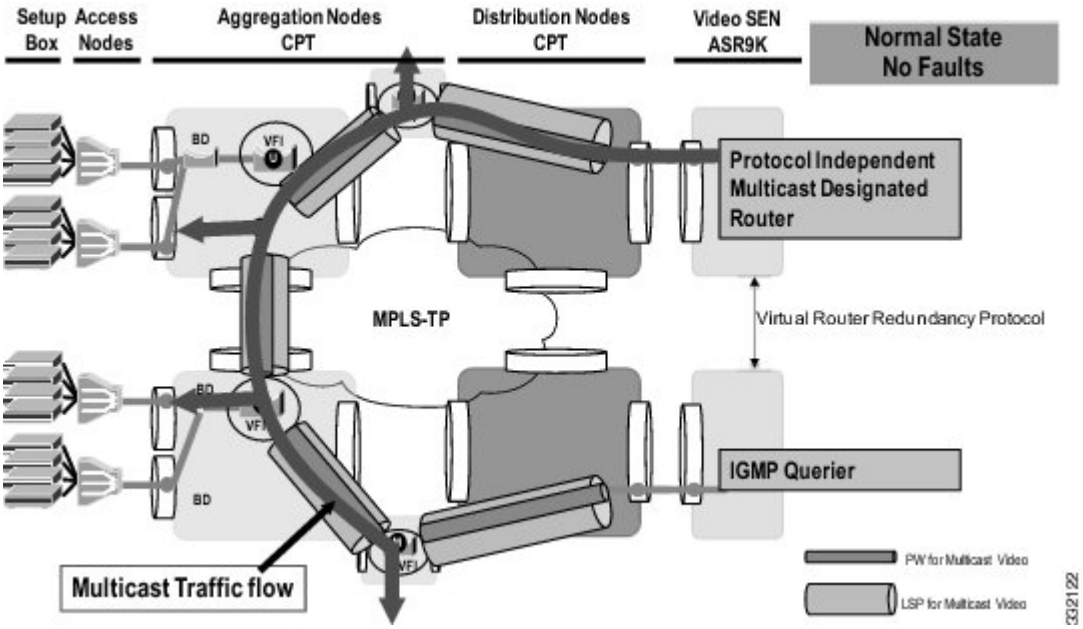
VPLS builds a full mesh of connections by default. In full mesh VPLS, multiple copies of customer traffic is present in the network path. In full mesh VPLS, if the number of multicast receiving node is N, there will be around N/2~1 copies of traffic along the network path.

In ring VPLS, a single copy of customer traffic traverses the network path. IGMP snooping feature replicates multicast steam to all destination sites which have joined the multicast group. Its forwarding mechanism is similar to Ethernet multicast forwarding mechanism. Ring topology is best suited for multicast application where the receivers are distributed across the PEs. Flooding of multicast traffic in the ring can be controlled by enabling IGMP snooping on the VPLS service.

Fault Handling in Ring VPLS

It is recommended to have protected TP tunnels between all PEs for robust network. In such a topology, a single link fault has no effect on the multicast entries and has a switch time of 50 milli-seconds. To counter multiple failures in the ring, redundancy at the router end is relied upon as shown in the below figure.

Figure 62: Efficient Video Distribution Logical Topology



The active or the standby state at the router is handled by the native multicast protocol and redundancy configurations at the router end.

Configuring VPLS

Provisioning a VPLS link involves provisioning the associated bridge-domain and the VFI on the PE. Before you configure VPLS, ensure that the network is configured as follows:

- (Only Dynamic MPLS) Configure IP routing in the core network so that the PE routers can reach each other through the IP.
- Configure MPLS in the core network so that a LSP exists between the PE routers.
- Configure a loopback interface for originating and terminating Layer 2 traffic. Make sure that the PE routers can access the loopback interface of other routers.

VPLS configuration requires you to identify peer PE routers and to attach Layer 2 circuits to the VPLS at each PE router.

Restrictions of VPLS

- The attachment circuit (AC)-less model is used to provision PWs. There is no AC-VFI binding in any of the VPLS deployment scenarios. AC is transparent to VFI and is handled completely by the bridge-domain.
- VC Type 5 (Ethernet) is supported and not VC Type 4 pseudowire for VPLS.

- Double tag encapsulation with rewrite POP 1 operation is not supported for VPLS EFP.

Supported Features on VPLS

- Multicast ring topology
- Internet Group Management Protocol (IGMP) Snooping
- MAC learning and flushing
- Port-based Quality of Service (QoS) for MPLS core port
- Service-based QoS for VPLS EFP
- Split-horizon and shut or no shut operations on VPLS EFP

Interaction of VPLS with other Features

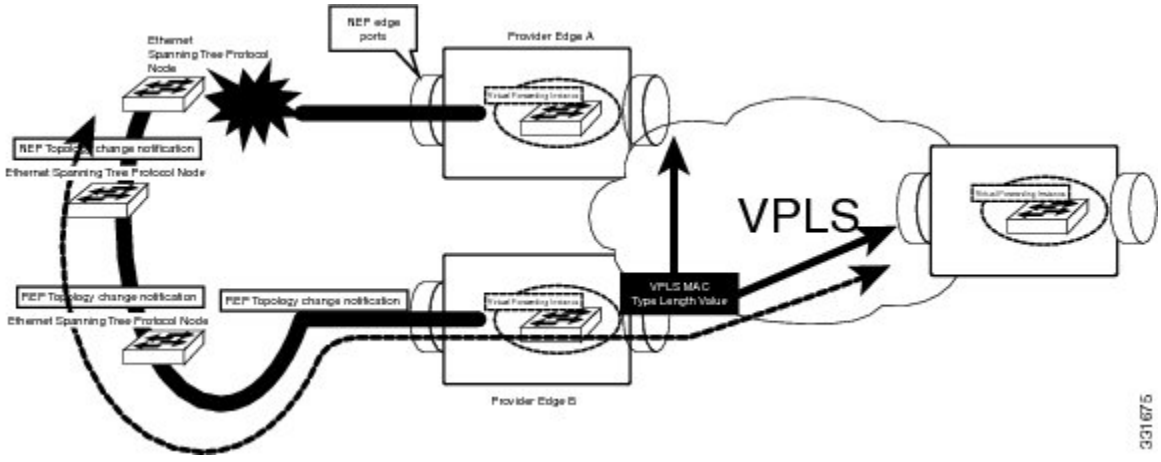
The VPLS feature supports QoS, In-Service Software Upgrade (ISSU), High Availability (HA), and active-active forwarding. Active-Active forwarding is supported by VPLS only when graceful-restart is enabled.

The VPLS feature provides multicast support that is required for efficient video traffic distribution. This is achieved by enabling IGMP snooping on the VPLS bridge-domain. The IGMP snooping for VPLS, provides the ability to send Layer 2 multicast frames from the CE in a VPLS VFI only to those remote peer CEs that have sent an IGMP request to join the multicast group. IGMP on VPLS does not support static multicast routers.

The VPLS feature supports MAC learning and MAC flush on the VPLS bridge-domain and MAC withdrawal, based on the LDP update. VPLS-capable systems must dynamically learn MAC addresses on the EFPs and PWs and must be able to forward and replicate packets across both EFPs and PWs. MAC entries are learnt per VFI.

The VPLS feature supports Link Aggregation (LAG) on the EFP side and not the PW side.

On the EFP side, if Resilient Ethernet Protocol (REP) is enabled, the VPLS feature supports MAC flush and withdrawal when REP switchover is triggered. MAC flush is triggered when access PW switchover occurs and when the VPLS EFP comes up per bridge-domain. When the core PW goes down, the MAC flush occurs per PW. The following figure explains the REP and VPLS interaction:



When there is a link failure, the REP ports are unblocked and the REP ring is restored in less than a second. REP access failure is propagated through REP Topology Change Notification (TCN) across the ring. REP TCN triggers MAC withdrawal and the traffic can be quickly restored over the VPLS domain

Supported Encapsulation and Rewrite Operations

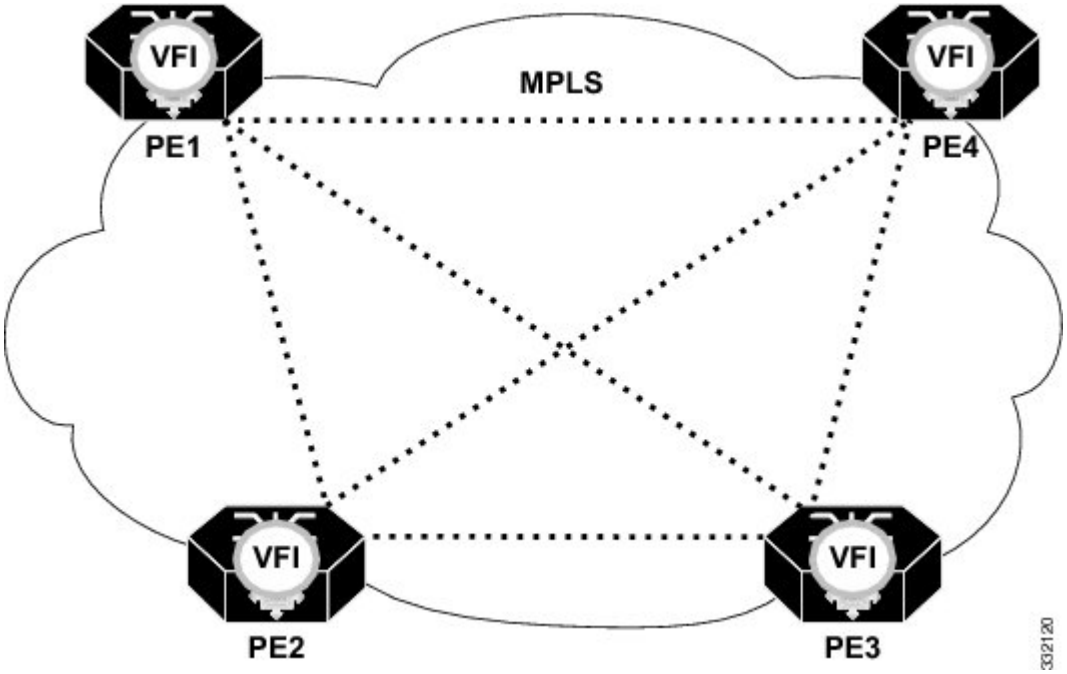
The supported encapsulation and rewrite operations for VPLS are listed in Table 10: Supported Encapsulation and Rewrite Operations for P2MP EVC , on page 162.

This section contains examples that show how to configure VPLS using Cisco IOS commands.

Example: Mesh Topology

The example in this section explains how to configure VPLS in case of a mesh topology that is shown in the below figure:

Figure 63: Mesh Topology



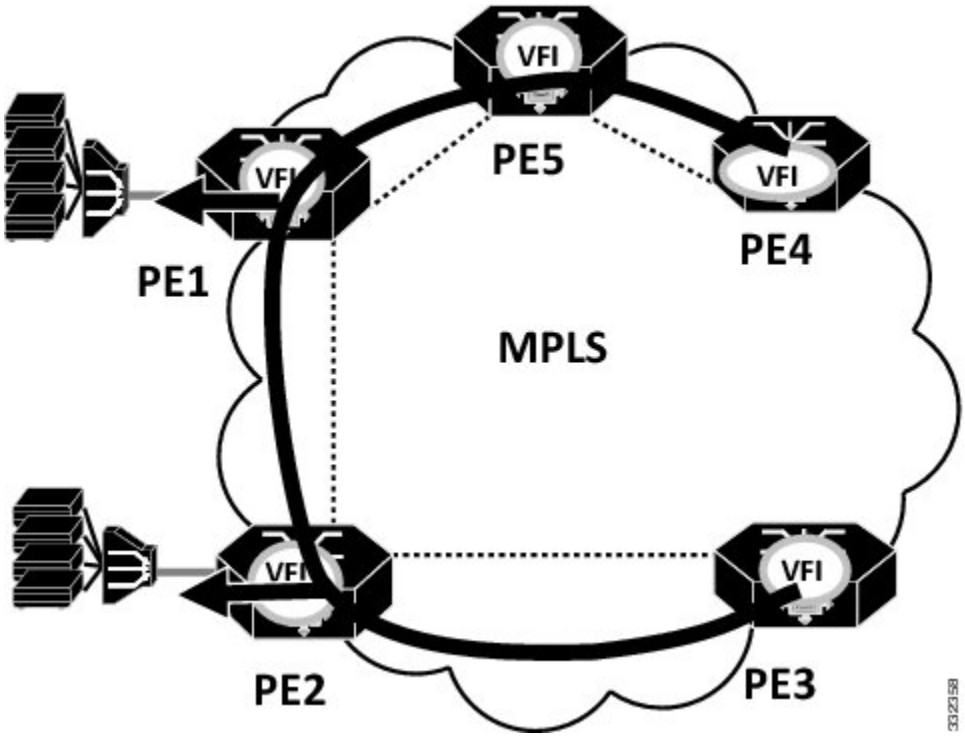

```
! Configuration on PE1
bridge-domain 100
mode vpls

l2 vfi vpls-100 manual
vpn id 100
bridge-domain 100
neighbor 2.2.2.2 encapsulation mpls
neighbor 3.3.3.3 encapsulation mpls
neighbor 4.4.4.4 encapsulation mpls

! Configuration on PE2
bridge-domain 100
mode vpls

l2 vfi vpls-100 manual
vpn id 100
bridge-domain 100
```

```
neighbor 1.1.1.1 encapsulation mpls
neighbor 3.3.3.3 encapsulation mpls
neighbor 4.4.4.4 encapsulation mpls

! Configuration on PE3
bridge-domain 100
mode vpls

l2 vfi vpls-100 manual
vpn id 100
bridge-domain 100
neighbor 1.1.1.1 encapsulation mpls
neighbor 2.2.2.2 encapsulation mpls
neighbor 4.4.4.4 encapsulation mpls

! Configuration on PE4
bridge-domain 100
mode vpls

l2 vfi vpls-100 manual
vpn id 100
bridge-domain 100
neighbor 1.1.1.1 encapsulation mpls
neighbor 2.2.2.2 encapsulation mpls
neighbor 3.3.3.3 encapsulation mpls
```

Example: Ring Topology

The example in this section explains how to configure VPLS in case of a ring topology that is shown in the below figure:

Figure 64: Ring Topology



Note Split-horizon is disabled on PE1 and PE2 to allow packet to go from one VPLS PW to another VPLS PW

```
! Configuration on PE1
bridge-domain 100
mode vpls

l2 vfi vpls-100 manual
vpn id 100
bridge-domain 100
neighbor 2.2.2.2 encapsulation mpls no-split-horizon
neighbor 4.4.4.4 encapsulation mpls no-split-horizon

Interface 36/11
Service instance 10 ethernet
Encap dot1q 10
Bridge-domain 100

! Configuration on PE2
bridge-domain 100
mode vpls

l2 vfi vpls-100 manual
vpn id 100
bridge-domain 100
neighbor 1.1.1.1 encapsulation mpls no-split-horizon
neighbor 3.3.3.3 encapsulation mpls no-split-horizon

Interface 36/12
Service instance 10 ethernet
Encap dot1q 10
Bridge-domain 100


! Configuration on PE3
bridge-domain 100
mode vpls

l2 vfi vpls-100 manual
vpn id 100
bridge-domain 100
neighbor 2.2.2.2 encapsulation mpls

Interface 4/2
Service instance 10 ethernet
Encap dot1q 10
Bridge-domain 100

! Configuration on PE4
bridge-domain 100
mode vpls

l2 vfi vpls-100 manual
vpn id 100
bridge-domain 100
neighbor 1.1.1.1 encapsulation mpls

Interface 4/2
Service instance 10 ethernet
Encap dot1q 10
Bridge-domain 100
```

Example: IGMP Snooping

The following example shows how to enable IGMP snooping on the VPLS bridge-domain and how to configure the source and host ports:

```
! Configuration on the bridge-domain
Router(config)# bridge-domain 200
Router(config-bdomain)# mode vpls
Router(config-bdomain)# ip igmp snooping

! Configuration on port 1
Router(config)# interface gi 36/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation untagged
Router(config-if-srv)# bridge-domain 30

! Configuration on port 2
Router(config)# interface gi 36/2
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 200
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 30

! Configuration on port 3
Router(config)# interface gi 36/6
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 101 second-dot1q 20
Router(config-if-srv)# rewrite ingress tag pop 2 symmetric
Router(config-if-srv)# bridge-domain 30
```

The following example shows how to enable IGMP immediate leave on the VPLS bridge-domain:

```
Router(config)# bridge-domain 200
Router(config-bdomain)# mode vpls
Router(config-bdomain)# ip igmp snooping immediate-leave
```

The following example shows how to disable IGMP report suppression on the VPLS bridge-domain:

```
Router(config)# bridge-domain 200
Router(config-bdomain)# mode vpls
Router(config-bdomain)# no ip igmp snooping report-suppression
```

NTP-J107 Configure a VPLS Circuit Using CTC

Purpose	This procedure configures a VPLS circuit using CTC.
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 DLP-J335 Create a VPLS Circuit Using CTC, on page 392.

Step 2 Create an access pseudowire on the node (user provider edge (U-PE)) that must be added to the existing VPLS circuit. The access pseudowire must be created from U-PE to an unmanaged node only. To create an access pseudowire, see DLP-J91 Create a Pseudowire Using CTC, on page 359.

Step 3 Complete DLP-J336 Edit a VPLS Circuit Using CTC, on page 394.

DLP-J335 Create a VPLS Circuit Using CTC

Purpose	This procedure creates a VPLS circuit using CTC.
Tools/Equipment	None
Prerequisite Procedures	• Create loopback addresses on the nodes. • Enable Open Shortest Path First (OSPF) (for a TP tunnel, enable OSPF on loopback interface). • Enable OSPF on the physical interface (for a TP tunnel without IP, enabling OSPF is not required). • Establish LDP, TE, or TP connectivity between the nodes. • Enable OSPF on the TP or TE interface or create a static route for the destination IP using tunnel interface. • DLP-J89 Create a Pseudowire Class Using CTC, on page 348.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to create a VPLS circuit.

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

Step 3 Click the **Layer2+** tab.

Step 4 From the left pane, click **Circuits**.

Step 5 Click the **VPLS** tab.

Step 6 Click **Create**. The Circuit Creation wizard appears.

Step 7 In the Global Attributes area of the Circuit Attributes screen, specify the global attributes:

a) Enter the name of the VPLS circuit that you want to create.
b) Enter the description of the VPLS circuit.
c) Enter the VPN ID.
d) From the Admin State drop–down list, choose **UP** or **DOWN** . The default value is UP.
e) Specify the bandwidth of the VPLS circuit in Kbps, Mbps, or Gbps.
f) In the VPLS Type area of the Circuit Attributes screen, choose any one of the following VPLS types:

- Open Ring
- Mesh

Step 8 Click **Next**. The VPLS Configuration screen is displayed.

Step 9 Click **Select Nodes for the VPLS Network**. The Select Nodes for the VPLS Network screen is displayed.

Step 10 To select the nodes for the VPLS network:

a) Select a node from the network map and click **Add**. The Add node dialog box appears.
b) Check the **Unmanaged Node** check box when the node is not a node. If this check box is checked, enter the IP address of the unmanaged node.
c) From the list of nodes, choose nodes and click **Apply**.
d) Click **Apply**. The nodes are added to the VPLS network and are displayed in the VPLS Configuration screen.

Step 11 In the VPLS Configuration screen, choose the pseudowire class from the PW Class A and PW Class Z drop-down lists.
The available attributes are:

- Span—(Display only) Indicates the circuit span information.
- VC ID A—(Display only) Indicates the VC ID of the first node in the span.
- VC ID Z—(Display only) Indicates the VC ID of the second node in the span.
- Split Horizon A—(Display only) Indicates the split horizon status (enabled or disabled) of the first node in the span.
- Split Horizon Z—(Display only) Indicates the split horizon status (enabled or disabled) of the second node in the span.
- Manual Route—Adds an intermediate node between the first and the second nodes in the span.

- S-PE Right—(Display only) Indicates that the intermediate service provider edge (S-PE) node is present on the right side of the first node in the span.
- S-PE Left—(Display only) Indicates that the intermediate S-PE node is present on the left side of the second node in the span.

Step 12 Click **Finish**.

Step 13 Return to your originating procedure (NTP).

DLP-J336 Edit a VPLS Circuit Using CTC

Purpose	This procedure edits a VPLS circuit using CTC: • Create new endpoint PWs for the VPLS circuit • Create new endpoint EFPs for the VPLS circuit • Specify the QoS policies to apply on individual EFPs • Specify the IGMP snooping settings for the bridge-domain • Specify the MAC learning settings for the bridge-domain
Tools/Equipment	None
Prerequisite Procedures	DLP-J335 Create a VPLS Circuit Using CTC, on page 392
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to edit a VPLS circuit.

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

Step 3 Click the **Layer2+** tab.

Step 4 Click **VPLS**.

Step 5 From the list of VPLS circuits, select a VPLS circuit to edit.

Step 6 Click **Edit**. The Edit Circuit dialog box appears.

Step 7 In the General tab, view the name, description, service ID, and MTU of the VPLS circuit.

Step 8 In the Endpoint PWs tab, view the node list that are part of the selected VPLS circuit. Select the node in the VPLS Node List area to view the details of its neighbor node in the Neighbors area.
You can create new endpoints only for Ethernet Private LAN and Ethernet Virtual Private LAN.

To create new endpoint PWs for this VPLS circuit:

a) Click **Create**. The Define New Drop wizard appears.
b) In the New Drop screen of the wizard, choose a VPLS type.
c) Click **Next**. The VPLS Configuration screen is displayed.
d) Click **Select Nodes for the VPLS Network**. The Select Nodes for the VPLS Network screen is displayed.
e) To select the nodes for the VPLS network:

1. Select a node from the network map and click **Add**. The Add node dialog box appears.
2. Check the **Unmanaged Node** check box when the node is not a node. If this check box is checked, enter the IP address of the unmanaged node.
3. From the Node drop-down list, choose a node and click **Apply**.
4. Repeat Step 8ei to Step 8eiii to add the remaining nodes.
5. Click **Apply**. The nodes are added to the VPLS network and are displayed in the VPLS Configuration screen.

f) In the VPLS Configuration screen, choose the pseudowire class from the PW Class A and PW Class Z drop-down lists.
The available attributes are:

- Span—(Display only) Indicates the circuit span information.
- VC ID A—(Display only) Indicates the VC ID of the first node in the span.
- VC ID Z—(Display only) Indicates the VC ID of the second node in the span.
- Split Horizon A—(Display only) Indicates the split horizon status (enabled or disabled) of the first node in the span.
- Split Horizon Z—(Display only) Indicates the split horizon status (enabled or disabled) of the second node in the span.
- Manual Route—Adds an intermediate node between the first and the second nodes in the span.
- S-PE Right—(Display only) Indicates that the intermediate S-PE node is present on the right side of the first node in the span.

- S-PE Left—(Display only) Indicates that the intermediate S-PE node is present on the left side of the second node in the span.

g) Click **Finish**.
To delete an endpoint PW, select the node in the VPLS Node List area and click **Delete Node**.

Step 9 In the S-PE Nodes tab, view the node list that is part of the selected VPLS circuit. Select the node in the VPLS Node List area to view the details of its neighbor node in the Neighbors area. You can delete the neighbor and node by selecting them and clicking the **Delete Neighbor** or the **Delete Node** button.

Step 10 In the Endpoint EFPs tab, view the EFPs that are part of the selected VPLS. You can create new endpoints only for Ethernet Private LAN and Ethernet Virtual Private LAN. To create a new endpoint EFP for this VPLS:

a) Click **Create**. The Define New Drop wizard appears.
b) In the New Drop screen of the wizard, choose a node from the Node drop-down list.
c) To choose a port to serve as the EFP:

1. From the Fabric/Line/Satellite Slot drop-down list, choose a slot.
2. From the Port drop-down list, choose a port to serve as the EFP.

d) To choose a channel group to serve as the EFP:

1. Check the **CHGRP as EFP** check box.
2. From the CHGRP drop-down list, choose a channel group to serve as the EFP.
3. Click **Manual Load Balancing** to configure manual load balancing on the ports of the channel group. The Manual Load Balancing dialog box appears.

e) Click **Next**. In the EFP Configuration Preview screen of the wizard, CTC displays the VPLS path.
f) Select the Node from the network map. The EFP Selection area displays the node selected.
g) From the Available Ports drop-down list, choose the ports.
h) In the EFP Configuration tab, specify the VLAN configuration for this EFP.
i) Click **Finish** to create a new EFP for this VPLS.

Note After you have completed the DLP-J335 Create a VPLS Circuit Using CTC, on page 392 procedure, you can create new endpoints EFPs/PWs or add existing EFPs/PWs to this VPLS circuit. CTC allows you to add only until 127 entries; EFPs or neighbor nodes. This number includes the total number of entries made in both, Endpoint PWs tab and Endpoint EFP tab. CTC blocks any attempts to add more than 127 entries to this VPLS circuit.

Step 11 In the EFP Configuration tab, view the configurations of the EFP. Also, specify the VLAN configuration for the selected EFP.

a) From the EFP drop-down list, choose an EFP to view its configuration.
b) From the EFP State drop-down list, choose UP or Down to change the up or down status of EFP.
c) In the Outer VLAN Configuration area, choose the type of VLAN tagging:

- Double Tagged
- Single Tagged
- Untagged
- Default

- Any

Note The VLAN tagging type chosen for Ethernet Private Line and Ethernet Private LAN is Default. Do not change this option for the source EFP.

d) Enter a VLAN tag in the VLAN Tag field. For example, enter 10,20,30-50 without white spaces in the VLAN Tag field.
e) In the Inner VLAN Configuration area, enter the VLAN tag. You cannot enter VLAN range for inner VLANs. The inner VLAN TPID cannot be changed.
f) In the Rewrite Ingress Operation area, choose the rewrite operation:

- PUSH 1
- PUSH 2
- POP 1
- POP 2
- TRANSLATE 1-to-1
- TRANSLATE 1-to-2
- TRANSLATE 2-to-1
- TRANSLATE 2-to-2

g) Enter the outer VLAN tag in the Outer VLAN Tag field. The Outer VLAN TPID cannot be changed.
h) Enter the inner VLAN tag in the Inner VLAN Tag field. The Inner VLAN TPID is dot1q and cannot be changed.
i) Click **Apply** to apply this configuration to the selected EFP
You Cannot edit the VLAN configurations of the EFP for VPLS if the following services are present.

- QOS
- Span
- IGMP
- MVR

Step 12 In the QoS tab, specify the QoS policies to apply on the individual EFPs:
a) From the Ingress Policy drop-down list, choose the required policy.
b) From the Egress Policy drop-down list, choose the required policy.
c) Click **Apply**.

Step 13 (Only for Ethernet Virtual Private LAN type) In the IGMP Snooping tab, specify the settings for the bridge domain:
a) Check the **IGMP Snooping** check box to enable IGMP snooping on this bridge domain.
b) Check the **Immediate Leave** check box to enable IGMP snooping to immediately remove a port when it detects an IGMP version 2 leave a message on that port.
c) Check the **Report Suppression** check box to ensure that the bridge domain forwards only one IGMP report for each multicast query.

d) Click **Apply**.

Step 14 (Only for Ethernet Private LAN and Ethernet Virtual Private LAN types) In the MAC Learning tab, specify the MAC learning settings for the bridge domain:

a) Check the **MAC Learning** check box to enable MAC learning on this bridge domain. MAC learning is enabled by default for Ethernet Private LAN and Ethernet Virtual Private LAN.

b) Enter the upper limit on the number of MAC addresses that reside in a bridge domain. The maximum MAC address limit on a bridge domain is 128000.

c) Click **Apply**.

d) Click **Static MAC Address Configuration**. The EFP Static MAC Address Configuration dialog box appears. Enter the static MAC addresses for each EFP or PW.

e) Select the **EFP** or the **PW** radio button and from the drop-down list, choose an EFP or the PW.

f) Enter one or more static MAC addresses for the EFP or the PW in the MAC Address field and click **Add**. The added MAC addresses appear in the Entered MAC Addresses area.

g) Click **Apply** and close the EFP Static MAC Address Configuration dialog box.

h) Click **Clear MAC Address(es)**. The Clear MAC Addresses dialog box appears. Select the specific MAC address to remove from the MAC address table.

i) Select the **System**, **EFP** or the **PW** radio button and from the drop-down list, choose the system, EFP or the PW where you want to clear the MAC address.

j) Enter the MAC address in the MAC Address field and click **Add**.

k) Click **Clear** to clear all the MAC addresses in the MAC Addresses to clear area.

l) Click **Clear All** to clear all the MAC addresses learned on the system, EFP, or PW.

m) Close the Clear MAC Addresses dialog box.

n) Click **Display MAC Address(es)** to display the configured static MAC addresses for each EFP or the PW. The Configured EFP Static MAC Addresses dialog box appears.

o) Select the **EFP** or the **PW** radio button and from the drop-down list, choose an EFP or the PW. The MAC addresses configured on the EFP or the PW appear in the Configured MAC Addresses area.

p) Close the Configured EFP Static MAC Addresses dialog box.

Step 15 In the State tab, edit the state of the VPLS circuit:

a) From the Target VPLS Admin state drop-down menu, select **UP** or **DOWN**.

b) Click **Apply**.

Step 16 Return to your originating procedure (NTP).

NTP-J108 Configure a VPLS Circuit Using Cisco IOS Commands

Purpose	This procedure configures a VPLS circuit using Cisco IOS commands.
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 DLP-J216 Configure a Bridge Domain Using Cisco IOS Commands, on page 140.

Step 2 (Optional) Complete DLP-J1 Configure an Ethernet Service Instance Using Cisco IOS Commands, on page 141 when the CE is connected to the PE using Ethernet services.

Step 3 Complete any one of the following procedures as applicable:

- DLP-J119 Enable MPLS LDP-IGP Synchronization Using Cisco IOS Commands, on page 196.
- NTP-J48 Configure MPLS-TE Parameters, on page 220.
- NTP-J41 Configure an MPLS-TP Tunnel, on page 309.

Step 4 Complete DLP-J337 Create a Layer 2 Virtual Forwarding Instance Using Cisco IOS Commands, on page 399.

Step 5 Complete DLP-J90 Create a Pseudowire Using Cisco IOS Commands, on page 351 when the PE (U-PE) is connected to another PE using MPLS services.

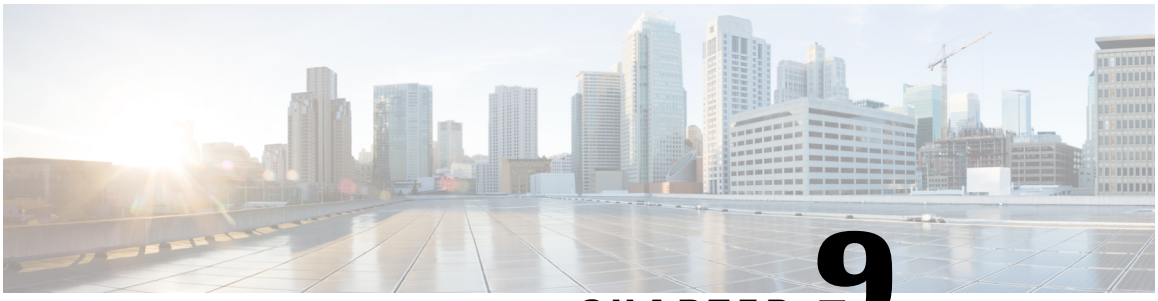
DLP-J337 Create a Layer 2 Virtual Forwarding Instance Using Cisco IOS Commands

Purpose	This procedure creates a layer 2 virtual forwarding instance (VFI) using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J216 Configure a Bridge Domain Using Cisco IOS Commands, on page 140 (with VPLS mode)
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Router> enable	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**l2 vfi** *name* **manual** **Example:** Router(config)# l2 vfi VPLSA manual	Creates a named Layer 2 Virtual Forwarding Instance (VFI) and enters the L2 VFI manual configuration mode.
Step 4	**vpn id** *vpnid* **Example:** Router(config-vfi)# vpn id 100	Configures a VPN ID for the VPLS domain.
Step 5	**bridge-domain** *bridge-id* **Example:** Router(config-vfi)# Bridge-domain 22	Specifies the bridge-domain number.
Step 6	**neighbor** *ip-address id* **{encapsulation mpls | pw-class** *pw-class-name***} [no-split-horizon]** **Example:** Router(config-vfi)# neighbor 33.33.33.33 6 encapsulation mpls	Specifies the remote peer router ID and the IP address of the router, and the tunnel encapsulation type (always set to mpls), or the pseudowire property.
Step 7	**exit** **Example:** Router(config-vfi)# exit	Exits the L2 VFI manual configuration mode.



CHAPTER 9

Configuring Quality of Service

This chapter describes the Quality of Service and procedures to configure Quality of Service.

Introduction to Quality of Service

The Cisco Carrier Packet Transport (CPT) system is a Carrier Ethernet based crossponder solution used as an access or an aggregation device. To maximize the utility of network bandwidth, service providers can aggregate different types of traffic (voice, video, broadband data, and so on) and transmit them over the network. Because a single device supports a wide range of traffic (voice, video, broadband data, and so on), it is important to distinguish traffic from one another and provide differential services.

Quality of Service (QoS) refers to the ability of a network to provide improved services to selected network traffic over various underlying technologies including Ethernet and IEEE 802.1 networks, and MPLS networks.

The Cisco CPT system can be configured to provide different levels of treatment to different services. The different levels are defined through the service elements of bandwidth, including loss and delay. A service-level agreement (SLA) is a guaranteed level of these service elements. The CPT system supports flat and hierarchical QoS up to three levels.

You configure QoS throughout a network to provide an end-to-end QoS delivery. The following two components are necessary to deliver QoS across a heterogeneous network:

- QoS within a single network element, which includes queuing, scheduling, and traffic shaping features.
- QoS policing and management functions to control and administer end-to-end traffic across a network.

Advantages of QoS

Enabling QoS in the network has the following advantages:

- Control over resources—You can control resources like bandwidth that is being used.
- Tailored services—If you are a service provider, the control and visibility that QoS provides enable you to offer carefully tailored grades of service differentiation to your customers.
- Coexistence of mission-critical applications:
  - Your WAN is used efficiently by mission-critical applications that are most important to your business.
  - Bandwidth and minimum delays required by time-sensitive multimedia and voice applications are available.
  - Other applications using the link get their fair service without interfering with mission-critical traffic.

Understanding QoS

The QoS mechanism has three basic steps. It classifies types of traffic, specifies what action to take against a type of traffic, and specifies where the action should take place. The following sections explain how the CPT system accomplishes these steps.

Classification Mechanism for IP, Ethernet, and MPLS

For any QoS service to be applied to data, there must be a way to classify an IP packet or an Ethernet frame. When identified, a specific priority can be assigned to each individual IP packet or Ethernet frame. The IP Precedence field or the IP Differentiated Services Code Point (DSCP) field can be used to classify IP packets, and the Ethernet class of service (IEEE 802.1p defined class of service [CoS]) can be used for classifying Ethernet frames. IP precedence, IP DSCP, Ethernet CoS, and MPLS EXP are further described in the following sections.

IP Precedence

Use of IP precedence enables you to specify the class of service (CoS) for a packet using the three precedence bits in the type of service (ToS) field of the IP version 4 (IPv4) header. By default, each precedence corresponds to a name. These names, which continue to evolve, are defined in RFC 791.

Number	Name
0	routine
1	priority

Number	Name
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	networks

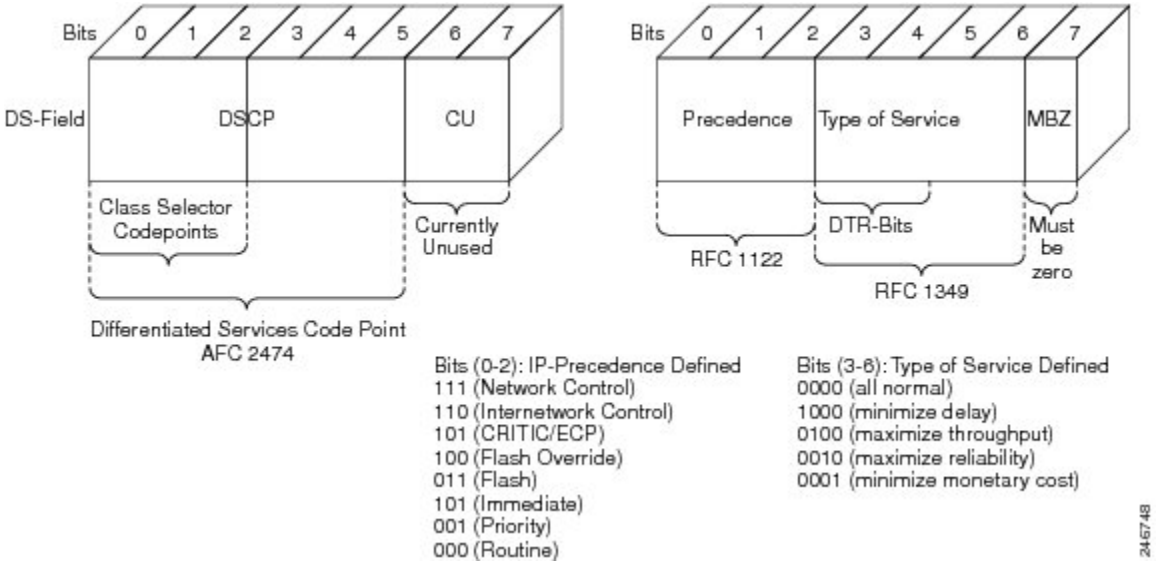
Note IP precedence bit settings 6 and 7 are reserved for network control information, such as routing updates.

IP Differentiated Services Code Point

IP DSCP uses the six bits in the IPv4 header to specify class of service for each IP packet (IETF RFC 2474). The DSCP field classifies packets into any of the 64 possible classes. On the network edge, the IP DSCP is assigned by the client device or the router, so that each subsequent network element can provide services based on the determined policy or the SLA.

IP Precedence and DSCP is illustrated in this figure.

Figure 65: IP Precedence and DSCP

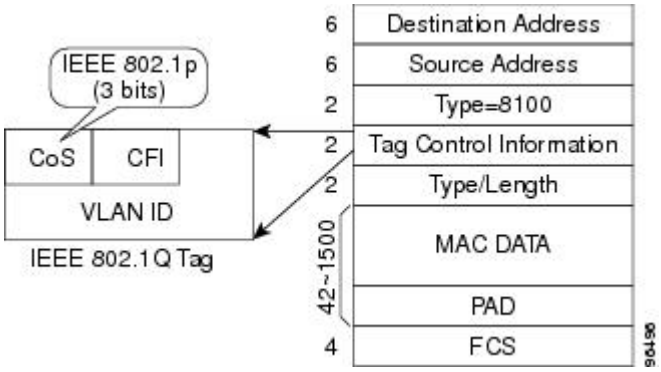


Ethernet CoS

The Ethernet CoS refers to the three bits within a four byte IEEE 802.1Q (VLAN) header used to indicate the priority of the Ethernet frame as it passes through a switched network. The CoS bits in the IEEE 802.1Q header are commonly referred to as the IEEE 802.1p bits. There are three CoS bits that provide eight classes,

matching the IP precedence number. In many real-world networks, a packet might traverse both Layer 2 and Layer 3 domains. To maintain QoS across the network, the IP ToS can be mapped to the Ethernet CoS and vice versa. For example, in a linear or one-to-one mapping where each mechanism supports eight classes. Similarly, a set of DSCP values (64 classes) can be mapped into each of the eight individual Ethernet CoS values. An IEEE 802.1Q Ethernet frame, which consists of a 2-byte Ethertype and a 2-byte tag (IEEE 802.1Q tag) on the Ethernet protocol header is shown in this figure.

Figure 66: Ethernet Frame and the CoS Bit (IEEE 802.1p)



Multiprotocol Label Switching Experimental

The Multiprotocol Label Switching (MPLS) Experimental (EXP) is a 3-bit field and part of the Multiprotocol Label Switching (MPLS) header. It was created by the IETF on an experimental basis, but later became part of the standard MPLS header. The EXP bits in the MPLS header carry the packet priority. Each label switch router (LSR) along the path honors the packet priority by queuing the packet into the proper queue and servicing the packet accordingly.

CPT System QoS

The CPT system QoS classifies each packet in the network based on its Ethernet CoS, IP precedence, IP DSCP, MPLS EXP bits. After they are classified into class flows, further QoS functions can be applied to each packet as it traverses the CPT system.

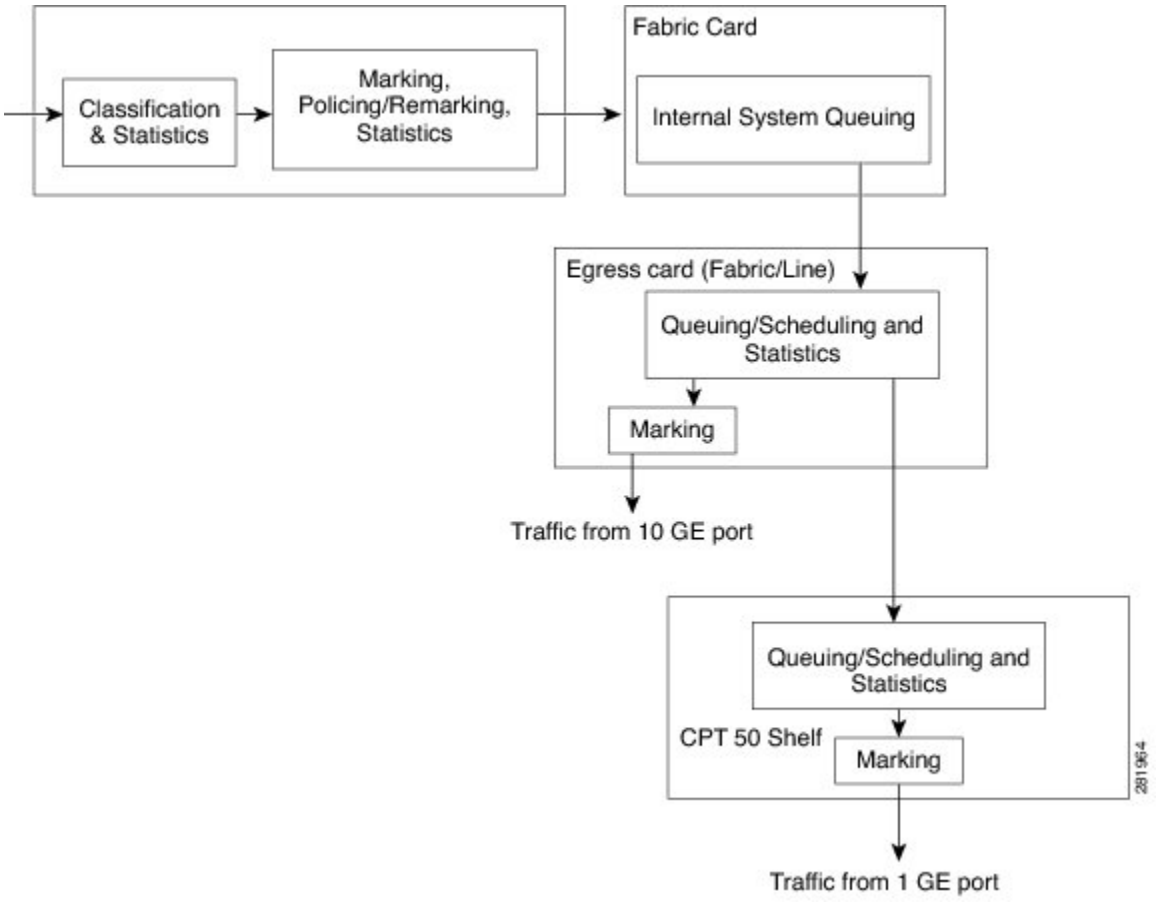
The policing feature of the CPT system ensures that the attached equipment does not submit more than a predefined amount of bandwidth (Rate Limiting) into the network. The policing feature can be used to enforce the committed information rate (CIR) and the peak information rate (PIR) available to a customer at an interface. The policing action is applied per classification.

The marking feature can set the Ethernet CoS, IP precedence, or IP DSCP bits when packets enter the CPT system. For MPLS traffic, marking sets the MPLS EXP bits when the packets leave the system. The marking feature operates on the outer IEEE 802.1p tag, IP precedence, or IP DSCP bits and provides a mechanism for tagging packets at the ingress; and on the MPLS EXP bits at the egress by using table-maps. The subsequent network elements can provide a QoS based only the QoS indicator that the service provider has created.

The per-class queuing allows various queuing applications to support SLA. For example, allocation of committed information rate, ensuring low latencies and rate limiting traffic to down stream nodes based on the configuration, and also enabling fair access to excess network bandwidth. The CPT system uses a combination of Strict Priority Queuing (SPQ) and Weighted Round Robin (WRR) scheduling process to

guarantee throughput and latency requirements and to provide fair access to excess bandwidth. The CPT system QoS flow is illustrated in this figure.

Figure 67: CPT System QoS flow



NTP-J62 Configuring QoS Features Using Cisco IOS Commands

Purpose	This procedure configures QoS features using IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or Remote
Security Level	None

Note Users can create traffic policies and attach these policies to targets. A traffic policy contains a traffic class and one or more QoS features. A traffic class is used to classify traffic, while the QoS features in the traffic policy determine how to treat the classified traffic.

Procedure

Step 1 Define a traffic class using the **class-map** command:

a) To configure traffic classification at the ingress, see DLP-J190 Configuring Ingress Classification Using Cisco IOS Commands, on page 408.

b) To configure traffic classification at the egress, see DLP-J199 Configuring Egress Classification Using Cisco IOS Commands, on page 433.

Step 2 Create a traffic policy using the **policy-map** command to associate the traffic class with one or more QoS features (using the **policy-map** command):

a) To configure policing at the ingress, see DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 414.

b) To configure marking at the ingress, see DLP-J197 Configuring Ingress Marking Using Cisco IOS Commands, on page 429.

c) To configure marking at the egress using table maps, see DLP-J207 Configuring Table Maps for Egress Marking Using Cisco IOS Commands, on page 436.

d) To associate table maps at the egress using table maps, see DLP-J200 Associating Table Maps at Egress Using Cisco IOS Commands, on page 439.

e) To configure shaping at the egress, see DLP-J203 Configuring Egress Shaping Using Cisco IOS Commands, on page 447.

f) To configure the egress bandwidth, see DLP-J202 Configuring Egress Bandwidth Using Cisco IOS Commands, on page 445.

g) To configure low-latency queuing (LLQ), see DLP-J201 Configuring Egress LLQ Using Cisco IOS Commands, on page 442.

h) To configure bandwidth remaining ratio (BRR) or bandwidth remaining percent (BRP), see DLP-J204 Configuring Egress Bandwidth Remaining Ratio or Bandwidth Remaining Percent Using Cisco IOS Commands, on page 450.

Note Bandwidth Remaining Ratio of class default is 1 if not explicitly configured.

Step 3 Attach the traffic policy to the target using the **service-policy** command, see DLP-J195 Attaching or Removing a Traffic Policy from the Target Using Cisco IOS Commands, on page 424.

Step 4 Monitor and verify the QoS configuration. See DLP-J205 Monitoring and Verifying QoS Configuration Using Cisco IOS Commands, on page 453.

NTP-J63 Configuring QoS Features Using CTC

Purpose	This procedure configures QoS using CTC.
Tools/Equipment	None

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

Procedure

Step 1 Create a class-map.
To create or edit a class-map, see DLP-J191 Creating or Editing a Class Map Using CTC, on page 411.

Step 2 Create a policy-map.
To create or edit a policy-map, see DLP-J193 Creating or Editing a Policy Map Using CTC, on page 420.

Step 3 Create a traffic policy by associating the traffic class with one or more QoS features. See DLP-J194 Setting Policy Class Actions Using CTC, on page 422.

Step 4 Attach the traffic policy to the target.
To attach or remove a traffic policy from the target, see DLP-J196 Attaching or Removing a Traffic Policy from the Target Using CTC, on page 427.

Step 5 Monitor and verify QoS configuration.
To monitor and verify QoS configuration, see DLP-J206 Monitoring and Verifying QoS Configuration Using CTC, on page 454

Ingress QoS Functions

Ingress QoS on the Cisco CPT system involves classification, marking, and policing. The ingress card classifies the packets and assigns a traffic-class to it. The traffic-class is used for internal queuing and congestion management, as well as classification at the egress. At ingress, policy application is supported on multiple targets, which are:

- Ten Gigabit Ethernet (10 GE) and one Gigabit Ethernet (1 GE) interface
- Port-channel interface
- Port-channel member interface
- Service instance on 10 GE and 1 GE interfaces
- Service instance on port-channel

Ingress Classification

Classifying network traffic enables you to organize traffic (that is, packets) into traffic classes or categories on the basis of whether the traffic matches specific criteria. Using the packet classification, you can partition

network traffic into multiple priority levels or classes of service. Traffic is classified to determine whether it should be:

- Marked for further processing
- Policed to rate limit specific traffic types

The CPT system supports ingress classification. The default class, named class-default, is the class to which any traffic that does not match any of the selection criteria in the configured class maps, is directed.

Ingress Classification Restrictions and Usage Guidelines

- The **match** commands are used to specify various criteria for classifying packets. The packets are checked to determine whether they match the criteria specified in the **match** commands.
- Only the **match-any** keyword is supported and is the default option. Traffic classification based on multiple QoS fields (Ethernet class of service [CoS], IP precedence, and so on) for a single packet is not supported. Traffic classification is based only on the first matching parameter (in the user-specified order) of the QoS fields, if multiple match criteria are specified in a single class.
- The match on **cos inner** or **vlan inner** is supported only in IOS mode

Configure ingress classification using Cisco IOS commands, see DLP-J190 Configuring Ingress Classification Using Cisco IOS Commands, on page 408.

To create or edit a class-map using CTC, see DLP-J191 Creating or Editing a Class Map Using CTC, on page 411.

DLP-J190 Configuring Ingress Classification Using Cisco IOS Commands

Purpose	This procedure creates a class map using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**class-map [match-any]** *class-map-name* **Example:** Router(config)# class-map match-any class1	Creates a class to be used with a class map and enters the class-map configuration mode. The class map is used for matching packets to the specified class. • **match-any—** Specifies that one of the match criterion must be met. Use this keyword only if you have to specify more than one match command. • *class-map-name—* Class map name. This is the name of the class map and can have a maximum of 40 alphanumeric characters.
Step 4	**match cos** *cos-number* **Example:** Router(config-cmap)# match cos 2	Matches a packet on the basis of a Layer 2 CoS number. • *cos-number—* CoS value. The value can range from 0 to 7. **Note** The **match cos** command is just an example of one of the match commands that can be used. For a list of other match commands, see Table 12: Traffic Class Commands, on page 409
Step 5	end **Example:** Router(config-cmap)# exit	Exits class-map configuration mode and returns to privileged EXEC mode.

The following table provides the traffic class commands supported at the ingress:

Table 12: Traffic Class Commands

Command	Description
match cos *cos-number* **Example:** Router(config-cmap)# match cos 2	Matches a packet on the basis of a Layer 2 CoS number. • *cos-number—* CoS value. The value can range from 0 to 7.
match ip precedence *ip-precedence-value* **Example:** Router(config-cmap)# match ip precedence 5	Identifies the IP precedence value as match criteria. • *ip-precedence-value—* IP precedence value. The value can range from 0 to 7.

Command	Description
match ip dscp *ip- dscp-value* **Example:** Router(config-cmap)# match ip dscp 6	Identifies a specific IP DSCP value as a match criterion. • *ip- dscp-value* — IP DSCP value. The value can range from 0 to 63.
match mpls experimental topmost *exp-value* **Example:** Router(config-cmap)# match mpls experimental topmost 5	Matches the MPLS EXP value in the topmost label. • *exp-value* — MPLS EXP value. The value can range from 0 to 7.

Examples: Ingress Classification

The following example shows how to configure a class-map named ipp5, and enter a match statement for IP precedence 5:

```
Router# enable
Router# configure terminal
Router(config)# class-map ipp5
Router(config-cmap)# match ip precedence 5
```

The following example shows how to configure a class-map on multiple match statements:

```
Router# enable
Router# configure terminal
Router(config)# class-map match-any IPP
Router(config-cmap)# match ip precedence 3
Router(config-cmap)# match ip precedence 4
```

The following example shows a logical OR operation in a child policy with match cos and class-default in a parent class.

```
Router(config)# class-map match-any childOR
Router(config-cmap)# match cos 5
Router(config)# policy-map testchildOR
Router(config-pmap)# class childOR
Router(config-pmap-c)# police cir percent 10
Router(config)# policy-map parentOR
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir percent 20
Router(config-pmap-c)# service-policy testchildOR
```

This example shows how to display class-map information for a specific class map:

```
Router# show class-map ipp5

class Map match-any ipp5 (id 1)
match ip precedence 5
```

DLP-J191 Creating or Editing a Class Map Using CTC

Purpose	The following procedure creates a class map using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

Step 1 Complete the "NTP-J22 Log into CTC, on page 15" procedure at a node where you want to create a class map.

Step 2 In the **node view**, right-click the **Fabric**or **Line card**and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click the **QoS** tab.

Step 5 To create a class map in the **Class Map** tab, click **Create Class Map**. In the Class Map Creation dialog box:

a) Enter the class map name in the Class-Map name field.

b) Choose **Match Any** option.

c) Select one of the following match attributes in the Match Attribute field:

- cos
- ip precedence
- ip dscp
- mpls experimental topmost
- qos group
- inner cos
- inner vlan

d) Enter the attribute value in the Attribute field based on the option that was selected in the Match Attribute field, see this table:

Table 13: Match Attribute and Attribute Value

Match Attribute	Attribute Value
cos	Value between 0-7

Match Attribute	Attribute Value
ip precedence	Value between 0-7
ip dscp	Value between 0-63
mpls experimental topmost	Value between 0-7
qos group	Value between 0-7
inner cos	Value between 0-7
inner VLAN	Value between 1-4095

e) Click **Add**.
f) Repeat Step 5.b to Step 5.d to add additional match criteria to the class map.
g) Click **Finish**.

Step 6 To edit the class map, in the **Class Map** tab, select the class map and click **Edit Class Map**. In the Class Map Creation dialog box:

a) Select the match attribute in the Match Attribute field to edit.
b) Change the attribute value in the Attribute field based on the option that was selected in the Match Attribute field (see DLP-J191 Creating or Editing a Class Map Using CTC, on page 411).
c) Click **Add**.
d) Repeat Step 6.b to Step 6.c to edit the remaining match attributes.
Note To remove the match attribute from the class map, select the match attribute and click **Remove**.
e) Click **Finish**.

Ingress Policing

Ingress policing ensures that an attached equipment does not submit more than a predefined amount of bandwidth (Rate Limiting) into the network. The policing feature can be used to enforce the committed information rate (CIR) and the peak information rate (PIR) available to a customer at an interface or a service instance on an interface. Policing enables to limit the data flow through the CPT system by dropping or marking down the QoS value according to the configuration.

The Cisco CPT system supports ingress policing. When policing is configured, traffic is placed in one of the following categories:

- Conform
- Exceed
- Violate

Within these three categories, users can decide the actions to be applied. For instance, packets that conform to the policy rate can be configured to be transmitted, packets that exceed the policy rate can be configured to be sent with a decreased priority, and packets that violate the policy rate can be configured to be dropped.

If no actions are specified, the default conform-action is transmit, and default exceed-action or violate-action is drop.

The following table contains the list of policing actions supported at the ingress:

Table 14: Policing Actions

Action	Purpose
transmit	Transmits the packet.
drop	Drops the packet.
set-discard-class-transmit	Sets the discard-class internal label to a specified value and transmits the packet. This action is effective only when egress QoS marking of an MPLS or Virtual Private Wire Service (VPWS) traffic is achieved using table-maps.
set-cos-transmit	Sets the CoS value and transmits the packet.
set-dscp-transmit	Sets the IP DSCP value and transmit the packet.
set-precedence-transmit	Sets the IP precedence value and transmits the packet.
set-qos-transmit	Sets the QoS-group value and transmits the packet.

The policing features supported are:

- Individual actions
- Multiple actions
- Single rate, 2-color policer
- Single rate, 3-color policer
- Dual rate, 3-color policer
- Color blind mode
- Hierarchical policing (two levels)
- Micro-flow policing

Ingress Policing Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS ingress policing on a CPT system are as follows:

- In a hierarchical QoS policy, only a single-rate, 2-color policer is supported at the parent level. This should be configured using the **police [rate]** *bps-value* action command. The **police cir** command is not supported at the parent level.
- In a hierarchical QoS policy with policer configured at the parent level, only a single-rate, 2-color policer or a dual-rate, 3-color policer is supported at the child level.

To create a policy-map using Cisco IOS commands, see DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 414.

To create or edit a policy-map using CTC, see DLP-J193 Creating or Editing a Policy Map Using CTC, on page 420.

To set policing actions using CTC, see DLP-J194 Setting Policy Class Actions Using CTC, on page 422.

To attach or remove a traffic policy from the interface using Cisco IOS commands, see DLP-J195 Attaching or Removing a Traffic Policy from the Target Using Cisco IOS Commands, on page 424.

To attach or remove a traffic policy from the interface using CTC, see DLP-J196 Attaching or Removing a Traffic Policy from the Target Using CTC, on page 427.

DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands

Purpose	This procedure creates a policy map and sets policing actions using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J190 Configuring Ingress Classification Using Cisco IOS Commands, on page 408
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** Router(config)# policy-map policy1	Creates or specifies the name of the traffic policy and enters the policy-map configuration mode. • *policy-map-name*—Policy map name. This is the name of the policy map and can have a maximum of 40 alphanumeric characters.
Step 4	**class** {*class-name* | **class-default**} **Example:**	Specifies the name of a traffic class to which the policy applies and enters the policy-map class configuration mode. • Enter the previously configured class-map name.

	Command or Action	Purpose
	Router(config-pmap)# class class1	◦ *class-name*—User-defined class name to which the policy applies. ◦ **class-default**—Specifies that the policy applies to the default traffic class. **Note** This step associates the traffic class with the traffic policy.
Step 5	**police [cir | rate]** *bps-value* **[bc | burst]** *bc* **[be | peak-burst]** *be* **conform-action** *action* **exceed-action** *action* **violate-action** *action* **Example:** Router(config-pmap-c)# police cir 5000000 bc 200000 be 400000 conform-action transmit exceed-action set-dscp-transmit violate-action drop	Specifies a maximum bandwidth usage by a traffic class through the use of a token bucket algorithm: • **cir**—Indicates that the committed information rate (CIR) is used for policing traffic. • **rate**—Indicates that the police rate is used for policing traffic. • *bps value*—Average rate in bits per second. The valid values range from 8000 to 10000000000. • **bc**—Indicates that the committed (conform) burst size is used for policing traffic. • **burst**—Indicates that the burst size is used for policing traffic. • *bc*—Committed (conform) burst size or burst size in bytes. The valid values range from 1000 to 256000000. • **be**—Indicates that the excess burst size is used for policing traffic. • **peak-burst**—Indicates that the peak-burst size is used for policing traffic. • *be*—Excess burst size or peak-burst size in bytes. The valid values range from 1000 to 256000000. • *action*—Action taken on a packet when it conforms, exceeds, or violates the interface bandwidth. The possible actions are shown in Table 14: Policing Actions, on page 413. **Note** The **police [cir | rate]** *bps-value* **[bc | burst]** *bc* **[be | peak-burst]** *be* **conform-action** *action* **exceed-action** *action* **violate-action** *action* command is just an example of one of the policy commands that can be used. For a list of other policy commands, see Table 15: Traffic Policy Commands, on page 416.
Step 6	end **Example:**	Exits policy-map configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	Router(config-pmap)# end	

The following table provides the traffic policy commands supported at the Ingress:

Table 15: Traffic Policy Commands

Command	Description
police [cir | rate] *bps-value* **[bc | burst]** *bc* **[be | peak-burst]** *be* **conform-action** *action* **exceed-action** *action* **violate-action** *action* **Example:** Router(config-pmap-c)# police cir 5000000 bc 200000 be 400000 conform-action transmit exceed-action set-dscp-transmit violate-action drop	Specifies a maximum bandwidth usage by a traffic class through the use of a token bucket algorithm: • **cir—**Indicates that the committed information rate (CIR) is used for policing traffic. • **rate—**Indicates that the police rate is used for policing traffic. • *bps value*—Average rate in bits per second. The valid values range from 8000 to 10000000000. • **bc—**Indicates that the committed (conform) burst size is used for policing traffic. • **burst—**Indicates that the burst size is used for policing traffic. • *bc*—Committed (conform) burst size or burst size in bytes. The valid values range from 1000 to 256000000. • **be—**Indicates that the excess burst size is used for policing traffic. • **peak-burst—**Indicates that the peak-burst size is used for policing traffic. • *be*—Excess burst size or peak-burst size in bytes. The valid values range from 1000 to 256000000. • *action*—Action taken on a packet when it conforms, exceeds, or violates the interface bandwidth. The possible actions are shown in Table 14: Policing Actions, on page 413.

Command	Description
police [cir | rate] percent *%* **[bc | burst]** *bc* **[be | peak-burst]** *be* **conform-action** *action* **exceed-action** *action* **violate-action** *action* **Example:** Router(config-pmap-c)# police cir percent 10 bc 200000 be 400000 conform-action transmit exceed-action set-dscp-transmit violate-action drop	Configures traffic policing on the basis of a percentage of bandwidth available on an interface, where: • **cir—**Indicates that the committed information rate (CIR) is used for policing traffic. • **rate—**Indicates that the police rate is used for policing traffic. • **percent—**Indicates that a percentage of bandwidth is used for calculating CIR or rate. • *%—* CIR or rate bandwidth percentage. The valid values range from 1 to 100. • **bc—**Indicates that the committed (conform) burst size is used for policing traffic. • **burst—**Indicates that the burst size is used for policing traffic. • *bc—*Committed (conform) burst size or burst size in mill-seconds or micro-seconds. • **be—**Indicates that the excess burst size is used for policing traffic. • **peak-burst—**Indicates that the peak-burst size is used for policing traffic. • *be—*Excess burst size or peak-burst size in mill-seconds or micro-seconds. • *action—*Action taken on a packet when it conforms, exceeds, or violates the interface bandwidth. The possible actions are shown in Table 14: Policing Actions, on page 413.

Command	Description
police [cir | rate] *bps-value* **[bc | burst]** *bc* **[pir | peak-rate]** *pir* **[be | peak-burst]** *be* **conform-action** *action* **exceed-action** *action* **violate-action** *action*	Configures traffic policing using two rates (CIR and PIR) where: • **cir—**Indicates that the committed information rate (CIR) is used for policing traffic. • **rate—**Indicates that the police rate is used for policing traffic. • *bps value*—Average rate in bits per second. The valid values range from 8000 to 10000000000 • **bc—**Indicates that the committed (conform) burst size is used for policing traffic. • **burst—**Indicates that the burst size is used for policing traffic. • *bc*—Committed (conform) burst size or burst size in bytes. The valid values range from 1000 to 256000000. • **pir—** Indicates that the peak information rate (PIR) is used for policing traffic. • **peak-rate—** Indicates that the peak rate is used for policing traffic. • *pir*—Peak information rate or peak rate in bits per second. The valid values range from 8000 to 10000000000 • **be—**Indicates that the excess burst size is used for policing traffic. • **peak-burst—**Indicates that the peak-burst size is used for policing traffic. • *be*—Excess burst size or peak-burst size in bytes. The valid values range from 1000 to 256000000. • *action*—Action taken on a packet when it conforms, exceeds, or violates the interface bandwidth. The possible actions are shown in Table 14: Policing Actions, on page 413.

Examples: Ingress Policing

The following example shows how to configure policing actions:

```
Router(config)# policy-map ABC
Router(config-pmap)# class class-default
Router(config-pmap-c)# police 10000000 8000 8000
```

```
Router(config-pmap-c-police)# conform-action set-cos-transmit 2
Router(config-pmap-c-police)# exceed-action set-cos-transmit 1
Router(config-pmap-c-police)# end
Router#
```

The following example shows how to display policy map information:

```
Router# show policy-map ABC
```

```
Policy Map ABC
class class-default
police cir 10000000 bc 8000 be 8000
conform-action set-cos-transmit 2
exceed-action set-cos-transmit 1
Router#
```

The following example shows how to configure a single rate 2-color policer:

```
Router(config)# policy-map 1r2c
Router(config-pmap)# class class-default
Router(config-pmap-c)# police 2000000
Router(config-pmap-c-police)# conform-action transmit
Router(config-pmap-c-police)# exceed-action drop
Router(config-pmap-c-police)# end
```

The following example shows how to configure a single rate, 2-color policer with percent:

```
Router(config)# policy-map 1r2c_percent
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir percent 20
Router(config-pmap-c-police)# conform-action set-cos-transmit 0
Router(config-pmap-c-police)# exceed-action drop
Router(config-pmap-c-police)# end
Router#
```

The following example shows how to configure a dual rate, 3-color policer:

```
Router(config)# policy-map 2r3c
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir 2000000 pir 3000000
Router(config-pmap-c-police)# conform-action set-prec-transmit 3
Router(config-pmap-c-police)# exceed-action set-prec-transmit 2
Router(config-pmap-c-police)# violate-action set-prec-transmit 1
Router(config-pmap-c-police)# end
Router#
```

The following example shows how to configure a dual rate, 3-color policer with percent:

```
Router(config)# policy-map 2r3c_percent
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir percent 10 pir percent 20
Router(config-pmap-c-police)# conform-action transmit
Router(config-pmap-c-police)# exceed-action set-cos-transmit 0
Router(config-pmap-c-police)# violate-action drop
Router(config-pmap-c-police)# end
Router#
```

The following example shows how to configure a single rate, 2-color policer in class-default and a child policy:

```
Router# enable
Router# configure terminal
Router(config)# policy-map police5
Router(config-pmap)# class test18
```

```
Router(config-pmap-c)# service policy child-level
Router(config-pmap-c)# police cir 64000 50
```

The following example shows how to configure a dual rate, 3-color policer configuration in a class and policy-map:

```
Router# enable
Router# configure terminal
Router(config)# policy-map test
Router(config-pmap)# class cos2
Router(config-pmap-c)# police 1000000 pir 2000000 conform-action set-cos-transmit 3
exceed-action set-cos-transmit 1 violate-action drop
```

The following example shows how to configure a dual rate, 3-color policer in class-default with a CIR of 64 Kbps, and PIR doubled the CIR rate, a conform action of transmit, and an exceed action mark dscp af 11:

```
Router# enable
Router# configure terminal
Router(config)# policy-map qos_test
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir 64000 bc 2000 pir 128000 be 2000 conform-action transmit

exceed-action set-dscp-transmit af11 violate-action set-dscp-transmit cs1
```

The following example shows how to configure a dual rate, 3-color policer in class-default:

```
Router# enable
Router# configure terminal
Router(config)# policy-map qos_test
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir 64000 bc 2000 pir 128000 be 2000 conform-action transmit

exceed-action set-dscp-transmit af11 violate-action set-dscp-transmit cs1
```

DLP-J193 Creating or Editing a Policy Map Using CTC

Purpose	This procedure creates or edits a policy map using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J191 Creating or Editing a Class Map Using CTC, on page 411
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

Step 1 Complete the "NTP-J22 Log into CTC, on page 15" procedure at a node where you want to create a policy map.

Step 2 In the node view, right-click the Fabric or Line card and choose Open Packet Transport System View. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click the **QoS** tab.

Step 5 To create a policy map, in the **Policy Map** tab, click **Create Policy Map**. In the Policy Creation dialog box:

a) Enter the policy map name in the Policy-Map field.

b) Choose the class to be added to the policy map.

c) Click **Add**.

d) (Optional) Choose the child policy to be added from the Child Policy column.

Note A child policy is present only if there is another policy map created previously.

e) Add policy actions. See DLP-J194 Setting Policy Class Actions Using CTC, on page 422.

f) Repeat Step 5.a to Step 5.e to create additional policy maps.

g) Click **Finish**.

Step 6 To edit the policy map, in the **Policy Map** tab, select the policy map and click **Edit Policy Map**. In the Policy Creation dialog box, do the following to add a new class map to the policy map:

a) Choose the class to be added to the policy map.

b) Click **Add**.

c) (Optional) Choose the child policy to be added from the Child Policy column.

Note A child policy is present only if there is another policy map created previously.

d) Add policy actions. See DLP-J194 Setting Policy Class Actions Using CTC, on page 422.

e) Repeat Step 6.a to Step 6.d to add the remaining class maps to the policy map.

Note To remove the class map from the policy map, select the class from the Traffic Classes interface area and click **Remove**.

f) Click **Finish**.

DLP-J194 Setting Policy Class Actions Using CTC

Purpose	This procedure sets the following policy class actions using CTC: • Configuring Ingress Policing • Configuring Ingress Marking • Configuring Egress Shaping • Configuring Egress Bandwidth • Configuring Low-Latency Queuing (LLQ) • Configuring Egress Bandwidth Remaining Ratio (BRR) or Bandwidth Remaining Percent (BRP)
Tools/Equipment	None
Prerequisite Procedures	DLP-J193 Creating or Editing a Policy Map Using CTC, on page 420
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

Step 1 Complete the "NTP-J22 Log into CTC, on page 15" procedure at a node where you want to set the policy class actions.

Step 2 In the node view, right-click the Fabric or Line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click the **QoS** tab.

Step 5 In the **Policy Map** tab, select the policy map and click **Edit Policy Map**. The Policy Map Creation dialog box appears.

Step 6 In the traffic classes area, click **Actions** to set policy actions for a specific class. The Policy Class Actions wizard is displayed.

Step 7 In the **Traffic Marking** tab:

a) Choose the attribute from the Set Attribute drop-down list.

b) Enter the attribute value based on the selection made in the Set Attribute drop-down list:

Table 16: Attribute and Attribute Value

Attribute	Attribute Value
cos	Value between 0-7
ip precedence	Value between 0-7
ip dscp	Value between 0-63
qos group	Value between 0-7
discard class	Value between 0-2
cos inner	Value between 0-7
vlan inner	Value between 0-4096. For each vlan, you can have up to 30 entries.

c) Click **Add**.
d) Repeat steps 7.a through 7.c to set values for the remaining marking attributes.
e) Click **Finish**.

Step 8 In the **Policing** tab:

a) Choose one of the rates:

- Single-Rate Dual Color (CIR)
- Single-Rate Dual Color (PIR)
- Single-Rate Three Color
- Dual-Rate Three Color

b) Enter the rate and burst size for the attributes:

- Committed Information Rate and Burst Size and choose the unit from the drop-down list.
- Peak Information Rate and PeakBurst Size and choose the unit from the drop-down list.

Note The burst size unit must be **ms** if the CIR or the PIR value specified is in terms of percentage (%), and **bytes/Kbytes/mbytes** if the CIR or the PIR value specified is in terms of bits per second (bps).

c) Set the actions:

- From the Conform Action drop-down list, select the action and click **Add**.
- From the Exceed Action drop-down list, select the action and click **Add**.
- From the Violate Action drop-down list, select the action and click **Add**.

d) Click **Finish**.

Step 9 (At Egress Only) In the **Queuing** tab:

a) To set the shape average:

- Select the **Shape Average** radio button.
- Enter the Average Rate value and choose the unit from the drop-down list.
- Select the **Minimum Bandwidth** or the **Remaining Bandwidth** radio button.
- Enter the minimum or the remaining bandwidth configuration values and choose the units.

b) To set the priority:

- Select the **Priority** radio button.
- Enter the priority value and choose the unit.
- Check the **Blank** check box to set the priority without entering any value.

Note CTC supports configuring priority without any values.

c) Click **Finish**.

DLP-J195 Attaching or Removing a Traffic Policy from the Target Using Cisco IOS Commands

Before a traffic policy can be enabled for a class of traffic, it must be configured on a target. Use the **service-policy {input | output}** configuration command to attach a traffic policy to a target and to specify the direction in which the policy should be applied (either on packets entering/ingressing the target or packets exiting/egressing the target). Only one traffic policy can be applied to an interface in a given direction. Use the **no** form of the command, that is, **no service-policy {input | output}** *policy-map-name* to detach a traffic policy from a target.

Purpose	This procedure attaches or removes the traffic policy from the target using Cisco IOS commands.
Tools/Equipment	None

Prerequisite Procedures	One of the following: • DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 414 • DLP-J197 Configuring Ingress Marking Using Cisco IOS Commands, on page 429 • DLP-J207 Configuring Table Maps for Egress Marking Using Cisco IOS Commands, on page 436 • DLP-J200 Associating Table Maps at Egress Using Cisco IOS Commands, on page 439 • DLP-J203 Configuring Egress Shaping Using Cisco IOS Commands, on page 447 • DLP-J202 Configuring Egress Bandwidth Using Cisco IOS Commands, on page 445 • DLP-J201 Configuring Egress LLQ Using Cisco IOS Commands, on page 442 • DLP-J204 Configuring Egress Bandwidth Remaining Ratio or Bandwidth Remaining Percent Using Cisco IOS Commands, on page 450
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	enable **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:**	Configures an interface type and enters the interface configuration mode. • *interface-type*—Interface type

	Command or Action	Purpose
	Router(config)# interface TenGigabitEthernet 4/1	• *interface-number*—Interface number.
Step 4	**service instance** *id* **ethernet** **Example:** Router(config-if)# service instance 100 ethernet	Enters the service instance mode. • *id*—Service instance ID.
Step 5	**service-policy {input | output}** *policy-map-name* **Example:** Router(config-if-srv-instance)# service-policy input policy1	Attaches a policy map to a target. • Enter either the input or output keyword and the policy map name. • *policy-map-name*—Name of the policy map.
Step 6	**no service-policy {input | output}** *policy-map-name* **Example:** Router(config-if-srv-instance)# no service-policy input policy1	Removes the policy map from the target. • Enter either the input or output keyword and the policy map name.
Step 7	end **Example:** Router(config-if-srv-instance)# end	Exits the service instance mode.

Example: Attaching or Removing a QoS Traffic Policy for a Target

The following example shows how to attach a traffic policy to a target:

```
Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv-instance)# service-policy input policy1
Router(config-if-srv-instance)# end
```

The following example shows how to remove a traffic policy from a target:

```
Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# service instance 100 ethernet
Router(config-if)# no service-policy input policy1
Router(config-if)# end
```

DLP-J196 Attaching or Removing a Traffic Policy from the Target Using CTC

Purpose	This procedure attaches or removes a traffic policy from the target using CTC.
Tools/Equipment	None
Prerequisite Procedures	• DLP-J193 Creating or Editing a Policy Map Using CTC, on page 420 • DLP-J194 Setting Policy Class Actions Using CTC, on page 422 • DLP-J198 Creating or Editing a Table Map Using CTC, on page 441
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Note A target can be a port, an EFP, pseudo-wire, or a channel-group.

Procedure

Step 1 Complete the "NTP-J22 Log into CTC, on page 15" procedure at a node.

Step 2 In the node view, right-click the Fabric or Line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click **QoS**.

Step 5 To attach a traffic policy to the port, in the **Ports** tab:

a) From the **Select the slot** drop-down list, choose the slot.
b) To apply an ingress policy to the port, select the policy from the **Ingress Policy** drop-down list.
c) To apply an egress policy to the port, select the policy from the **Egress Policy** drop-down list.
d) To apply a table map, select the table map and configuration from the **Table Map** and **Table Map Config** drop-down lists.
e) Click **Apply**.
f) Repeat Step 5.a to Step 5.e to attach traffic policies to the remaining ports.

Step 6 To remove a traffic policy from the port:

a) From the **Select the slot** drop-down list, choose the slot.
b) To remove an ingress policy from the port, select **None** from the **Ingress Policy** drop-down list.
c) To remove an egress policy from the port, select **None** from the **Egress Policy** drop-down list.

d) To remove a table map, select **None** from the **Table Map** and **Table Map Config** drop-down lists.
e) Click **Apply**.
f) Repeat Step 6.a to Step 6.e to remove traffic policies from the remaining ports.

Note
- To attach a traffic policy to an EVC circuit, see Step 10 of DLP-J3 Edit an EVC Circuit Using CTC, on page 147.
- To attach a traffic policy to a pseudo-wire, see Step 12.o and Step 12.p of DLP-J91 Create a Pseudowire Using CTC, on page 359.
- To attach a traffic policy to a channel group:
  1. Complete the "NTP-J22 Log into CTC, on page 15" procedure at a node.
  2. In the node view, right-click the Fabric or Line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.
  3. Click the **Provisioning** tab.
  4. From the left pane, click **Channel Groups**.
  5. Select the channel group and choose the table map or policy map that you want to attach.
  6. Click **Apply**.

Ingress Marking

Marking is a way to selectively modify QoS bits in a packet to identify traffic within the system and/or the network. The downstream devices in the network and the egress targets within the system can match the traffic based on the marking done at the ingress of the system. The Cisco CPT system supports ingress marking.

After you create traffic classes, configure traffic policies and traffic marking features to apply certain actions to the selected traffic in those classes.

In most cases, the purpose of a packet mark is identification. After a packet is marked, downstream devices identify traffic based on the marking and categorize the traffic according to network needs. This categorization occurs when the match commands in the traffic class are configured to identify the packets by their marking (for example, match IP precedence, match IP DSCP, match CoS, and so on). The traffic policy using this traffic class can then set the appropriate QoS features for the marked traffic.

Ingress Marking Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS ingress marking on a CPT system are as follows:

- Marking of the MPLS EXP bits is not supported at the ingress. However, the egress marking feature enables to mark the MPLS EXP bits by using table-maps.
- Marking of the Layer 2 CoS bit for VPWS traffic is not supported.
- The **discard-class** command for marking is not effective for end-to-end Ethernet traffic.

To configure ingress marking using Cisco IOS commands, see DLP-J197 Configuring Ingress Marking Using Cisco IOS Commands, on page 429.

To configure ingress marking using CTC, see Step 7 in DLP-J194 Setting Policy Class Actions Using CTC, on page 422.

DLP-J197 Configuring Ingress Marking Using Cisco IOS Commands

Purpose	This procedure configures ingress marking using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 414
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** Router(config)# policy-map policy1	Creates or specifies the name of the traffic policy and enters the policy-map configuration mode. • *policy-map-name*— Policy map name. This is the name of the policy map and can have a maximum of 40 alphanumeric characters.
Step 4	**class** {*class-name* | **class-default**} **Example:** Router(config-pmap)# class class1	Specifies the name of a traffic class to which the policy applies and enters the policy-map class configuration mode. • Enter the previously configured class-map name. ◦ *class-name*—User-defined class name to which the policy applies. ◦ **class-default**—Specifies that the policy applies to the default traffic class.

	Command or Action	Purpose
		Note This step associates the traffic class with the traffic policy.
Step 5	**set ip precedence** *ip precedence value* **Example:** Router(config-pmap-c)# set ip precedence 2	Marks the precedence value in the IP header with a value between 0 to 7. • *ip precedence value*— IP precedence value. **Note** The **set ip precedence** command is just an example of one of the marking commands that can be used. For a list of other marking commands, see Table 17: Traffic Marking Commands, on page 430.
Step 6	end **Example:** Router(config-pmap)# end	Exits policy-map configuration mode and returns to privileged EXEC mode.

The following table provides the traffic marking commands supported at Ingress:

Table 17: Traffic Marking Commands

Command	Description
set ip precedence *ip-precedence-value* **Example:** Router(config-pmap-c)# set ip precedence 2	Marks the precedence value in the IP header with a value between 0 to 7. • *ip precedence value*—IP precedence value.
set cos *cos-value* **Example:** Router(config-pmap-c)# set cos 2	Marks the CoS value between 0 to 7 in an 802.1Q tagged frame • *cos-value*—CoS value.
set ip dscp *ip-dscp-value* **Example:** Router(config-pmap-c)# set ip dscp 22	Marks the IP DSCP in the ToS byte with a value between 0 to 63. • *ip-dscp-value*—IP DSCP value.
set qos group *qos-group-value* **Example:** Router(config-pmap-c)# set qos group 3	Marks a QoS group identifier (ID) with a value between 0 to 7 that can be used later to classify packets. • *qos-group-value*—QoS group value.

Command	Description
set discard-class *value* **Example:** Router(config-pmap-c)# set discard-class 0	Sets the discard-class internal label to a specified value between 0 to 2. This command is supported only during table-map creation. • *value*—Discard-class value.

Examples: Ingress Marking

The following example shows the creation of a service policy called policy1. This service policy is associated to a previously defined classification policy through the use of the class command. This example assumes that a classification policy called class1 was previously configured. This example configures marking to set the IP precedence value:

```
Router# enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip precedence 1
```

This example configures marking to set the CoS value:

```
Router# enable
Router# configure terminal
Router(config)# policy-map test
Router(config-pmap)# class test
Router(config-pmap-c)# set cos 1
```

Egress QoS Functions

Egress QoS on the CPT system involves classification, shaping, queuing & scheduling, and marking. At egress, policy application is supported on multiple targets, which are:

- 10 Gigabit Ethernet (10GE) and 1 Gigabit Ethernet (1GE) interface
- Port channel interface
- Service instance on 10GE and 1GE interfaces
- Service instance on port channel

  At egress, QoS traffic can broadly be classified into two types--unicast and multicast traffic. Each of these traffic can be further classified into priority traffic which requires low latency queuing and normal traffic which does not have latency considerations.

In the CPT system, QoS at the egress can be divided into unicast traffic QoS and multicast traffic QoS. Any QoS operation performed at the egress using qos-group as a match criteria is applied only to the unicast traffic.

Unicast Versus Multicast Traffic QoS at Egress

In the CPT system, QoS at egress can be split into unicast traffic QoS and multicast traffic QoS. Any QoS operation performed at egress using qos-group as a match criteria is applied only to the unicast traffic.

Unicast traffic includes:

- Point-to-point EVC traffic
- Point-to-multipoint EVC traffic flows for L2 learned traffic
- VPWS traffic

Multicast traffic includes:

- Broadcast data traffic, unknown destination MAC flood traffic, IP multicast traffic in point-to-multipoint EVC configurations
- VPLS flood traffic

Traffic Handling in the Absence of an Output Policy

If there is no output policy configured on an EVC or an interface, the unicast traffic will be queued at the egress based on the traffic class set at the ingress. In the absence of an output policy, all the egress queues will be treated equally and will be scheduled according to the Round Robin method.

Unicast QoS Restrictions

Traffic is queued in separate queues at the egress based on the traffic-class set in the frame at the ingress. This is irrespective of whether there is an egress policy applied or not.

Note The “class-default” classification does not work at the leaf level of an output policy. This works only at a parent level in a hierarchical policy. It must be ensured that all traffic that needs to be matched using “class-default” at the leaf level is set to “qos-group 0” at the ingress, which forces the traffic-class to 0 resulting in traffic being queued in queue 0 which corresponds to the class-default.

Egress Classification

The egress classification is limited to using a traffic class field in frames to categorize the frames and make them available for QoS handling. Therefore, classification based on frame fields, such as Ethernet CoS, IP DSCP, IP precedence, MPLS EXP, and so on, should be done at ingress, and the traffic class should be assigned to the corresponding frames using the ingress marking feature.

Traffic is classified to determine whether it should be:

- Marked for further processing
- Queued and scheduled

Egress Classification Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS egress classification on a Cisco CPT system are as follows:

- Only one match filter is supported for each class-map.
- Only qos-group based matching is supported for user-defined classes.
- Match based on qos-group 3 and qos-group 7 is used only for low latency queuing across the system.

- Match based on the class-default in the output policy suggests that matching is based on the qos-group 0 and not the class where traffic, which does not match any selection criteria in the configured class maps, is directed.

Note Multicast traffic classification at egress differs from that of the unicast traffic classification. For details, see Understanding Multicast QoS, on page 456.

To configure classification at the egress using Cisco IOS commands, see DLP-J199 Configuring Egress Classification Using Cisco IOS Commands, on page 433.

To configure classification at the egress using CTC, see DLP-J191 Creating or Editing a Class Map Using CTC, on page 411.

DLP-J199 Configuring Egress Classification Using Cisco IOS Commands

Purpose	This procedure explains how to configure classification at the egress using Cisco IOS commands
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**class-map [match-any]** *class-map-name* **Example:** Router(config)# class-map match-any class1	Creates a class to be used with a class map and enters the class-map configuration mode. The class map is used for matching packets to the specified class. • *class-map-name*—Class name. This is the name of the class map and can have a maximum of 40 alphanumeric characters.

	Command or Action	Purpose
		The **match-any** keyword specifies that one of the match criteria must be met. Use this keyword only if you have to specify more than one match command.
Step 4	**match qos-group** *qos-group-number* **Example:** Router(config-cmap)# match qos-group 2	Matches a packet on the basis of traffic class represented by the qos-group. • *qos-group-number*—QoS-group value. The value can range from 0 to 7.
Step 5	end **Example:** Router(config-cmap)# exit	Exits class-map configuration mode and returns to privileged EXEC mode.

The following example shows how to create a class map:

```
Router# enable
Router# configure terminal
Router(config)# class-map c1
Router(config-cmap)# match qos-group 1
```

The following example shows a logical OR operation in a child policy with match qos-group and class-default in a parent class.

```
Router# enable
Router# configure terminal
Router(config)# class-map match-any childOR
Router(config-cmap)# match qos-group 1
Router(config)# policy-map testchildOR
Router(config-pmap)# class childOR
Router(config-pmap-c)# shape average 100000000
Router(config)# policy-map parentOR
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 500000000
Router(config-pmap-c)# service-policy testchildOR
```

This example shows how to display class-map information for a specific class map using the **show run class-map** command:

```
Router# show run class-map

Building configuration...
Current configuration : 275 bytes
!
class-map match-any EgressClassmap
 match qos-group 3
class-map match-any IngressClassMap
 match cos  1
end
```

Egress Marking

The egress marking sets the MPLS EXP bits in frames egressing the Cisco CPT system in case of the VPWS (Virtual Private Wire Service) initiation and MPLS LSR (Label Switching Router) interfaces; and sets CoS bits at the VPWS termination. This is based on the qos-group, discard-class setting at the ingress. At egress, marking is done using table maps. Table-map is used for mapping the values from qos-group and discard-class to the MPLS EXP or Ethernet CoS bit at egress.

Egress Table-Map Marking

Table maps are used to mark traffic attributes. A table-map lists and maps one traffic attribute to another. In the Cisco CPT system, table-maps are created to mark the:

- MPLS EXP bit for the VPWS initiation or LSR traffic
- VLAN CoS bit for the VPWS termination traffic

In the Cisco CPT system, up to 16 table maps can be created.

A table-map is applied on the imposition PE for marking the CoS or IP DSCP/IP Precedence bits to the EXP bits and on the disposition PE for remarking the EXP bits to the CoS bits.

For carrier Ethernet circuits, marking is done using the regular ingress QoS policy options and do not require table-maps.

A table-map is applied at the LER (label edge router) port for marking the CoS or IP DSCP/IP Precedence bits to the EXP bits. A table-Map is applied at the LSR (label switch router) port or the SPE (service provider edge) port to remark the EXP bits.

A table-map is applied to the pseudo-wire (or VPWS) for marking or remarking the EXP bits to the CoS bits. A table-map can be applied only at the VPWS termination point.

Note If a table-map is not attached, the MPLS EXP or the VLAN CoS bit is set to zero. Also, the system default setting is zero.

Egress Table-Map Marking Restrictions and Usage Guidelines

The restrictions and guidelines when configuring the QoS egress marking using table maps on a Cisco CPT system are as follows:

- The **set** action commands are not allowed in an output policy.
- Egress MPLS EXP marking is supported only in the interface mode of an MPLS interface.
- Egress marking of MPLS EXP bits using the **platform set mpls-exp-topmost** command is not effective on penultimate hop popping (PHP) nodes because the tunnel label is popped in PHP scenarios and inner virtual circuit (VC) label EXP marking is forwarded as is.
- Egress CoS marking is supported only for attachment circuits and only in the service instance mode.
- Egress pseudowire CoS marking is supported with the following limitations:
  - For type-5 pseudowires, CoS marking is supported when user-configured tag rewrite actions trigger VLAN tag addition on the egress interface.

- For type-4 pseudowires, CoS marking is supported when user-configured tag rewrite actions trigger VLAN tag addition or modification on the egress interface.

To configure table-maps using Cisco IOS commands, see DLP-J207 Configuring Table Maps for Egress Marking Using Cisco IOS Commands, on page 436 .

To associate table-maps at the egress using Cisco IOS commands, see DLP-J200 Associating Table Maps at Egress Using Cisco IOS Commands, on page 439.

To configure table-maps using CTC, see DLP-J198 Creating or Editing a Table Map Using CTC, on page 441.

To associate table-maps at egress using CTC, see Step 5d in DLP-J196 Attaching or Removing a Traffic Policy from the Target Using CTC, on page 427.

DLP-J207 Configuring Table Maps for Egress Marking Using Cisco IOS Commands

Purpose	This procedure explains how to configure table maps for egress marking using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**table-map** *table-map-name* **Example:** Router(config)# table-map table1	Creates or specifies the name of the table map and enters table-map configuration mode. • *table-map-name*—Table map name. This is the name of the table map and can have a maximum of 40 alphanumeric characters.

	Command or Action	Purpose
Step 4	**map from** *from-value1, from-value2* **to** *to-value* **Example:** Router(config-tablemap)# map from 0, 2 to 2	Maps the QoS-group and discard values to the MPLS EXP or VLAN COS bit. • *from-value1*—Value of the qos-group which can range from 0 to 7. • *from-value2*—Value of the discard class which can range from 0 to 2. • *to-value*—Value of the MPLS EXP or VLAN CoS bits which can range from 0 to 7.
Step 5	**default copy** **Example:** Router(config-tablemap)#default copy	(Optional) Copies the qos-group value set at ingress to the MPLS EXP or VLAN COS bits.
Step 6	**default value** *value* **Example:** Router(config-tablemap)# default value 2	(Optional) Sets the MPLS EXP bits or the VLAN COS bits to the value stated in the command, that is, it sets the "*to-value*" to the value specified in the command, when there is no explicit mapping configured for a specific {qos-group, discard-class} tuple in the given table map. • *value*—Default value which can range from 0 to 7.
Step 7	end **Example:** Router(config-tablemap)# end	Exits table-map configuration mode and returns to privileged EXEC mode.

Note After creating the table map, the users can set the qos-group and discard class parameters to the desired value by using the sequence of commands given below. For more information on these commands, see DLP-J207 Configuring Table Maps for Egress Marking Using Cisco IOS Commands, on page 436:

```
Router(config)# policy-map ingresspolicy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set qos-group 1
Router(config-pmap-c)# set discard-class 2
```

Table 18: Set Commands

Command	Description
set qos group *qos group value* **Example:** Router(config-pmap-c)# set qos group 3	Marks a QoS group identifier (ID) with a value between 0 to 7 that can be used later to classify packets. • *qos group value*—QoS group value.
set discard-class *value* **Example:** Router(config-pmap-c)# set discard-class 0	Sets the discard-class internal label to a specified value between 0 to 2. • *value*—Discard-class value.

Note To associate table maps to an interface using IOS commands, see DLP-J200 Associating Table Maps at Egress Using Cisco IOS Commands, on page 439.

Examples: Table-Map Marking

The following example shows how to create a table map that contains multiple entries.

```
Router# enable
Router# configure terminal
Router(config)# table-map test_table
Router(config-tablemap)# map from 0,2 to 2
Router(config-tablemap)# map from 0,0 to 0
```

The following example shows how to display the table-map information:

```
Router# show table-map test_table

 Table Map test_table
    map from 0,2 to 2 (hw idx: 2)
    default 0
Router#
```

The following example shows how to create a discard class and attach a policy-map to an interface (associates a table-map to the VPWS initiation or termination):

```
Router(config)# policy-map ingresspolicy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set qos-group 1
Router(config-pmap-c)# set discard-class 2

Router(config)# interface tenGigabitEthernet 4/2
Router(config-if)# service-policy input ingresspolicy1
Router(config-if)# end
Router#

Router# show running-config policy-map ingresspolicy1

Building configuration...
```

```
Current configuration : 329 bytes
!
policy-map ingresspolicy1
 class class-default
  set qos-group 1
  set discard-class 2
!
End
```

DLP-J200 Associating Table Maps at Egress Using Cisco IOS Commands

Purpose	This procedure explains how to associate table maps at the egress to an interface for VPWS initiation, LSR, and the VPWS termination scenarios using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J207 Configuring Table Maps for Egress Marking Using Cisco IOS Commands, on page 436
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TengigabitEthernet 4/1	Enters the interface configuration mode. • *type number*—Interface type and interface number.
Step 4	**service-policy output** *policy-map-name* **Example:** Router(config-if)# service-policy output policy1	Attaches a policy map to an interface. • *policy-map-name*— Policy map name.

	Command or Action	Purpose
Step 5	**service instance** *id* **ethernet** **Example:** Router (config-if)# service instance 200 ethernet	(Only for VPWS termination) Enters the service instance mode. • *id* — Service instance id.
Step 6	**platform set mpls-exp-topmost from qos-group, discard-class table** *table-map-name* **Example:** Router(config-if-srv-instance)#platform set mpls-exp-topmost from qos-group, discard-class table table1	(Only for VPWS initiation and LSR scenarios) Maps the MPLS-EXP value from the table map. • *table-map-name*—Name of the table map.
Step 7	**platform set cos from qos-group, discard-class table** *table-map-name* **Example:** Router(config-if-srv-instance)#platform set cos from qos-group, discard-class table table1	(Only for VPWS termination scenario) Maps the VLAN CoS value from the table map. • *table-map-name*—Name of the table map.
Step 8	end **Example:** Router(config-if)# end	Exits the interface configuration mode.

Examples: Egress Table-Map Marking

The following example shows how to map the MPLS-EXP value for VPWS initiation (that is, the frame contains MPLS header):

```
Router(config)# int tenGigabitEthernet 4/4
Router(config-if)# service-policy output egresspolicy1
Router(config-if)# platform set mpls-exp-topmost from qos-group, discard-class table
test_table
```

The following example shows how to map the VLAN CoS value for VPWS termination where the MPLS header is removed from the frame. The **platform set cos from qos-group** command is accepted at the service instance level.

```
Router(config)# int tenGigabitEthernet 4/4
Router(config-if)# service-policy output egresspolicy1
Router(config-if)# service instance 200 ethernet
Router(config-if-srv-instance)# platform set cos from qos-group, discard-class table
test_table
```

DLP-J198 Creating or Editing a Table Map Using CTC

Purpose	The following procedure explains how create or edit a table map using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

Step 1 Complete the "NTP-J22 Log into CTC, on page 15" procedure at a node where you want to create a table map.

Step 2 In the node view, right-click the Fabric or Line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 From the left pane, click the **QoS** tab.

Step 5 To create a table map, in the **Table Map** tab, click **Create Table Map**. In the Table Map Creation dialog box:

a) Enter the table map name in the Table-Map name field.
b) Enter the default value.
c) Enter the values for QoS Group and Discard Class.
d) Enter the value to set MPLS or CoS attributes.
e) Click **Add**.
f) Repeat Step 5a to Step 5e to create multiple table map entries.
g) Click **Finish**.

Note To associate table maps to an interface using CTC, see Step 5d in DLP-J196 Attaching or Removing a Traffic Policy from the Target Using CTC, on page 427.

Step 6 To edit the table map, in the **Table Map** tab, select the table map and click **Edit Table Map**. In the Table Map Creation dialog box:

a) Change the default value.
b) Change the values for QoS Group and Discard Class.
c) Change the value to set MPLS or CoS attributes.
d) Click **Add**.
e) Click **Finish**.

Egress Queue Scheduling

The CPT system supports Weighted Round Robin (WRR) and Low Latency Queueing (LLQ). Queueing is based on the class based classification done at egress. LLQ prioritizes and ensures low latency to the traffic in queues configured to be in LLQ, and the remaining traffic is scheduled using WRR.

Note Queue depth is not configurable. Each queue has a minimum depth of 25600 bytes and maximum depth of 1048576 bytes.

For information on egress LLQ, see Egress LLQ, on page 442.

For information on egress bandwidth, see Egress Bandwidth, on page 444.

For information on egress shaping, see Egress Shaping, on page 447.

For information egress Bandwidth Remaining Ratio (BRR) or Bandwidth Remaining Percent (BRP), see Egress Bandwidth Remaining Ratio and Bandwidth Remaining Percent, on page 449.

Egress LLQ

Applications which are latency sensitive require handling of data with least possible delay within the system. In the Cisco CPT system, low latencies are guaranteed by using strict priority scheduling at various congestion points and egress.

LLQ Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS egress LLQ on a Cisco CPT system are as follows:

- The **priority** command enables the rate-limit option to ensure that a particular rate is not exceeded. However, in the Cisco CPT system, egress rate limiting is achieved using shapers that can cause additional delays. Therefore, it is advised to ensure that for LLQ traffic, rate limiting is done at ingress, and the rates specified at egress are just placeholders that are never exceeded. Exceeding the rate limit at egress would mean increased latencies for LLQ traffic.
- The **priority** command is supported only under class-map with qos-group 3 or 7 as the match criteria and multicast-priority class.

To configure LLQ using Cisco IOS commands, see DLP-J201 Configuring Egress LLQ Using Cisco IOS Commands, on page 442.

To configure LLQ using CTC, see Step 9.b in DLP-J194 Setting Policy Class Actions Using CTC, on page 422.

DLP-J201 Configuring Egress LLQ Using Cisco IOS Commands

Purpose	This procedure explains how to configure egress LLQ using Cisco IOS commands
Tools/Equipment	None

Prerequisite Procedures	Step 1 to Step 5 of DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 414
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**policy map** *policy-map-name* **Example:** Router(config)# policy-map policy1	Creates or modifies a traffic policy and enters the policy-map configuration mode. The *policy-map-name* specifies the name of the traffic policy, which can have a maximum of 40 alphanumeric characters.
Step 4	**class** {*class-name* | **class-default**} **Example:** Router(config-pmap)# class class_qos_1	Specifies the name of the traffic class to which this policy applies and enters the policy-map class configuration mode, where: • *class-name*—Name of a predefined class included in the service policy. • **class-default**—Specifies that the policy applies to the default traffic class.
Step 5	**priority** *bandwidth value* **Example:** Router(config-pmap-c)# priority 10000	Provides strict priority to a class of traffic belonging to the policy-map. Specifies the maximum bandwidth usage by a traffic class through the use of a token bucket algorithm. The *bandwidth value* is in kbps, and can range from 1 to 10000000. **Note** The **priority** *bandwidth value* command is just an example of one of the priority commands that can be used. For a list of other priority commands, see Table 19: Priority (LLQ) Commands, on page 444.
Step 6	end **Example:**	Exits the configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	Router(config-pmap-c)# end	

The following table provides the priority commands:

Table 19: Priority (LLQ) Commands

Command	Description
priority *bandwidth value* **Example:** Router(config-pmap-c)# priority 10000	Provides strict priority to a class of traffic belonging to the policy-map. Specifies the maximum bandwidth usage by a traffic class through the use of a token bucket algorithm. The *bandwidth value* is in kbps, and can range from 1 to 10000000.
priority **Example:** Router(config-pmap-c)# priority	This command provides low-latency queuing without specifying the rate limiter.
priority percent *x%* **Example:** Router(config-pmap-c)# priority 10%	Indicates that the rate of traffic that is given low latency handling is *x%* of the parent interface bandwidth or *x%* parent class CIR if policy not applied on an interface. The percentage can be a number from 1 to 100.

Examples: Egress LLQ

The following example shows how to configure priority queue at the egress:

```
Router# config terminal
Router(config)# policy-map Test1
Router(config-pmap)# class Test
Router(config-pmap-c)# priority 10000
```

Egress Bandwidth

Applications that require committed information rate (CIR) should reserve the CIR on a per-target basis at the egress. After configuring the CIR, the traffic rates are guaranteed to be met in case of congestion at the egress.

Egress Bandwidth Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS egress bandwidth on a CPT system are as follows:

- Bandwidth action is not supported on classes with qos-group 3 or 7 as the match criteria, or multicast-priority class.

- The **bandwidth** command cannot be used in combination with BRR or BRP in a class-map or a policy-map.
- The system does not validate the total CIR configured on all the targets for various congestion points. Therefore, it should be ensured that the total CIR configured does not exceed the total bandwidth available.
  - Total CIR configured for a 1 Gbps interface should not exceed 1 Gbps, which includes CIR in the policy applied on the interface and services on that interface.
  - Total CIR configured for a 10 Gbps interface should not exceed 10 Gbps, which includes CIR in the policy applied on the interface and services on that interface.
  - Total CIR for all the targets on a CPT 50 shelf should not exceed 9.882 Gbps; this is the least bandwidth for a CPT50 shelf in a scenario where only one of the interconnects for a CPT50 shelf is functional.
  - Total CIR on all the unicast targets on two SFP+ interfaces on a fabric card or two CPT 50 shelves that are connected to two SFP+ interfaces of the same fabric card should not exceed 13 Gbps.

To configure the egress bandwidth using Cisco IOS commands, see DLP-J202 Configuring Egress Bandwidth Using Cisco IOS Commands, on page 445.

To configure the egress bandwidth using CTC, see Step 9.b in DLP-J194 Setting Policy Class Actions Using CTC, on page 422.

DLP-J202 Configuring Egress Bandwidth Using Cisco IOS Commands

Purpose	This procedure explains how to configure egress bandwidth using IOS commands:
Tools/Equipment	None
Prerequisite Procedures	Step 1 to Step 5 of DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 414
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**policy map** *policy-map-name* **Example:** Router(config)# policy-map policy1	Creates or modifies a traffic policy and enters the policy-map configuration mode. The *policy-map-name* specifies the name of the traffic policy that can have a maximum of 40 alphanumeric characters.
Step 4	**class** {*class-name* | **class-default**} **Example:** Router(config)# class c3	Specifies the name of the traffic class to which this policy applies and enters the policy-map class configuration mode, where: • *class-name*—User-defined class name to which the policy applies. • **class-default**—Specifies that the policy applies to the default traffic class.
Step 5	**bandwidth** *bandwidth value* **Example:** Router(config-pmap-c)# bandwidth 10000	Specifies the amount of bandwidth in kbps to be assigned to the class. Implies that the class where this is applied is given a minimum bandwidth guarantee of *bandwidth value* in kbps. The amount of bandwidth configured should be large enough to also accommodate Layer 2 overheads. **Note** The **bandwidth** *bandwidth value* command is just an example of one of the bandwidth commands that can be used. For a list of other bandwidth commands, see Table 20: Bandwidth Commands, on page 446.
Step 6	end **Example:** Router(config-pmap-c)# end	Exits the configuration mode and returns to privileged EXEC mode.

The following table provides the bandwidth commands:

Table 20: Bandwidth Commands

Command	Description
bandwidth *bandwidth-value* **Example:** Router(config-pmap-c)# bandwidth 10000	Specifies the amount of bandwidth in kbps to be assigned to the class. Implies that the class where this is applied is given a minimum bandwidth guarantee of *bandwidth-value* kbps. The amount of bandwidth configured should be large enough to also accommodate Layer 2 overhead.

Command	Description
bandwidth percent *%* **Example:** Router(config-pmap-c)# bandwidth percent 20	Specifies the amount of bandwidth, in percentage from the available bandwidth, to be assigned to the class. The value ranges from 1 to 100.

Examples: Egress Bandwidth

This example shows how to configure minimum bandwidth guarantee at the egress:

```
Router# config terminal
Router(config)# policy-map Test
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth 10000
Router(config-pmap-c)# exit
```

Egress Shaping

Traffic shaping enables you to control the traffic going out of an interface in order to match its flow to the speed of the remote target interface and to ensure that the traffic conforms to policies contracted for it. Shaping can be used to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches.

Shaping is the process of delaying packets in queues to make them conform to a specified profile.

Egress Shaping Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS egress shaping on a CPT system are as follows:

- The **shaping** command is not supported on classes with qos-group 3 or 7 as the match criteria or multicast-priority class.
- Shape on a traffic class would mean buffering of traffic in the system memory, which could result in increased latencies for these streams.

To configure shaping at the egress using IOS commands, see DLP-J203 Configuring Egress Shaping Using Cisco IOS Commands, on page 447.

To configure shaping at the egress using CTC, see Step 9.b in DLP-J194 Setting Policy Class Actions Using CTC, on page 422.

DLP-J203 Configuring Egress Shaping Using Cisco IOS Commands

Purpose	This procedure explains how to configure egress shaping using Cisco IOS commands:
Tools/Equipment	None
Prerequisite Procedures	Step 1 to Step 5 of DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 414

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**class-map [match-any]** *class-map-name* **Example:** Router(config)# class-map class-interface-all	Creates a class map to be used for matching packets to a class.
Step 4	**policy map** *policy-map-name* **Example:** Router(config)# policy-map test2	*policy-map-name*—Name of the policy-map to configure.
Step 5	**class** *class-name* **Example:** Router(config-pmap)# class classtest	*class-name*—Name of a predefined class included in the service policy.
Step 6	**shape average** *cir value* **Example:** Router(config-pmap-c)# shape average 10000000	*cir value*—Average rate traffic shaping. The committed information rate (CIR) value ranges from 8000 to 10000000000 bps. **Note** The **shape average** *cir value* command is just an example of one of the shape commands that can be used. For a list of other shape commands, see Table 21: Traffic Shaping Commands, on page 449.
Step 7	end **Example:** Router(config-pmap-c)# end	Exits the configuration mode and returns to privileged EXEC mode.

Table 21: Traffic Shaping Commands, on page 449 provides the traffic shaping commands:

Table 21: Traffic Shaping Commands

Command	Description
shape average percent *%* **Example:** Router(config-pmap-c)# shape average percent 20	Shapes a class to a percent of visible bandwidth. • *%*—Percentage. The value should range from 1 to 100.
shape average *cir value* **Example:** Router(config-pmap-c)# shape average 10000000	Specifies the average rate traffic shaping. • *cir value*—CIR value in bps. The committed information rate (CIR) value ranges from 8000 to 10000000000 bps.

Examples: Egress Shaping

The following example shows traffic shaping on a main interface; traffic leaving interface gi36/1 is shaped at the rate of 10 Mb/s:

```
Router# enable
Router# configure terminal
Router(config)# class-map class-interface-all
Router(config-cmap)# match qos-group 1
Router(config-cmap)# exit
Router(config)# policy-map dts-interface-all-action
Router(config-pmap)# class class-interface-all
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# exit
Router(config)# interface gi36/1
Router(config-if)# service-policy output dts-interface-all-action
```

In the following example, the **shape average** command is applied at the parent level of an H-QoS policy-map:

```
Router# enable
Router# configure terminal
Router(config)# policy-map child2
Router(config-pmap)# class test
Router(config-pmap-c)# shape average 100000000
Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 300000000
Router(config-if)# service-policy child2
```

Egress Bandwidth Remaining Ratio and Bandwidth Remaining Percent

Bandwidth Remaining Ratio (BRR) or Bandwidth Remaining Percent (BRP) specifies the ratio or percentage of the bandwidth that is divided between targets when there is congestion. BRR indicates the ratio with which the various classes are serviced when parent target is scheduled. BRP indicates the bandwidth to be allocated to each class as a percentage of the allocation done to the parent target in a hierarchical QoS model.

Bandwidth Remaining Ratio and Bandwidth Remaining Percent Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS egress BRR or BRP on a CPT system are as follows:

- The **BRR and BRP** commands are not supported in combination with the **bandwidth** action in a class-map or a policy-map.
- The **BRR and BRP** command are not supported on classes with qos-group 3 or 7 as the match criteria as or multicast-priority class.

BRR is implemented on logical interfaces using hierarchical policy-maps.

To configure egress BRR or BRP using Cisco IOS commands, see DLP-J204 Configuring Egress Bandwidth Remaining Ratio or Bandwidth Remaining Percent Using Cisco IOS Commands, on page 450.

To configure egress BRR or BRP using CTC, see Step 9.b in DLP-J194 Setting Policy Class Actions Using CTC, on page 422.

DLP-J204 Configuring Egress Bandwidth Remaining Ratio or Bandwidth Remaining Percent Using Cisco IOS Commands

Purpose	This procedure explains how to configure egress BRR or BRP using Cisco IOS commands
Tools/Equipment	None
Prerequisite Procedures	Step 1 to Step 5 of DLP-J192 Configuring Ingress Policing Using Cisco IOS Commands, on page 414
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**policy map** *policy-map-name* **Example:** Router(config)# policy-map policy1	Creates or modifies a traffic policy and enters the policy-map configuration mode. The *policy-map-name* specifies the name of the traffic policy, which can have a maximum of 40 alphanumeric characters.

	Command or Action	Purpose
Step 4	**class** {*class-name* | **class-default**} **Example:** Router(config-pmap)# class c3	Specifies the name of the predefined traffic class to which this policy applies and enters the policy-map class configuration mode, where: • *class-name*—User-defined class name to which the policy applies. • **class-default**—Specifies that the policy applies to the default traffic class.
Step 5	**bandwidth remaining ratio** *ratio* **Example:** Router(config-pmap-c)# bandwidth remaining ratio 2	Specifies a bandwidth-remaining ratio for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to non priority queues. The value should be between 1 to 127. **Note** The **bandwidth remaining percent** *x%* can be used instead of the **bandwidth remaining ratio** *ratio* command to configure BRP. For details on bandwidth remaining percent command, see Table 22: Bandwidth Remaining Ratio and Bandwidth Remaining Percent Commands, on page 451.
Step 6	end **Example:** Router(config-pmap-c)# end	Exits the configuration mode and returns to privileged EXEC mode.

The following table provides the bandwidth remaining ratio or percent commands:

Table 22: Bandwidth Remaining Ratio and Bandwidth Remaining Percent Commands

Command	Description
bandwidth remaining percent *x%* **Example:** Router(config-pmap-c)# bandwidth remaining percent 20	Specifies that the class where the command is specified should be given x% of the excess bandwidth, where excess bandwidth is the bandwidth in excess of all the minimum bandwidth guarantees of all the classes at the same level. The value should range from 1 to 100.
bandwidth remaining ratio *ratio* **Example:** Router(config-pmap-c)# bandwidth remaining ratio 2	Specifies a bandwidth-remaining ratio for class-level or sub interface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to non priority queues. The value should be between 1 to 127.

Examples: Egress Bandwidth Remaining Ratio

The following example shows how to configure bandwidth remaining ratio at the egress:

```
Router(config)# policy-map BRR
Router(config-pmap)# class Test1
Router(config-pmap-c)# bandwidth remaining ratio 10
Router(config-pmap-c)# exit
Router(config-pmap)# class Test2
Router(config-pmap-c)# bandwidth remaining ratio 20
Router(config-pmap-c)# exit
Router(config-pmap)# class Test3
Router(config-pmap-c)# bandwidth remaining ratio 30
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)#bandwidth remaining ratio 40
```

The following example shows how to verify the bandwidth remaining ratio at the egress:

```
Router# show policy-map BRR
```

```
Building configuration...
Current configuration : 209 bytes
!
policy-map BRR
 class Test1
  bandwidth remaining ratio 10
 class Test2
  bandwidth remaining ratio 20
 class Test3
  bandwidth remaining ratio 30
 class class-default
  bandwidth remaining ratio 40
!
end
```

Examples: Egress Bandwidth Remaining Percent

The following example shows how to configure bandwidth remaining percent at the egress:

```
Router(config)#policy-map BRP
Router(config-pmap)#class Test1
Router(config-pmap-c)#bandwidth remaining percent 10
Router(config-pmap-c)#exit
Router(config-pmap)# class Test2
Router(config-pmap-c)# bandwidth remaining percent 20
Router(config-pmap-c)# exit
```

The following example shows how to verify the bandwidth remaining percent at the egress:

```
Router# show policy-map BRP
```

```
!
policy-map BRP
 class Test1
  bandwidth remaining 10 (%)
 class Test2
  bandwidth remaining 20 (%)
!
```

DLP-J205 Monitoring and Verifying QoS Configuration Using Cisco IOS Commands

Purpose	This procedure explains how to display configuration of class maps and policy maps using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	Configuring QoS on a CPT system
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show class-map** **Example:** Router# show class-map	(Optional) Displays all class maps and their matching criteria.
Step 3	**show policy-map** *policy-map-name* **class** *class-name* **Example:** Router# show policy-map policy1 class class1	(Optional) Displays the configuration for the specified class of the specified policy map. • Enter the policy map name and the class name.
Step 4	**show policy-map** **Example:** Router# show policy-map	(Optional) Displays the configuration of all classes for all existing policy maps.
Step 5	**show policy-map interface** *interface-type interface-number* **Example:** Router# show policy-map interface TenGigabitEthernet 4/1	(Optional) Displays the statistics and the configurations of the input and output policies that are attached to an interface. • Enter the interface type and number.

	Command or Action	Purpose
Step 6	**show table-map** **Example:** Router# show table-map Table Map t1	(Optional) Displays the configuration of existing Table Map. • Enter the interface type and number.
Step 7	exit **Example:** Router# exit	Exits class-map configuration mode and returns to privileged EXEC mode. **Note** It will take approximately 20 minutes to get the actual or output rate which is equal to the configured rate when there is traffic .

Examples: Monitoring and Verifying QoS Configuration

This example shows how to display the class-map information for a specific class map using the **show class-map** command:

```
Router# show class-map ipp5

class Map match-any ipp5 (id 1)
match ip precedence 5
```

This example shows how to display the policy map information using the **show policy-map** command:

```
Router(config)# show policy-map

policy-map testchildOR
 class childOR
   police  100000000
policy-map parentOR
 class class-default
  police 500000000
  service-policy testchildOR
```

This example shows how to display the policy map information using the **show table-map** command:

```
Router(config)# show table-map

 Table Map t1
map from 1,1 to 1
default 0
```

DLP-J206 Monitoring and Verifying QoS Configuration Using CTC

Purpose	This procedure displays configuration of class maps and policy maps using CTC.
Tools/Equipment	None
Prerequisite Procedures	Configuring QoS on a CPT system

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

Procedure

Step 1 Complete the "NTP-J22 Log into CTC, on page 15" procedure at a node where you want to verify QoS configuration.

Step 2 In the node view, right-click the Fabric or Line card and choose **Open Packet Transport System View**. The Packet Transport System View screen appears.

Step 3 Click the **Maintenance** tab.

Step 4 From the left pane, click **IOS** and click **Open IOS Connection**. The IOS interface screen appears.

Step 5 Enter the user name and password.

Step 6 Enter one of the following show commands:

- **show class-map**
- **show policy-map** *policy-map-name* **class** *class-name*
- **show policy-map**
- **show policy-map interface** *interface-type interface-number*

Step 7 Press **Enter.** The output is displayed.

NTP-J66 Load or Store Class Maps, Table Maps, or Policy Maps Using CTC

Purpose	This procedure explains how to load or store class maps, table maps, or policy maps present in one node into another node in the network.
Tools/Equipment	None
Prerequisite Procedures	• Create a class-map • Create a policy-map • Create a table-map
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

Step 1 Complete the "NTP-J22 Log into CTC, on page 15" procedure at a node.

Step 2 In the node view, click the **Layer2+** tab.

Step 3 From the left pane, click **Provisioning**.

Step 4 Click the **QoS** tab .

Step 5 To load the maps from a node:

a) Click any one of tabs—**Class Map**, **Table Map** or **Policy Map**.
b) Click **Load**. The Load Maps From Selected Node dialog box appears.
c) Select the node from the drop-down list and click **Load**. The maps are displayed on the screen.
d) Select the map(s) that you want load and click **OK**. The selected maps are loaded.

Step 6 To store the maps in a node:

a) Click any one of tabs—**Class Map**, **Table Map** or **Policy Map**.
b) Click **Store**. The Store Maps To Selected Node dialog box appears.
c) Select the node in which you want to store the maps.
d) Select the maps that you want to store and click **Store**. The confirmation dialog box appears.
e) Click **OK**. The selected maps are stored on the selected node.

Understanding Multicast QoS

In the CPT system, multicast traffic at egress is queued differently than the unicast traffic. At the egress of the CPT system, a maximum of two multicast queues can be configured on each interface—a priority queue and a non-priority queue. In addition to configuring multicast QoS per interface, multicast guarantee can be configured on the interlink interfaces between the fabric or line card and the CPT 50 shelf, for priority and non-priority multicast traffic. The definition of priority traffic for multicast is the same as for unicast, that is, the traffic-class explained in Egress Classification , on page 432 shall be used to differentiate priority traffic from non-priority traffic in the egress hardware.

Note Multicast QoS configurations use predefined multicast classes of which only two classes are supported. They are multicast-priority and multicast-normal. Multicast-priority class matches any multicast traffic with qos-group set to 3 or 7, whereas multicast-normal class matches any multicast-traffic with qos-group set to 0, 1, 2, 4, 5 or 6.

Note Configurations at the egress show classification based on predefined multicast class-maps; however, the CPT system differentiates priority and non priority multicast traffic using traffic-class set at the ingress.

Multicast QoS Restrictions

The following restrictions apply to multicast QoS:

- Multicast QoS is possible only per interface
- Only two queues are available at each interface for multicast traffic—one for priority and one for non-priority

Static Configurations for Multicast Traffic on a Card

The following example displays the static configuration for multicast traffic on a card:

```
Router# show class-map
```

```
Router# show run class-map
Building configuration...

Current configuration : 170 bytes
!
class-map match-any multicast-normal
match access-group name multicast-normal
class-map match-any multicast-priority
match access-group name multicast-priority
end

Router#
```

Dynamic Configurations for Multicast Traffic on a Card

Note Multicast class-maps are preconfigured. Multicast traffic with qos-group 3 or 7 is considered as priority multicast traffic, and rest of the multicast traffic is considered as normal multicast traffic. You can only decide the bandwidth allocation for CIR, PIR and priority traffic.

The following example shows how to configure multicast QoS at egress:

```
Router(config)# policy-map out2
Router(config-pmap)# class multicast-normal
Router(config-pmap-c)# bandwidth percent 20
Router(config-pmap-c)# shape average percent 30
Router(config-pmap-c)# class multicast-priority
Router(config-pmap-c)# priority percent 15
Router(config-pmap-c)# end
Router#
Router# show policy-map
```

```
  Policy Map out2 (oid: 69874467, cgid: FFFFFFFF)
    Class multicast-normal (classid: 1, cid: FFFFFFFF)
       (Action oid: 933929563)
      bandwidth 20 (%)
       (Action oid: 1470800472)
      Average Rate Traffic Shaping
      cir 30%
    Class multicast-priority (classid: 2, cid: FFFFFFFF)
       (Action oid: 910587090)
      priority 15 (%)
```

```
Router#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int ten4/1
Router(config-if)#service-policy output out2
Router(config-if)#
```

Hierarchical QoS

The Cisco CPT system supports hierarchical quality-of-service (H-QoS) that includes QoS at multiple levels in a hierarchy.

Ingress H-QoS

An H-QoS policy can be attached to an interface or a service instance. The number of levels is limited to two for an input QoS policy, where the parent level denotes the policy target and the child level denotes the QoS traffic class:

- Only the default class, that is, **class-default** is allowed at the parent level. User-defined classes are not supported at the parent level.
- Only the **police** action command is allowed at the parent level. Marking action is not supported. Also, remarking actions are not supported for the parent policer. In effect, a hierarchical policy is configured to achieve only hierarchical metering.

Egress H-QoS

The targets for H-QoS at egress are interface, service instance, and queue. There is support for up to three levels of hierarchy with the following configurations:

- Single-level policy on an interface with multicast classes for multicast traffic and class-default for unicast traffic.
- Two-level policy on a service instance with class-default queuing at parent and per qos-group queuing at the child level.

The various combination of hierarchical and flat policies are in this table.

Serial Number	EVC Policy	EVC Policy Level	EVC Class Actions (parent level[1])	EVC Classes Supported (parent level)	EVC Class Actions (child level[2])	EVC Classes Supported (child level)
1	Flat	1	—	—	• Bandwidth • Shape • Priority	Unicast classes[3]
2	Hierarchical	2	• Bandwidth • Shape	Class-default	• Bandwidth • Shape • Priority	Unicast classes

	Interface Policy	Interface Policy Level	Interface Class Actions (parent level)	Interface Classes Supported (parent level)	Interface Class Actions (child level)	Interface Classes Supported (child level)
3	Flat	1	—	—	• Bandwidth • Shape • Priority	All classes [4]
4	Flat	1	—	—	• Bandwidth • Shape • Priority (with multicast class)	Class-default and multicast classes[5]
5	Hierarchical	2	• Bandwidth • Shape • Priority (with multicast class)	Class-default and multicast classes	• Bandwidth • Shape • Priority	Unicast classes

1 Higher level in a hierarchical policy.
2 Lower level in a hierarchical policy or the only level in a flat policy.
3 All qos-group based classes and class-default.
4 Unicast and multicast classes.
5 Multicast-priority and multicast-normal classes.

The above table lists the possible level one and level two hierarchies. The possible combination of interface and EVC level policies are as follows:

- Entries of serial number 1 and 4 resulting in a two-level hierarchy
- Entries of serial number 2 and 4 resulting in a three-level hierarchy

EVCS QoS Support

The Ethernet Virtual Connection Services (EVCS) uses the concept of service instances and EVC (Ethernet Virtual Circuit). A service instance is the instantiation of an EVC on a given interface on a given router. An EVC is an end-to-end representation of a single instance of a Layer 2 service being offered by a provider to a customer. It embodies the different parameters on which the service is being offered.

QoS works with the following EVC combinations:

- One TAG case
- Two TAG case
- One TAG to one TAG
- One TAG to two TAG
- Two TAG to one TAG
- Two TAG to two TAG
- One TAG termination
- Two TAG termination
- Tag to Tag translation

Restrictions and Usage Guidelines

The restrictions and usage guidelines to configure QoS on EVCS are as follows:

- CoS marking or remarking is not supported for service instances defined using VLAN ranges or “encapsulation default”.
- CoS marking or remarking action applies to both inner and outer tags, when inner tag is modified within the system. In all other cases, the marking or remarking action that the user specifies is limited only to the outer tag.

Note For information on EVC, see Understanding Ethernet Virtual Circuit, on page 132.

QoS Support on Port-Channel

This section explains the QoS on the Port-Channel feature support for ingress and egress.

QoS Support on Port-Channel at Ingress

The QoS on the port-channel feature enables QoS service-policies to be applied at the ingress on the following targets:

- Port-channel member link
- Port-channel main interface
- Port-channel EVC

For a policy-map attached to a port-channel main interface, ingress traffic coming from any member link is subjected to the same policy-map configured on the port-channel main interface. If no policy-map is configured on the port-channel main interface, ingress traffic from the member-link is subjected to the policy-map attached to the:

- EVC through which the traffic is flowing.

- Member link.

The QoS policy can be attached to a port-channel even if the member interfaces are on different cards. Policy-maps cannot coexist on a port-channel main interface, EVC, and member link at the same time.

Restrictions and Usage Guidelines QoS Support on Port-Channel at Ingress

The policer configuration is enforced only on a single card and not across cards in a distributed link aggregation group (LAG). However, member links might span across cards.

QoS Support on Port-Channel at Egress

The QoS on port-channel feature enables QoS service-policies to be applied at the egress on the following targets:

- Port-channel main interface
- Port-channel EVC

Note Egress service policy is not supported on the port-channel member link.

At egress, if a policy is applied on both the port-channel main interface and the EVC, only class- default queuing is possible on the port-channel main interface for unicast traffic. In such a scenario, all the EVC traffic is subjected to both port-channel QoS and port channel EVC QoS. In the context of EVCs for which a policy is not applied, only port channel QoS is applied.

Restrictions and Usage Guidelines QoS Support on Port-Channel at Egress

A policy that is applied on a port channel is not applicable to the aggregate port channel traffic. It is applicable only on a per port-channel member basis. Therefore, if a configuration that shapes all the traffic to ***x*** **Mbps** on the port-channel main interface exists, it gets translated to a configuration that shapes each member link to ***x*** **Mbps**. As a result, the aggregate traffic on the port channel could be up to ***n*** times ***x*** **Mbps**, where *n* is the number of links in the port-channel.

QoS Statistics

Enhanced performance monitoring displays QoS statistics on the CPT card interfaces. QoS statistics are supported at the 1GE interface, 10GE interface, and service instance levels. At the ingress, only byte counters are supported and at the egress, both packet and byte counters are supported.

Statistics supported at ingress are shown in this table:

Table 23: Statistics at Ingress

Statistics Collected	1GE Interface	10GE Interface	EVC	Port Channel Interface
Classification statistics— Byte Counters	Yes	Yes	Yes	Yes

Statistics Collected	1GE Interface	10GE Interface	EVC	Port Channel Interface
Marking Statistics—Byte Counters	No	No	No	Yes
Policing Statistics—Byte Counters	Supported with limitations: • In a 2-color policer, both green and red byte counters are supported. • In a 3-color policer, green/non-green or non-red/red are supported	Supported with limitations: • In a 2-color policer, both green and red byte counters are supported • In a 3-color policer, green and non-green or non-red and red are supported	No	Yes

Statistics supported at egress are shown in this table:

Table 24: Statistics at Egress

Statistics Collected	1GE Interface	10GE Interface	EVC	Port Channel Interface
Classification statistics - Packet and Byte Counters	Yes	Yes	Yes	Yes
Queuing Statistics—(Accepted or Dropped) Packet and Byte Counters	Yes	Yes	Yes	Yes
Match Statistics—Packet and Byte Counters	Yes	Yes	Yes	Yes

Retrieving Egress QoS Statistics

Egress QoS statistics can be viewed by using show commands. To display this information, use one of the commands provided in the following table:

Table 25: Egress QoS Statistics Commands

Command	Purpose
show policy-map interface *interface name*	Displays the QoS statistics available for an interface.
show policy-map interface *interface name service instance number*	Displays the QoS statistics available for a service instance created under Gigabit Ethernet or 10 Gigabit Ethernet interface.

Examples: Egress QoS Statistics

The following example displays statistics available for an interface at the egress:

```
Router# show policy-map interface TenGigabitEthernet4/4
```

```
TenGigabitEthernet4/4
       Service-policy output: p22 (oid: 1310866, cgid: FFFFFFFF)

   Class-map: c1 (match-any)   (oid: 65536, cid: FFFFFFFF)
     0 packets, 0 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: qos-group 1 (oid: 65537, fid: FFFFFFFF)
       0 packets, 0 bytes
       5 minute rate 0 bps
     (ActionGrp Local Id: 1)
     Queueing
     queue limit 28201 packets
     (queue depth/total drops/no-buffer drops) 100/0/0
     (pkts output/bytes output) 0/0
     (Action oid: 65538)
     bandwidth 800000 kbps

   Class-map: class-default (match-any)   (oid: 131072, cid: 00000639)
     0 packets, 0 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: any  (oid: 131073, fid: 0000063A)
     (ActionGrp Local Id: 0)
```

The following example displays the QoS statistics available for a service instance created under 10 Gigabit Ethernet interface:

```
Router# show policy-map interface TenGigabitEthernet4/3 service instance 2
```

```
 TenGigabitEthernet4/3: EFP 2

 Service-policy output: p22 (oid: 2307558214, cgid: FFFFFFFF)

   Class-map: c1 (match-any)   (oid: 65536, cid: FFFFFFFF)
     0 packets, 0 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: qos-group 1 (oid: 65537, fid: FFFFFFFF)
       0 packets, 0 bytes
       5 minute rate 0 bps
     (ActionGrp Local Id: 1)
     Queueing
```

```
    queue limit 28201 packets
    (queue depth/total drops/no-buffer drops) 100/0/0
    (pkts output/bytes output) 0/0
    (Action oid: 65538)
    bandwidth 800000 kbps

  Class-map: class-default (match-any)   (oid: 131072, cid: 00000639)
    0 packets, 0 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: any  (oid: 131073, fid: 0000063A)
    (ActionGrp Local Id: 0)

    queue limit 324314 packets
    (queue depth/total drops/no-buffer drops) 100/0/0
    (pkts output/bytes output) 0/0
```

QoS Configuration Guidelines for the Cisco CPT 50 Shelf

Traffic that is sent to the CPT 50 shelf can either be unicast or multicast traffic. When multicast traffic is sent to a multicast group or a service-instance that is configured on 1 GE interfaces of the Cisco CPT 50 shelf, a copy of each multicast frame is sent to the CPT 50 shelf. The CPT 50 shelf replicates this multicast frame on the 1 GE interfaces based on the multicast group or a service-instance configuration. This replication process saves the bandwidth usage on the interconnect link for the CPT 50 shelf. However, there are two congestion points that must be configured with the bandwidth that should be reserved for unicast and multicast traffic. The congestion points are:

- Interlink CongestionRestrictionsExample, on page 464
- CPT 50 Shelf 1 GE Interface CongestionExampleExampleExampleRestriction, on page 465

Interlink Congestion

The first congestion point for unicast and multicast traffic is the interlink interface on the fabric or the line card to which the CPT50 shelf is connected. A policy-map with multicast classes must be used to reserve the multicast bandwidth for the CPT 50 shelf.

When multicast-normal and multicast-priority classes are configured with bandwidth, shape, or priority for multicast traffic, the unicast traffic is automatically shaped to the value derived as follows:

Unicast shaper for lowest interlink interface = maximum data bandwidth on the interlink interface – (bandwidth for multicast-normal + bandwidth for multicast-priority), where

- Maximum data bandwidth on the interlink interface = link bandwidth - control bandwidth
- Link bandwidth is 10 Gbps and control bandwidth is 118 Mbps

Therefore, the maximum data bandwidth on the interlink interface = 9.882 Gbps

Restrictions

- All multicast traffic meant for the CPT50 shelf uses the lowest interlink interface. There is no load balancing for multicast traffic that is meant for the CPT50 shelf. Therefore, the total multicast bandwidth for the CPT 50 shelf is limited by the maximum data bandwidth as stated above, which is 9.882 Gbps.

- There should be a shaper configured to the same rate as the bandwidth configured for multicast-normal class. This ensures that the sum of multicast and unicast traffic sent to a CPT 50 shelf does not exceed the interlink bandwidth.
- The same interface-level policy should be applied on all the interlink interfaces meant for the CPT 50 shelf. This is to ensure that the QoS minimum guaranteed bandwidth works even in the event of an interlink failure.

Example

To reserve 250 Mbps bandwidth for normal priority multicast and 120 Mbps bandwidth for priority multicast for a CPT50 shelf, use this configuration:

```
!
policy-map interlink-mc-policy
 class multicast-normal
  bandwidth 250000
  shape average 250000000
 class multicast-priority
  priority 120000
!
Apply the policy on the interconnect port on the fabric or line card
!
interface TenGigabitEthernet4/1
 no ip address
 no keepalive
 fanout-group 37
 service-policy output interlink-mc-policy
 l2protocol peer cdp lacp
 l2protocol forward stp vtp dtp pagp dot1x
end
```

CPT 50 Shelf 1 GE Interface Congestion

The second congestion point is at the one Gigabit Ethernet interface of the CPT50 shelf, where unicast traffic and the replicated multicast traffic converge. A policy-map is used to configure the unicast and multicast bandwidth reservations. There are three possible combinations that can be used:

- Interface level policy for both multicast and unicast queuing—In this case, there is no specific QoS requirement per service-instance or EVC, but there is a requirement per queue at the interface level as shown in this example.

Example

```
!
policy-map egress
 class q1
  bandwidth 155000
 class q2
  bandwidth 100000
 class q3
  priority 150000
 class q4
  bandwidth 25000
 class q5
  shape average 50000000
  bandwidth 50000
 class q6
  bandwidth 70000
 class q7
  priority 180000
 class multicast-normal
  bandwidth 80000
 class multicast-priority
```

```
  priority 150000
 class class-default
  bandwidth 40000
!
```

- Interface level queuing for multicast traffic and CIR for unicast traffic—In order to ensure that unicast traffic receives the required CIR, the unicast non-priority and priority traffic CIR must be configured separately. Use a two-level hierarchical policy as shown in the example below to ensure that the requirements are met.

Example

```
!
policy-map port-level-child
 class q7
  priority 170000
class q7
  priority 50000

 class class-default
  bandwidth 550000
!

!
policy-map port-parent
 class multicast-normal
  bandwidth 80000
 class multicast-priority
  priority 150000
 class class-default
  service-policy port-level-child
!
```

- Interface level queuing for multicast traffic and CIR/PIR for unicast queues at service-instance or the EVC level—In this configuration, ensure that the sum of unicast and multicast CIR/PIR do not exceed the interface bandwidth.

Example

```
!
policy-map port-default
 class multicast-normal
  bandwidth 80000
 class multicast-priority
  priority 150000
 class class-default
  shape average 770000000
!
end

!
policy-map evc1
 class q1
  bandwidth 30000
 class q2
  bandwidth 50000
 class q3
  priority 75000
 class q4
  bandwidth 12500
 class q5
  shape average 50000000
  bandwidth 25000
 class q6
  bandwidth 90000
```

```
 class q7
  priority 90000
 class class-default
  bandwidth 10000
!
end
```

Restriction

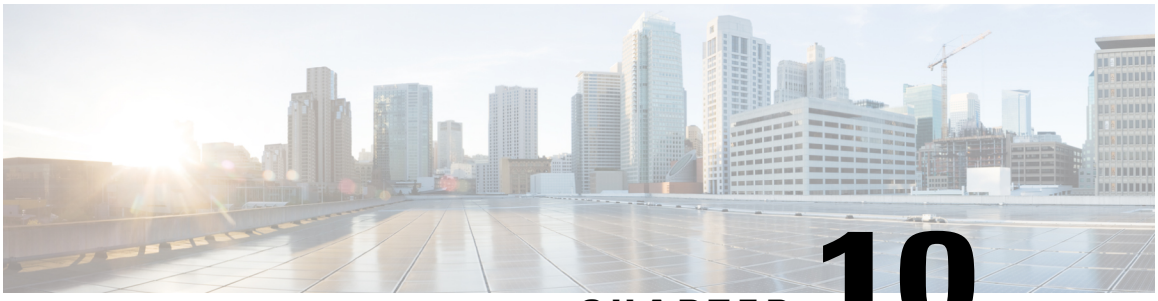
If a service-instance or EVC level CIR is present, configure a shaper on the class-default in the policy-map applied on the interface. This ensures that the unicast and multicast traffic converging at the CPT 50 shelf 1 GE interface do not interfere with each other.

Interlink QoS

The user can prioritize the traffic from 1 GE ports of CPT 50 to CPT 200 or CPT 600 when there is congestion on the 10 GE interlink ports. Each 1 GE port has eight queues to control the incoming traffic and each queue is marked with a qos-group value ranging from 0 to 7.

CPT provides strict priority queuing mode. In this mode, two queues with the qos-group value set to 7 and 3 share the highest priority and a low latency, and are scheduled on a round-robin basis if there is traffic on both these queues. The remaining six queues are configured in strict priority scheduling mode in the following order: Qos-group 6, 5, 4, 2, 1, and 0.

For information on how to configure strict priority, refer to the NTP-J72 Create a Fan–Out–Group Using CTC, on page 34 procedure.



CHAPTER 10

Configuring High Availability

This chapter describes Stateful Switchover, Cisco Nonstop Forwarding, and In-Service Software Upgrade. This chapter also describes the configuration procedures.

This chapter includes the following topics:

Stateful Switchover

Stateful switchover (SSO) ensures state synchronization and non-disruptive switchover from an active to a standby fabric card, thereby providing an increase in both system and network availability. In SSO, the standby fabric card is fully initialized and is ready to assume control from the active fabric card when the switchover occurs.

SSO is particularly useful at the network edge. Traditionally, core routers protect against network faults using router redundancy and mesh connections that allow traffic to bypass failed network elements. SSO provides protection for network edge devices with dual route processors (RPs) that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.

Because SSO maintains stateful protocol and application information, the user session information is maintained during a switchover. Line cards continue to forward network traffic with no loss of sessions, providing improved network availability.

SSO provides faster switchover by fully initializing and configuring the standby fabric card, and by synchronizing state information, which reduces the time required for routing protocols to converge. The CPT 50 panel that is connected directly to the active fabric card will be disconnected due to SSO.

SSO takes advantage of fabric card redundancy to increase network availability. SSO establishes one of the fabric cards as the active card and the other fabric card is established as the standby card, and then synchronizes critical state information between them. Following an initial synchronization between the two cards, SSO dynamically maintains state information between them.

SSO enables the system to keep all the sessions of HA-aware protocols up during a switchover. This ensures that the services are not affected during switchovers and upgrades.

Note Carrier Packet Transport (CPT) supports only the SSO redundancy mode.

Cisco Nonstop Forwarding (NSF) works with SSO to minimize the network downtime following a switchover. The main objective of NSF is to continue forwarding IP packets following a fabric card switchover.

Prerequisites for SSO

Two fabric cards must be installed on the CPT 200 and CPT 600 shelf.

Restrictions for SSO

General Restrictions

For NSF support, neighboring routers must run NSF-enabled images, though SSO need not be configured on the neighboring device.

Switchover Process Restrictions

If the active fabric card fails before the standby fabric card is ready to switchover, both the fabric cards are reset.

Platform Restrictions or Considerations

- CPT supports only the SSO redundancy mode.
- The active fabric card reload operation causes a switchover.

Card Crash During SSO

When the fabric card or line card crashes during SSO, the crash handler shuts down the laser signal on the front ports of the card. The far end detects loss of signal on this path and switches to the protection path if available.

SSO Synchronization

Fabric Card Synchronization

Both the fabric cards must be running the same configuration so that the standby fabric card is always ready to assume control if the active fabric card fails.

To achieve the benefits of SSO, synchronize the configuration information from the active fabric card to the standby fabric card at startup and whenever changes to the active fabric card configuration occur. This synchronization occurs in two separate phases:

- When the standby fabric card is booting, the configuration information is synchronized in bulk from the active fabric card to the standby fabric card.
- When configuration or state changes occur, an incremental synchronization is conducted from the active fabric card to the standby fabric card.

Note The CPT 50 panels connected to the active fabric card and the active fabric card are reset during the switchover.

Bulk Synchronization During Initialization

When a system with SSO is initialized, the active fabric card performs a chassis discovery (discovery of the number and type of line cards and fabric cards in the system) and parses the startup configuration file.

The active fabric card then synchronizes this data to the standby fabric card and instructs the standby fabric card to complete its initialization. This method ensures that both fabric cards contain the same configuration information.

Even though the standby fabric card is fully initialized, it interacts only with the active fabric card to receive incremental changes to the configuration files as they occur.

Incremental Synchronization

After both the fabric cards are fully initialized, any further changes to the running configuration or active states are synchronized to the standby fabric card as they occur. Active fabric card states are updated as a result of processing protocol information, external events (such as the interface coming up or down), user configuration commands (using CLI commands or CTC), or other internal events.

Line Card State Synchronization

Changes to the line card states are synchronized to the standby fabric card. Line card state information is initially obtained during bulk synchronization of the standby fabric card. Following bulk synchronization, line card events received at the active fabric card are synchronized to the standby fabric card.

The following line card states apply to line cards during switchover:

- Line cards are not reset during switchover.
- Line cards are not reconfigured during switchover.
- Line cards do not generate alarms during switchover.
- Subscriber sessions are not lost during switchover.

Note During the complete power cycle of the fully loaded CPT 200 or CPT 600 chassis with large scale service configurations, sometimes the state of the cards will show as Empty Slot. The line cards boot properly once the database is completely loaded.

Counters and Statistics Synchronization

The various counters and statistics maintained in the active fabric card are reset during a switchover and are not synchronized with the standby fabric card.

Redundancy Modes

CPT supports only the SSO redundancy mode.

SSO Redundancy Mode

In SSO redundancy mode, the standby fabric card is fully initialized. The active fabric card dynamically synchronizes the startup and running configuration changes to the standby fabric card, which means that the standby fabric card need not be reloaded and reinitialized. SSO supports synchronization of line card, protocol, and application state information between the fabric cards.

Switchover Operation

During switchover, the system control and routing protocol execution are transferred from the active fabric card to the standby fabric card.

Switchover Conditions

The following conditions cause a switchover from the active fabric card to the standby fabric card:

- The active fabric card fails.
- Online removal of the active fabric card automatically forces a stateful switchover to the standby fabric card.
- Forced switchover from the active fabric card to the standby fabric card through CTC or CLI.
- The **reload** command causes a switchover from the active fabric card to the standby fabric card.
- Keepalive or Heartbeat failure causes a switchover from the active fabric card to the standby fabric card.

  The fabric card polls the peer cards at regular intervals to check whether the cards are connected to the system. If the fabric card does not receive a message within a specific duration from its peer card, the fabric card assumes that the peer card is down. The default duration for the fabric card to receive the Keepalive indication message is 9000 milliseconds.

Switchover Exceptions

The following conditions will not cause a switchover from the active fabric card to the standby fabric card:

- The standby fabric card reset doest not cause a switchover from the active fabric card to the standby fabric card.
- The Dual TNC card reset does not cause a switchover from the active fabric card to the standby fabric card.

NTP-J17 Manage SSO

Purpose	This procedure manages SSO configuration.
Tools/Equipment	CPT 600 / CPT 200
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J46 Perform a Manual Switchover Using CTC, on page 473
- DLP-J47 Verify SSO Configuration Using Cisco IOS Commands, on page 474
- DLP-J48 Verify SSO Configuration Using CTC, on page 475
- DLP-J49 Troubleshoot SSO Using Cisco IOS Commands, on page 479

Stop. You have completed this procedure.

DLP-J46 Perform a Manual Switchover Using CTC

Purpose	This procedure performs a manual switchover from the active fabric card to the standby fabric card using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

The fabric card can be in one of the following states during the switchover.

- Active
- Failed
- Loading
- Standby

The active fabric card moves to one of the above states after the switchover.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to switchover from the active fabric card to the standby fabric card.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Maintenance** tab.

Step 5 From the left pane, click **High-Availability**.

Step 6 In the Fabric Cards area, click **Switch** to perform a manual switchover from the active fabric card to the standby fabric card.

Step 7 Click **YES**.

Step 8 Return to your originating procedure (NTP).

DLP-J47 Verify SSO Configuration Using Cisco IOS Commands

Purpose	This procedure allows you to verify that SSO is configured using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show redundancy** [**clients** | **config-sync** | **counters** | **domain** | **history** | **idb-sync-history** | **interlink** | **states** | **switchover** | **trace**] **Example:** Router# show redundancy	Verifies that SSO is configured on the networking device.

	Command or Action	Purpose
Step 3	Return to your originating procedure (NTP).	—

DLP-J48 Verify SSO Configuration Using CTC

Purpose	This procedure verifies SSO configuration using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to verify the SSO configuration.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Maintenance** tab.

Step 5 From the left pane, click **IOS**.

Step 6 Click **Open IOS Connection**. The IOS Login dialog box appears.

Step 7 Enter the user name and password.

Step 8 Enter show redundancy command at the prompt.

Step 9 Press **Enter**. The output is displayed.
The redundant system information, current processor, and peer processor information appears in the output area. The configured redundancy mode is SSO if an entry in the output reads as `Configured Redundancy Mode = SSO`.

Step 10 Return to your originating procedure (NTP).

Examples of SSO Configuration

Verify that SSO Is Configured

The following examples verify that SSO is configured on the device.

```
Router# show redundancy
```

```
Redundant System Information :
------------------------------
       Available system uptime = 18 hours, 44 minutes
       Switchovers system experienced = 1
       Standby failures = 0
       Last switchover reason = active unit failed

       Hardware Mode = Duplex
       Configured Redundancy Mode = SSO
       Operating Redundancy Mode = SSO
       Maintenance Mode = Disabled
       Communications = Up

Current Processor Information :
------------------------------
        Active Location = slot 5
        Current Software state = ACTIVE
        Uptime in current state = 10 minutes
        Image Version = Cisco IOS Software, ONS NGXP Software
(NGXP-ADVIPSERVICES-M), Experimental Version
        15.1(20110216:101154) [ios_ngxp_dev-georgeti-ios_ngxp_dev.pkg
100]
        Copyright (c) 1986-2011 by Cisco Systems, Inc.
        Compiled Wed 16-Feb-11 16:59 by georgeti
        Configuration register = 0x101

Peer Processor Information :
----------------------------
        Standby Location = slot 4
        Current Software state = STANDBY HOT
        Uptime in current state = 8 minutes
        Image Version = Cisco IOS Software, ONS NGXP Software
(NGXP-ADVIPSERVICES-M), Experimental Version
        15.1(20110215:170703) [ios_ngxp_dev-sathk-ngxp_Feb16th 109]
        Copyright (c) 1986-2011 by Cisco Systems, Inc.
        Compiled Wed 16-Feb-11 15:12 by sathk
        Configuration register = 0x101 (will be 0x8001 at next reload)
```

```
Router# show redundancy states
```

```
     my state = 13  -ACTIVE
     peer state = 8 -STANDBY HOT
     Mode = Duplex
     Unit ID = 4

    Redundancy Mode (Operational) = SSO
    Redundancy Mode (Configured)  = SSO
```

```
    Redundancy State               = SSO
    Manual Swact = enabled
    Communications = Up

    client count = 47
    client_notification_TMR = 30000 milliseconds
    keep_alive TMR = 9000 milliseconds
    keep_alive count = 0
    keep_alive threshold = 10
    RF debug mask = 0x0
```

```
Router# show redundancy history
```

```
00:00:12 client added: Redundancy Mode RF(29) seq=60
00:00:12 client added: IfIndex(139) seq=61
00:00:12 client added: CHKPT RF(25) seq=68
00:00:12 client added: NGXP Platform RF(4500) seq=76
00:00:12 client added: NGXP CardIntf Mgr RF(4505) seq=77
00:00:12 client added: Event Manager(77) seq=84
00:00:12 client added: Network RF Client(22) seq=109
00:00:12 client added: XDR RRP RF Client(71) seq=135
00:00:12 client added: CEF RRP RF Client(24) seq=136
00:00:12 client added: RFS RF(520) seq=157
00:00:12 client added: Config Sync RF client(5) seq=159
```

```
Router# show redundancy switchover history
```

```
Index  Previous  Current  Switchover         Switchover
       active    active   reason             time
-----  --------  -------  ----------------   --------------------
   1       4        5     active unit failed 10:58:11 PDT Wed Jun 7 2000
```

Verify SSO Protocols and Applications

Enter the **show redundancy** command with the **client** keyword to display the list of applications and protocols that have registered as SSO protocols or applications. You can also verify the list of supported line protocols.

```
Router# show redundancy clients
```

```
 clientID = 29       group_id = 1    clientSeq = 60       Redundancy Mode
 RF
 clientID = 139      group_id = 1    clientSeq = 61       IfIndex
 clientID = 25       group_id = 1    clientSeq = 68       CHKPT RF
 clientID = 4500     group_id = 1    clientSeq = 76       NGXP Platform
RF
 clientID = 4505     group_id = 1    clientSeq = 77       NGXP CardIntf
Mgr RF
 clientID = 4504     group_id = 1    clientSeq = 78       NGXP PB Manager

 clientID = 4501    group_id = 1    clientSeq = 79      NGXP HAL Resource
 Manager
 clientID = 4502     group_id = 1    clientSeq = 80       NGXP NMS Manager

 clientID = 4503     group_id = 1    clientSeq = 81       NGXP Mac Table
 Management
 clientID = 77       group_id = 1   clientSeq = 84       Event Manager
```

```
 clientID = 78       group_id = 1    clientSeq = 106      TSPTUN HA
 clientID = 22       group_id = 1    clientSeq = 109      Network RF
Client
 clientID = 75       group_id = 1    clientSeq = 126      Tableid HA
 clientID = 71       group_id = 1    clientSeq = 135      XDR RRP RF
Client
 clientID = 24       group_id = 1    clientSeq = 136      CEF RRP RF
Client
 clientID = 146      group_id = 1    clientSeq = 138      BFD RF Client
 clientID = 402      group_id = 1    clientSeq = 156      TPM RF client
 clientID = 520      group_id = 1    clientSeq = 157      RFS RF
 clientID = 5        group_id = 1    clientSeq = 159      Config Sync RF
 client
 clientID = 49       group_id = 1    clientSeq = 181      HDLC
 clientID = 72       group_id = 1    clientSeq = 182      LSD HA Proc
 clientID = 113      group_id = 1    clientSeq = 183      MFI STATIC HA
Proc
 clientID = 290      group_id = 1    clientSeq = 184      MPLS TP HA
 clientID = 204      group_id = 1    clientSeq = 188      ETHER INFRA RF
 clientID = 226      group_id = 1    clientSeq = 196      LACP
 clientID = 20       group_id = 1    clientSeq = 203      IPROUTING NSF
RF client
 clientID = 34       group_id = 1    clientSeq = 218      SNMP RF Client
 clientID = 35       group_id = 1    clientSeq = 228      History RF
Client
 clientID = 90      group_id = 1    clientSeq = 240      RSVP HA Services

 clientID = 54       group_id = 1    clientSeq = 256      SNMP HA RF
Client
 clientID = 73       group_id = 1    clientSeq = 257      LDP HA
 clientID = 76       group_id = 1    clientSeq = 258      IPRM
 clientID = 57       group_id = 1    clientSeq = 259      ARP
 clientID = 83       group_id = 1    clientSeq = 293      AC RF Client
 clientID = 82       group_id = 1    clientSeq = 294      CCM RF
 clientID = 84       group_id = 1    clientSeq = 296      AToM manager
 clientID = 85       group_id = 1    clientSeq = 298      SSM
 clientID = 280      group_id = 1    clientSeq = 299      ST PW OAM
 clientID = 212      group_id = 1    clientSeq = 309      REP Protocol
 clientID = 151      group_id = 1    clientSeq = 322      IP Tunnel RF
 clientID = 94       group_id = 1    clientSeq = 323      Config Verify
RF client
 clientID = 506      group_id = 1    clientSeq = 327      Igmp Snooping
 clientID = 3099     group_id = 1    clientSeq = 347      ISSU process
 clientID = 4005    group_id = 1    clientSeq = 350     ISSU Test Client

 clientID = 93       group_id = 1    clientSeq = 354      Network RF 2
Client
 clientID = 141     group_id = 1    clientSeq = 364      DATA DESCRIPTOR
 RF CLIENT
 clientID = 4020     group_id = 1    clientSeq = 393      IOS Config
ARCHIVE
 clientID = 4021     group_id = 1    clientSeq = 394      IOS Config
ROLLBACK
```

Possible SSO Problem Situations

This section describes the possible situations in which SSO troubleshooting may be needed.

- The standby fabric card was reset, but no error message was displayed. To display a log of SSO events and clues as to why a switchover or other event occurred, enter the **show redundancy history** command on the newly active fabric card:

  Router# **show redundancy history**

DLP-J49 Troubleshoot SSO Using Cisco IOS Commands

Purpose	This procedure allows you to troubleshoot the SSO feature using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

The following commands do not have to be entered in any specific order.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**crashdump-timeout** [*mm* | *hh:mm*] **Example:** router(config-red)# crashdump-timeout	Sets the longest time that the newly active fabric card waits before reloading the previously active fabric card.
Step 3	**show redundancy** [**clients** | **config-sync** | **counters** | **domain** | **history** | **idb-sync-history** | **interlink** | **states** | **switchover** | **trace**] **Example:** Router# show redundancy states	Displays the redundancy configuration mode of the fabric card. Also, displays information about the number of switchovers, system uptime, processor uptime, and redundancy state, and reasons for any switchovers.

	Command or Action	Purpose
Step 4	**show version** **Example:** Router# show version	Displays the image information for each fabric card.
Step 5	Return to your originating procedure (NTP).	—

SSO Aware Protocols and Applications

Protocols and applications that support SSO must be HA-aware. A feature or protocol is HA-aware if it maintains, either partially or completely, undisturbed operation through a fabric card switchover. State information for HA-aware protocols and applications is synchronized from the active fabric card to the standby fabric card to achieve stateful switchover for those protocols and applications.

The following protocols and applications are SSO aware:

- EVC, MVR, IGMP Snooping, MAC Address Table
- REP
- QoS
- LAG and LACP
- OSPF
- MPLS, LDP, RSVP-TE, L2VPN, BFD

Active-Active Data Path

Active-Active Data Path (AADP) is supported. AADP refers to the load sharing between the two fabric cards.

The redundant fabric cards run in an active-standby control model. However, both the fabric cards have ports that carry active traffic.

The active and standby fabric cards are used for load balancing the traffic that is received and destined for line cards. With dual fabric cards, the traffic from one line card to the other line card can be up to 40 Gbps. With a single fabric card, the traffic from one line card to the other line card cannot exceed 32 Gbps. However, the traffic between two fabric cards can be up to 32 Gbps for CPT 600 shelf, and up to 40 Gbps for CPT 200 shelf.

AADP provides the following benefits for the CPT System:

- Reduces the overall cost per 10 GE port.
- Increases the trunk capacity of the CPT system.
- Builds redundancy with rings or tunnels across the fabric cards.

Nonstop Forwarding

Cisco Express Forwarding

A key element of NSF is packet forwarding. In Cisco networking devices, packet forwarding is provided by Cisco Express Forwarding (CEF). Cisco Express Forwarding maintains the Forwarding Information Base (FIB), and uses the FIB information that was current at the time of the switchover to continue forwarding packets during a switchover. This feature eliminates downtime during the switchover.

During the normal NSF operation, Cisco Express Forwarding on the active fabric card synchronizes its FIB and adjacency databases with the FIB and adjacency databases on the standby fabric card. On switchover of the active fabric card, the standby fabric card initially has FIB and adjacency databases that are mirror images of those on the active fabric card. The packet forwarding continues after a switchover as soon as the interfaces and a data path are available.

Nonstop Forwarding

Nonstop Forwarding (NSF) works with the Stateful Switch Over (SSO) feature to minimize the amount of time a network is unavailable following a switchover. The main objective of the NSF is to continue forwarding IP packets after the switchover of the active fabric card.

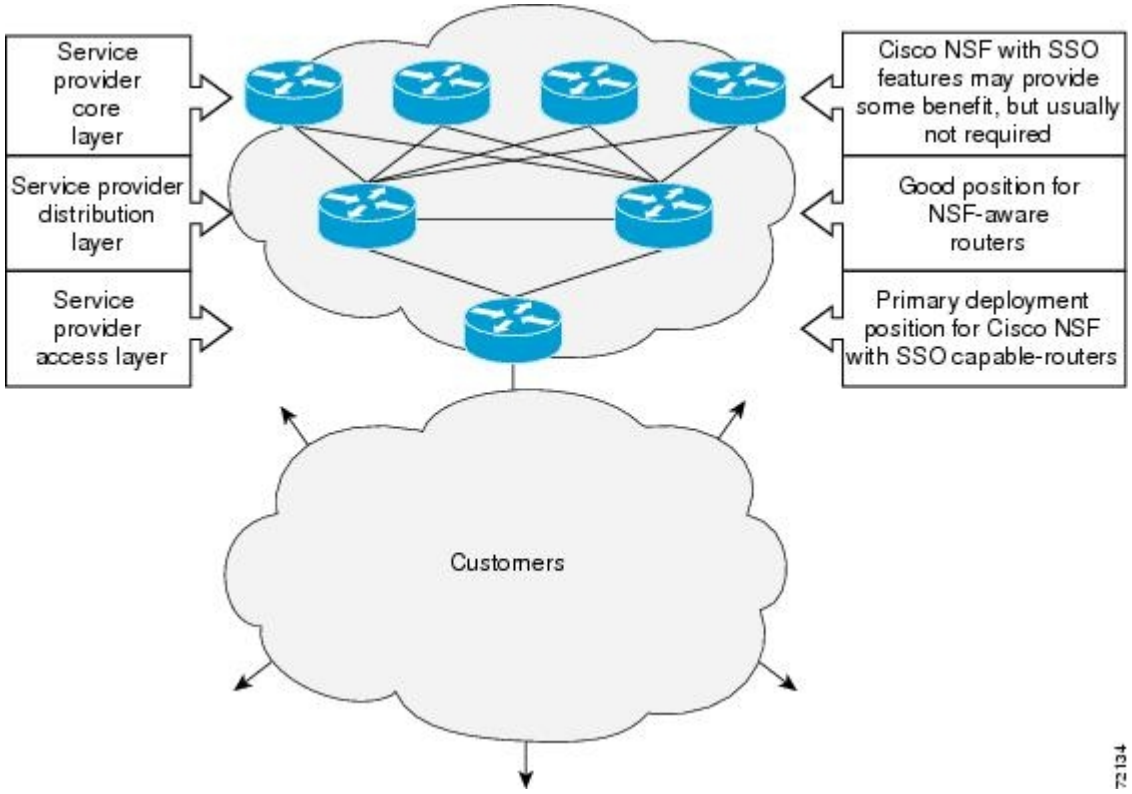
When a networking device restarts, all the routing peers of that device usually detect that the device went down and then came back up. This down-to-up transition results in routing flap, which could spread across multiple routing domains. Routing flaps caused by routing restarts create routing instabilities, which are detrimental to the overall network performance. NSF helps to suppress routing flaps and improves the network stability.

NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With NSF, peer networking devices do not experience routing flaps. Data traffic is forwarded through intelligent line cards while the standby fabric card assumes control from the failed active fabric card during a switchover. The ability of line cards to remain up during the switchover and to be kept current with the FIB on the active fabric card is key to NSF operation. The CPT 50s connected to the fabric card will have an impact on the traffic.

Note CPT does not support forwarding IP packets in hardware and supports forwarding only in software.

The following figure illustrates how SSO is typically deployed in service provider networks. In this example, NSF with SSO is primarily at the access layer (edge) of the service provider network. A fault at this point can result in loss of service for enterprise customers requiring access to the service provider network.

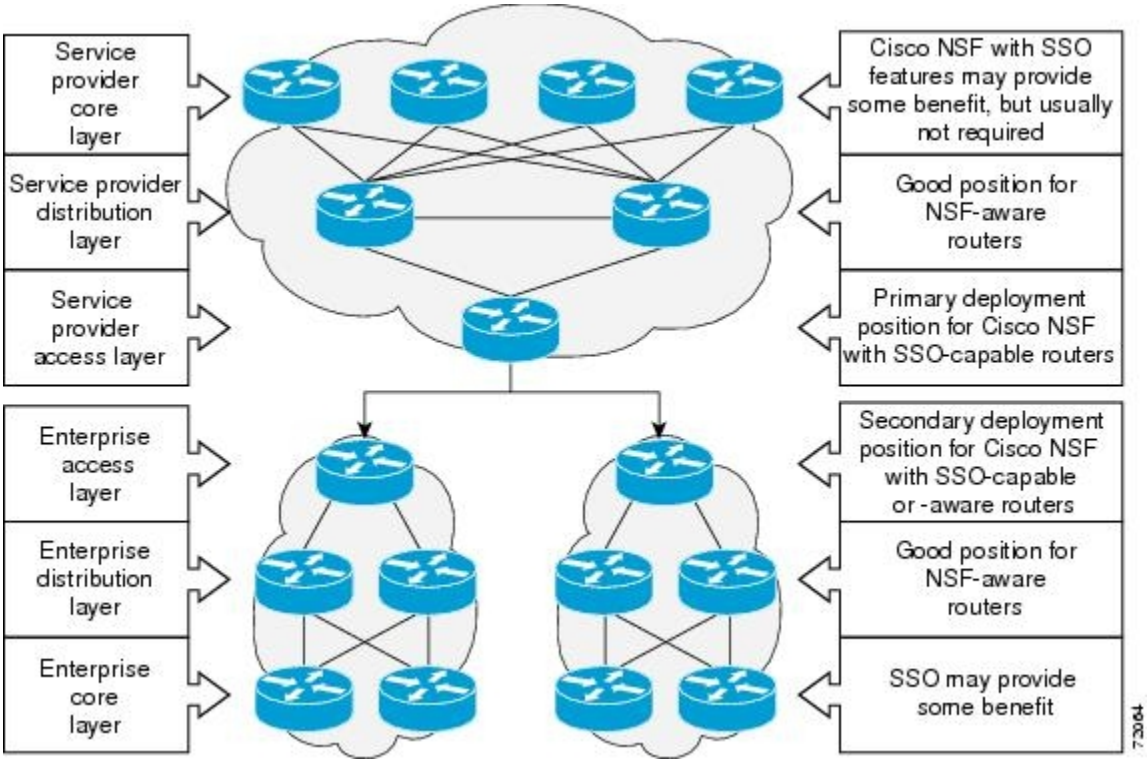
Figure 68: NSF with SSO Network Deployment: Service Provider Networks



Additional levels of availability may be gained by deploying NSF with SSO at other points in the network where a single point of failure exists. The following figure illustrates an optional deployment strategy that applies NSF with SSO at the enterprise network access layer. In this example, each access point in the enterprise

network represents another single point of failure in the network design. In the event of a switchover or a planned software upgrade, enterprise customer sessions would continue uninterrupted throughout the network.

Figure 69: NSF with SSO Network Deployment: Enterprise Networks



Prerequisite for NSF

- Ensure that Distributed Cisco Express Forwarding is operational.

Benefits of NSF

The NSF feature has the following benefits:

- Improved network availability—NSF continues to forward network traffic and application state information so that user session information is maintained after a switchover.
- Overall network stability—Network stability may be improved with the reduction in the number of route flaps that had been created when routers in the network failed and lost their routing tables.
- Prevents routing flaps—Because the NSF continues to forward network traffic in the event of a switchover, routing flaps are avoided.
- No loss of user sessions—User sessions established prior to the switchover are maintained.

NSF Routing

Each protocol depends on Cisco Express Forwarding to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables. After the routing protocols have

converged, Cisco Express Forwarding updates the FIB table and removes stale route entries. Cisco Express Forwarding updates the line cards with the new FIB information.

The routing protocols run only on the active fabric card, and they receive routing updates from the neighboring routers. After a switchover, the routing protocols request that the NSF-aware neighboring devices send the state information to help rebuild the routing tables.

Note During the NSF operation, the routing protocols depend on Cisco Express Forwarding to continue forwarding the packets while the routing protocols rebuild the routing information.

OSPF Operation

When an OSPF NSF-capable router performs a fabric card switchover, it must perform two tasks to resynchronize its link state database with its OSPF neighbors. Firstly, it must relearn the available OSPF neighbors on the network without causing a reset of the neighbor relationship. Secondly, it must reacquire the contents of the link state database for the network.

After the fabric card switchover, the NSF-capable router sends an OSPF NSF signal to the neighboring NSF-aware devices. The neighboring network devices recognize this signal as a clue that the neighbor relationship with this router must not be reset. As the NSF-capable router receives signals from other routers on the network, it can begin to rebuild its neighbor list.

When neighbor relationships are reestablished, the NSF-capable router begins to resynchronize its database with all of its NSF-aware neighbors. At this point, the routing information is exchanged between the OSPF neighbors. After this exchange is complete, the NSF-capable device uses the routing information to remove stale routers and update the RIB and FIB with the new forwarding information. The OSPF protocols are then fully converged.

Note The OSPF NSF requires that all the neighboring network devices be NSF-aware. If a NSF-capable router discovers that it has non NSF-aware neighbors on a particular network segment, it will disable NSF capabilities for that segment. Other network segments composed entirely of NSF-capable or NSF-aware routers will continue to provide NSF capabilities.

NSF Device Modes

Cisco had implemented the proprietary Cisco NSF. The Graceful OSPF Restart feature supports IETF NSF for OSPF processes in multivendor networks. The NSF device modes of operation common to the Cisco and IETF NSF implementations are as follows:

- Restarting mode—In this mode, the OSPF device is performing nonstop forwarding recovery because of the fabric card switchover.
- Helper mode—Also known as NSF–awareness. In this mode, the neighboring device is restarting and helping in the NSF recovery.

NTP-J18 Manage NSF

Purpose	This procedure manages NSF configuration.

Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J50 Verify Cisco Express Forwarding NSF Using Cisco IOS Commands, on page 485
- DLP-J51 Configure OSPF for NSF Using Cisco IOS Commands, on page 486
- DLP-J52 Verify OSPF for NSF Using Cisco IOS Commands, on page 487
- DLP-J53 Troubleshoot NSF Using Cisco IOS Commands, on page 489

Stop. You have completed this procedure.

DLP-J50 Verify Cisco Express Forwarding NSF Using Cisco IOS Commands

Purpose	This procedure verifies that Cisco Express Forwarding is NSF capable using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

The Cisco Express Forwarding NSF feature operates by default. Configuration of Cisco Express Forwarding NSF is not necessary.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show cef state** **Example:** Router# show cef state	Displays the state of Cisco Express Forwarding on a networking device.
Step 3	Return to your originating procedure (NTP).	—

DLP-J51 Configure OSPF for NSF Using Cisco IOS Commands

Purpose	This procedure configures OSPF for NSF using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** Router(config)# router ospf 12	Enables an OSPF routing process, and places the router in router configuration mode.
Step 4	**nsf** {**cisco** | **ietf**} **Example:** Router(config-router)# nsf cisco	Enables Cisco NSF or IETF NSF support on the router.

	Command or Action	Purpose
Step 5	Return to your originating procedure (NTP).	—

DLP-J52 Verify OSPF for NSF Using Cisco IOS Commands

Purpose	This procedure verifies OSPF for NSF using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config** **Example:** Router# show running-config	Displays the contents of the current running configuration file.
Step 3	**show ip ospf nsf** **Example:** Router# show ip ospf nsf	Displays NSF information about OSPF routing processes.
Step 4	Return to your originating procedure (NTP).	—

Examples of the NSF Configuration

Verify that Cisco Express Forwarding Is NSF-capable

The following example shows how to verify that Cisco Express Forwarding is NSF-capable.

```
show cef state
```

```
CEF Status:
 RP instance
 common CEF enabled
IPv4 CEF Status:
 CEF enabled/running
 dCEF enabled/running
 CEF switching enabled/running
 universal per-destination load sharing algorithm, id 7E0E20AE
RRP state:
 I am standby RRP:                   no
 RF Peer Presence:                   yes
 RF Peer Comm reached:               yes
 RF Peer Config done:                yes
 RF Progression blocked:            unblocked (blocked for 00:00:00.588)

 Redundancy mode:                    sso(3)
 CEF NSF sync:                       enabled/running

CEF ISSU Status:
  FIBHWIDB broker
    Slot(s): 3 5 40 (0x10000000028) (grp 0x37003204) - Not ISSU aware.
  FIBIDB broker
    Slot(s): 3 5 40 (0x10000000028) (grp 0x37003204) - Not ISSU aware.
  FIBHWIDB Subblock broker
    Slot(s): 3 5 40 (0x10000000028) (grp 0x37003204) - Not ISSU aware.
  FIBIDB Subblock broker
    Slot(s): 3 5 40 (0x10000000028) (grp 0x37003204) - Not ISSU aware.
  Adjacency update
    Slot(s): 3 5 40 (0x10000000028) (grp 0x37003204) - Not ISSU aware.
  IPv4 table broker
    Slot(s): 3 5 40 (0x10000000028) (grp 0x37003204) - Not ISSU aware.
  CEF push
    Slot(s): 3 5 40 (0x10000000028) (grp 0x37003204) - Not ISSU aware.
```

Configure OSPF for NSF

The following example shows how to configure OSPF for NSF on a networking device.

```
Router# configure terminal
Router(config)# router ospf 400
Router(config-router)# nsf
```

Verify OSPF for NSF

To verify OSPF for NSF, check whether the NSF is configured on the SSO enabled networking device. Verify that "nsf" appears in the OSPF configuration of the SSO-enabled device by entering the **show running-config** command:

```
Router# show running-config
```

```
router ospf 120
log-adjacency-changes
nsf
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 1
network 192.168.40.0 0.0.0.255 area 2
```

Next, use the **show ip ospf** command to verify that NSF is enabled on the device.

```
Router# show ip ospf
```

```
Routing Process "ospf 1" with ID 192.168.2.1 and Domain ID 0.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Non-Stop Forwarding enabled, last NSF restart 00:02:06 ago (took 44 secs)
Area BACKBONE(0)
Number of interfaces in this area is 1 (0 loopback)
Area has no authentication
SPF algorithm executed 3 times
```

DLP-J53 Troubleshoot NSF Using Cisco IOS Commands

Purpose	This procedure troubleshoots NSF using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

The following commands do not have to be entered in any specific order.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ospf nsf** [**detail**] **Example:** Router# debug ospf nsf [detail]	Displays debugging messages related to OSPF NSF commands.
Step 3	**show cef nsf** **Example:** Router# show cef nsf	Displays the current NSF state of Cisco Express Forwarding on both the active and standby fabric cards.
Step 4	**show cef state** **Example:** Router# show cef state	Displays the Cisco Express Forwarding state on a networking device.
Step 5	**show ip cef** **Example:** Router# show ip cef	Displays entries in the Forwarding Information Base (FIB) that are unresolved, or displays a FIB summary.
Step 6	**show ip ospf** **Example:** Router# show ip ospf	Displays general information about OSPF routing processes.
Step 7	**show ip ospf neighbor** [**detail**] **Example:** Router# show ip ospf neighbor [detail]	Displays OSPF neighbor information on a per-interface basis.
Step 8	**show ip protocols** **Example:** Router# show ip protocols	Displays the parameters and current state of the active routing protocol process.
Step 9	Return to your originating procedure (NTP).	—

In-Service Software Upgrade

Software upgrade is an important consideration for high availability. CPT supports the In-Service Software Upgrade (ISSU) process to perform planned software upgrades within the HA system. ISSU provides the ability to perform a stateful upgrade even when both the fabric cards are of different versions. ISSU is built over the SSO infrastructure.

ISSU allows you to perform a software upgrade or downgrade while the system continues to forward packets. In most networks, planned software upgrades are a significant cause of downtime. ISSU takes advantage of the NSF with SSO and eliminates downtime associated with software upgrades by allowing changes while the system remains in service. ISSU lowers the impact that planned maintenance activities have on network service availability; there is less downtime and better access to critical systems.

The software upgrade is always done at the node level and not directly on the CPT cards. When the package is upgraded, CPT cards must also upgrade to the Cisco IOS image present in the new package. Reverting to the earlier version of the software must be done for all the cards in the shelf and not just for CPT cards.

The Transport Node Controller (TNC) card stores the required images in its flash memory and manages the software upgrade process for all the cards.

SSO and ISSU work together to ensure that the states and configuration of the CPT cards are maintained before and after the upgrade.

Note You can perform the ISSU using CTC and TL1 and not using Cisco IOS commands.

The ISSU message transformations between the active fabric card and the standby fabric card is supported. All the CPT components support the ISSU message transformations between the active fabric card and the standby fabric card.

The ISSU message transformations between the active fabric card and the standby fabric card is supported .The ISSU message transformations between the active fabric card and the line card is also supported. All the CPT components support the ISSU message transformations between the active fabric card and the line card except EVC and QoS components.

Prerequisites for ISSU

- Both the active and standby fabric cards must be available in the system.
- New and existing software images must be loaded on the TNC cards before starting the ISSU process.
- SSO and Cisco NSF must be configured and working properly.

Restrictions for ISSU

- Do not make hardware changes while performing an ISSU process.
- (Recommended) Perform upgrades only during a maintenance window.
- Do not enable new features that require configuration changes, during the ISSU process.

Upgrade Activities in ISSU

The following upgrade activities take place sequentially in a system that has a single fabric card. However, it is recommended that two fabric cards are used in the system.

1 The TNC card boots with the latest image.

2 The TNC card sends the upgrade request to the active fabric card.

3 The active fabric card predownloads its image and the images for the line card.

4 The active fabric card sends the predownload request sequentially to all the line cards based on the slot ID.

5 All the line cards predownload their images.

6 The active fabric card and the line cards reboot with the latest image.

The following upgrade activities take place sequentially in a system that has two fabric cards:

1 The TNC card boots with the latest image.

2 The TNC card sends the upgrade request to both the active and standby fabric cards.

3 The active and standby fabric cards predownload their images and the images for the line card.

4 The active fabric card sends the predownload request sequentially to all the line cards based on the slot ID.

5 All the line cards predownload their images.

6 The active fabric card sends the reboot request to the standby fabric card.

7 The standby fabric card reboots with the latest image.

8 When the standby fabric card reaches the hot standby state, the active fabric card reboots.

9 On upgrade to release 9.3.x, when the rebooted active fabric card joins as standby fabric card, the new active fabric card reloads all the line cards sequentially based on the slot ID.

10 When all the line cards are up, the active fabric card clears the Upgrade alarm on the TNC card.

Table 26: Line Card Reload During Upgrade

Source Release	Destination Release	Line Card Reload
9.5.x	9.5.x	All the line cards reload sequentially.
9.5.x	9.7	All the line cards reload sequentially.

Table 27: Line Card Reload During Downgrade

Source Release	Destination Release	Line Card Reload
9.7	9.5.x	All the line cards reload sequentially.
9.5.x	9.5.x	All the line cards reload sequentially.

Approximate ISSU Duration

CPT supports up to 2 fabric cards, 20 CPT 50 panels, and 4 line cards on a CPT 600 shelf.

Total upgrade time = Boot of TNC card with latest image + Fabric and line card image download on the fabric card + (24 * Predownload of line cards) + Boot of the standby fabric card + Boot of the active fabric card + (4 * Boot of line cards)

24=4 Line cards+16 CPT 50 panels in line card + 4 CPT 50 panels in 2 Fabric cards

Total Upgrade time = 3 minutes + 3 minutes + (24 * 30 seconds) + 6 minutes + 6 minutes + (4 * 5 minutes) = 50 minutes

The above upgrade duration is calculated based on average boot delays. The delays due to ROM MONitoring (ROMMON) and Field Programmable Gate Array (FPGA) upgrades are not accounted in this calculation.

Card Crash During ISSU

When the active fabric card crashes during the predownload of the line card, the standby fabric card becomes active and resumes the predownload process. There are two possible scenarios:

- If the crashed active fabric card recovers and reaches the hot-standby state, the fabric card reboots all the cards sequentially.
- If the crashed active fabric card does not recover, all the cards reboot at once resulting in loss of traffic during the boot duration.

ISSU Commands

The following commands display the ISSU status details of a client.

- **show issu capability**
- **show issu comp-matrix**
- **show issu endpoints**
- **show issu clients**
- **show issu sessions**
- **show issu entities**
- **show issu fsm**
- **show issu negotiated**
- **show issu message**

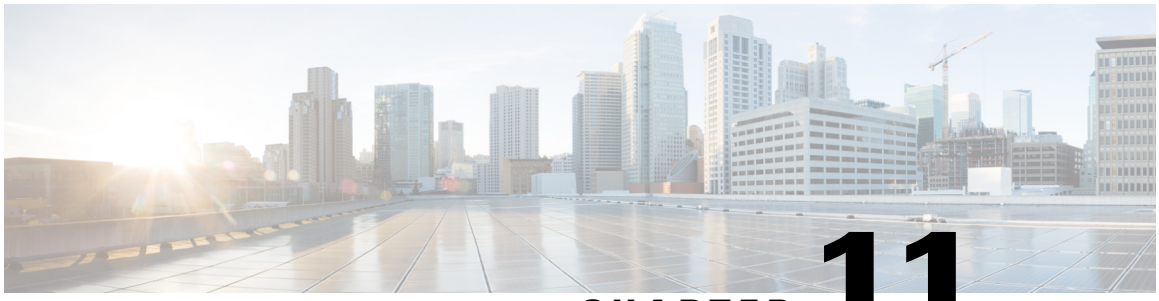
For more information on these commands, see the *Cisco CPT Command Reference Guide*.

Graceful Restart

LDP graceful restart protects traffic when an LDP session is lost. If an interface that supports a graceful-restart-enabled LDP session fails, MPLS LDP-IGP synchronization is still achieved on the interface while it is protected by graceful restart.

LDP graceful restart must be enabled for LDP to be HA compliant. Graceful restart helps to preserve the MPLS forwarding table entries built by LDP over a SSO.

LDP graceful restart must be enabled before establishing a LDP session. You can configure graceful restart through both CTC and Cisco IOS commands. See DLP-J134 Configure MPLS LDP Graceful Restart Using Cisco IOS Commands, on page 216 and DLP-J135 Configure MPLS LDP Graceful Restart Using CTC, on page 218 for more information.



CHAPTER 11

Configuring Resilient Ethernet Protocol

This chapter describes Resilient Ethernet Protocol (REP), REP configuration guidelines, VLAN load balancing, REP timers, and REP over EVC. This chapter also describes procedures to configure REP.

Understanding Resilient Ethernet Protocol

The Resilient Ethernet Protocol (REP) is a protocol that provides an alternative to Spanning Tree Protocol (STP) to support L2 resiliency, and fast switchover with Ethernet networks. REP provides a way to control network loops, handle link failures, and improve convergence time.

REP performs the following tasks:

- Controls a group of ports connected in a segment.
- Ensures that the segment does not create any bridging loops.
- Handles single link failure within the segment.
- Improves convergence time.
- Supports VLAN load balancing.

REP Configuration Procedures

The following procedures can be performed using Cisco IOS commands to configure REP:

- DLP-J32 Configure STCN on the Primary Edge Port Using Cisco IOS Commands, on page 508
- DLP-J38 Configure VLAN Load Balancing on the Primary Edge Port Using Cisco IOS Commands, on page 515
- DLP-J33 Configure Preemption Delay on the Primary Edge Port Using Cisco IOS Commands, on page 509
- DLP-J39 Configure the Preemption for VLAN Load Balancing Using Cisco IOS Commands, on page 517
- DLP-J42 Configure REP Link Status Layer Retries Using Cisco IOS Commands, on page 520
- DLP-J43 Configure the REP Link Status Layer Ageout Timer Using Cisco IOS Commands, on page 522
- DLP-J44 Configure REP over EVC Using a Cross–Connect Using Cisco IOS Commands, on page 525
- DLP-J45 Configure REP over EVC Using the Bridge Domain Using Cisco IOS Commands, on page 528
- Verify REP with EVC Configuration Using Cisco IOS Commands, on page 530

The following procedures can be performed using CTC to configure REP:

- DLP-J30 Configure REP Administrative VLAN Using CTC, on page 505
- DLP-J34 Create a Segment Using CTC, on page 511
- DLP-J35 Edit a Segment Using CTC, on page 513
- DLP-J40 Activate VLAN Load Balancing Using CTC, on page 518
- DLP-J41 Deactivate VLAN Load Balancing Using CTC, on page 519

Understanding REP Segments

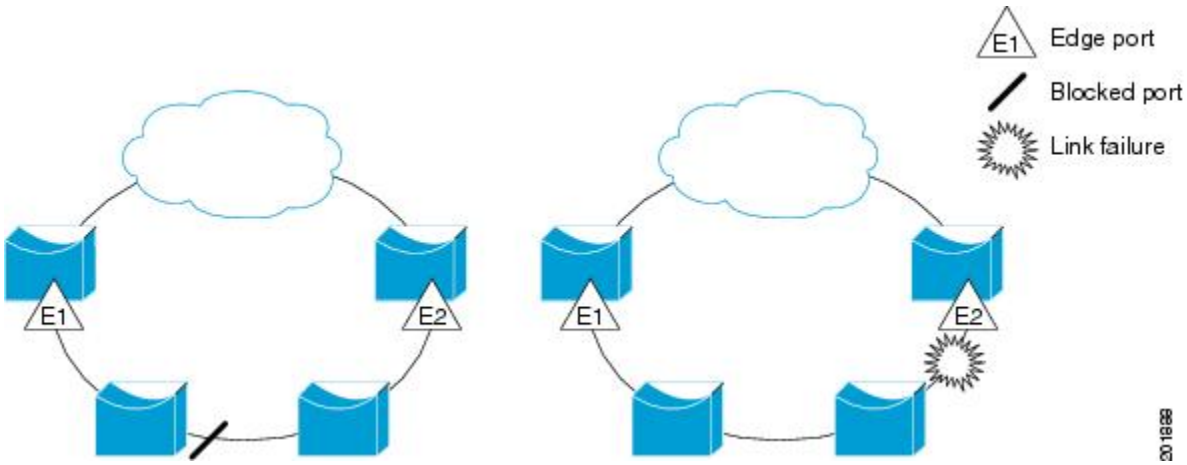
A REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (non-edge) segment ports and two user-configured edge ports. The two edge ports terminate the segments.

A router cannot have more than two ports that belong to the same segment, and each segment port can have only one external neighbor. A segment can go through a shared medium, but on any link only two ports can belong to the same segment. REP is supported only on Layer 2 interfaces.

Figure 70: REP Open Segments, on page 497 shows an example of a segment consisting of six ports spread across four switches. Ports E1 and E2 are configured as edge ports. When all ports are operational (as in the

segment on the left), a single port is blocked, shown by the diagonal line. When there is a failure in the network, the blocked port returns to the forwarding state to minimize network disruption.

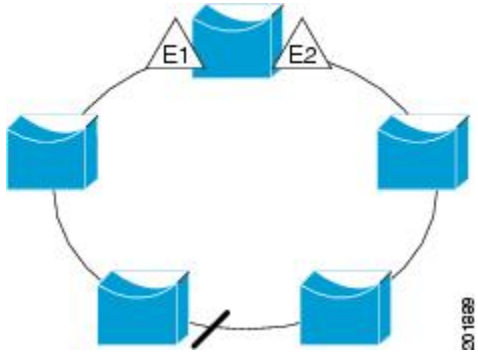
Figure 70: REP Open Segments



The segment shown in Figure 70: REP Open Segments, on page 497 is an open segment; there is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop and it is safe to connect the segment edges to any network. The traffic from a REP ring node toward the network cloud is sent to either of the edge nodes, depending on the location of the alternate port. If a failure is detected anywhere in the ring, the alternate port changes to a open port forwarding all traffic. This may cause the traffic being redirected to the other edge node depending on the fault location. It ensures that data flow is maintained between a particular REP node and the network cloud. If a failure occurs on any segment or any port on a REP segment, REP unblocks all the ports to ensure that connectivity is available through the other edge.

The segment shown in Figure 71: REP Ring Segment, on page 497, with both edge ports located on the same router, is a ring segment. In this configuration, there is connectivity between the edge ports through the segment. With this configuration, you can create a redundant connection between any two routers in the segment.

Figure 71: REP Ring Segment



Characteristics of REP Segments

REP segments have the following characteristics:

- If all the ports in the segment are operational, one port (referred to as the alternate port) blocks traffic for each VLAN. If VLAN load balancing is configured, two ports in the segment control the blocked state of VLANs.
- If one or more ports in a segment is not operational, causing a link failure, all ports forward traffic on all VLANs to ensure connectivity. The Failed ports are blocked for all traffic, while all the other ports in the ring stay in open state.
- In case of a link failure, the alternate ports are immediately unblocked. When the failed link comes up, a logically blocked port per VLAN is selected with minimal disruption to the network. When VLAN load balancing preemption timer is set, VLAN load balancing is automatically applied after the last failure has recovered. There are 2 alternate ports when VLAN load balancing takes effect.

Understanding Link Adjacency

REP does not use an end-to-end polling mechanism between edge ports to verify link integrity. It implements local link failure detection. When enabled on an interface, the REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. All VLANs are blocked on an interface until it detects the neighbor. After the neighbor is identified, REP determines which neighbor port should become the alternate port and which ports should forward traffic.

Each port in a segment has a unique port ID. When a segment port starts, the LSL layer sends packets that include the segment ID and the port ID. The port is declared as operational after it performs a three-way handshake with a neighbor in the same segment.

A segment port does not become operational under the following conditions:

- No neighbor port has the same segment ID.
- More than one neighbor port has the same segment ID.
- The neighbor port does not acknowledge the local port as a peer.

Each port creates an adjacency with its immediate neighbor. When the neighbor adjacencies are created, the ports negotiate to determine one blocked port for the segment, the alternate port. All other ports become unblocked.

Understanding Fast Convergence

A failure in a REP segment is noticed and propagated across the ring by LSL and HFL messages. LSL messages are sent hop by hop on the control plane, with each node receiving, processing, and forwarding LSL messages. This process is time-consuming.

HFL messages are flooded in the data plane across the ring on a preconfigured administrative VLAN, using a fixed multicast address. This results in each node receiving failure notifications instantaneously. Using HFL, traffic reconvergence is achieved fast, leading to insignificant loss of traffic on segment failure.

HFL messages are handled as data packets on the nodes in a ring which do not have the REP configured. The administrative VLAN is common to all the REP segments that are configured on a node.

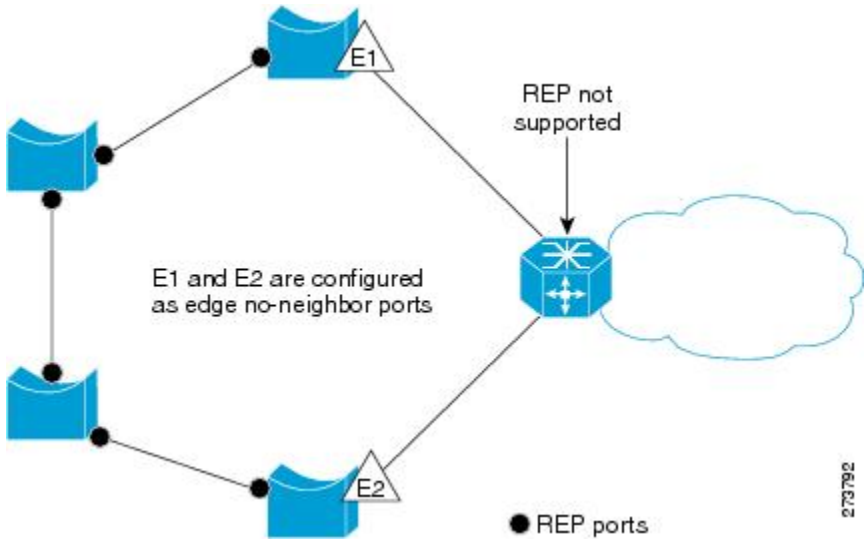
Convergence time varies depending on the type and number of nodes that are present on the ring.

REP Edge No-Neighbor

You can configure the non-REP switch facing ports as edge no-neighbor ports. These ports inherit the properties of edge ports, and overcome the limitation of not being able to converge quickly during a failure.

You can configure the non-REP facing ports (E1 and E2) as edge no–neighbor ports as shown in Figure 72: Edge No-Neighbor Ports, on page 499. These ports inherit all the properties of edge ports. You can configure these no-neighbor ports as any other edge port and also enable the ports to send REP topology change notifications to the aggregation switch.

Figure 72: Edge No-Neighbor Ports



Understanding REP Ports

Ports in REP segments take one of three roles or states—Failed, Open, or Alternate.

- A port configured as a regular segment port starts as a failed port.
- When the neighbor adjacencies are determined, the port transitions to the alternate port state, blocking all the VLANs on the interface. Blocked port negotiations occur and when the segment settles, one blocked port remains in the alternate role and all the other ports become open ports.
- When a failure occurs in a link, all the ports move to the failed state. When the alternate port receives the failure notification, it changes to the open state, forwarding all VLANs.

If you convert an edge port into a regular segment port, VLAN load balancing is not implemented unless it has been configured. For VLAN load balancing, you must configure two edge ports in the segment.

REP Actions on Packets

REP performs specific actions depending on the type of packets.

The following actions are taken by REP on packets that originate from an alternate port.

Packet type	Block/Allow (TX)	Action (TX)	Block/Allow (RX)	Action (RX)
REP LSL packet	Allow	—	Allow	Punt to CPU
REP HFL packet	Allow	—	Allow	Punt to CPU; no forward
Tagged control packet	Block if VLAN is blocked on the port	—	Block if VLAN is blocked on the port	As per the configured protocol and EVC, if VLAN is not blocked.
Untagged control packet	Block	—	Block	—
Tagged data packet	Block if VLAN is blocked on the port	—	Block if VLAN is blocked on the port	As per EVC, if VLAN is not blocked.
Untagged data packet	Block	—	Block	—

REP blocks untagged packets on a port only when VLAN load balancing is not in effect. When VLAN load balancing takes effect, all the untagged packets flow across an alternate port.

The following actions are taken by REP on packets that originate from an open port (a port that is not blocked by REP).

Packet type	Block/Allow (TX)	Action (TX)	Block/Allow (RX)	Action (RX)
REP LSL packet	Allow	—	Allow	Punt to CPU
REP HFL packet	Allow only packets that originate from the node	—	Allow	Punt to CPU and forward as per EVC
Tagged control packet	Allow	—	Allow	As per the configured protocol and EVC
Untagged control packet	Allow	—	Allow	As per the configured protocol and EVC
Tagged data packet	Allow	—	Allow	As per EVC
Untagged data packet	Allow	—	Allow	As per EVC

Default REP Configuration

REP is disabled on all the interfaces by default. When enabled, the interface is a regular segment port unless it is configured as an edge port.

When REP is enabled, the sending of segment topology change notifications (STCNs) is disabled, all VLANs are blocked, and the administrative VLAN is VLAN 1. When REP administrative VLAN or STCN configuration is changed, the changed configuration applies to ports.

When VLAN load balancing is enabled, the default is manual preemption with the delay timer disabled. If VLAN load balancing is not configured, the default action after manual preemption is to block all the VLANs at the elected alternate port.

Note REP cannot be enabled on the ports where link configuration is already present.

REP Configuration Guidelines

Follow these guidelines when configuring REP:

- REP ports must be a Layer 2 IEEE 802.1Q port or 802.1AD port.
- You must configure all trunk ports in the segment with the same set of allowed VLANs, or misconfiguration occurs.
- Be careful when configuring REP through a Telnet connection. Because REP blocks all VLANs until another REP interface sends a message to unblock it or you might lose connectivity to the router if you enable REP in a Telnet session that accesses the router through the same interface.
- If REP is enabled on two ports on a router, both ports must be either regular segment ports or edge ports. REP ports follow these rules:
  - If only one port on a router is configured in a segment, the port should be an edge port.
  - If two ports on a router belong to the same segment, both ports must be regular segment ports.
  - If two ports on a router belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.
- REP interfaces come up in a blocked state and do not forward traffic till they change to open ports through exchange of LSL HELLO messages with neighbors. You need to be aware of this to avoid sudden connection losses.
- REP configuration parameters for a port must not be changed without shutting down the port. However, the VLAN range for VLAN load balancing on primary edge port can be changed without this restriction.
- When configuring VLAN load balancing, the port selected for load balancing and the primary edge port must be on different nodes. Otherwise, it may cause HFL packets to flood, when VLAN Load Balancing is activated.
- When configuring STCN, ensure that STCN propagates across the REP segments in one direction. When STCN is sent from a segment, the STCN packet must not reach the original segment. Otherwise, it may cause an infinite loop of STCN packets flowing across the segments.

- REP is not supported on service instances configured with encapsulation, untagged, or default type.

REP Configuration Sequence

You must perform the following tasks in sequence to configure REP:

- Configure the REP administrative VLAN. The range of the REP admin VLAN is from 2 to 4094. The default VLAN 1 is always configured for HFL packets. However, EVC configuration must be explicitly done for VLAN 1, or any other VLAN that is selected to be an administrative VLAN. See DLP-J29 Configure REP Administrative VLAN Using Cisco IOS Commands, on page 504.
- Enable REP on ports and assign a segment ID to it. REP is disabled on all ports by default. The range of the segment ID is from 1 to 1024. See DLP-J31 Enable REP on a Port Using Cisco IOS Commands, on page 507.
- Configure two edge ports in the segment; one port as the primary edge port and the other as the secondary edge port. See DLP-J31 Enable REP on a Port Using Cisco IOS Commands, on page 507.

  If you configure two ports in a segment as the primary edge port, for example, ports on different switches, REP selects one of the ports to serve as the primary edge port based on port priority. The Primary option is enabled only on edge ports.
- Configure the primary edge port to send STCNs and VLAN load balancing to another port or to other segments. STCNs and VLAN load balancing configurations are enabled only for edge ports. See DLP-J32 Configure STCN on the Primary Edge Port Using Cisco IOS Commands, on page 508 and DLP-J38 Configure VLAN Load Balancing on the Primary Edge Port Using Cisco IOS Commands, on page 515.

Understanding REP in a Ring

Resilient Ethernet Protocol (REP) is supported on the front port Ethernet Flow Points (EFP) in a ring for loop prevention and network reconvergence. It is supported on the control channel of the 10G interlink ring ports. It is used for CPT 50 topology discovery and in keeping the control channel loop-free. By default, REP is enabled on all the ports in a ring.

This table lists the default values of the REP parameters on the east port of a ring.

Parameter	Default Value
Port Role	Primary (Edge)
STCN	Disable
VLAN Load Balancing	(For a closed-ended ring) Enable (For an open-ended ring) Disable
Neigbor No	-1
VLB Preempt Delay (in seconds)	(Only for a closed-ended ring) 15
Retries (in seconds)	5
Ageout Timer (in milliseconds)	5000

This table lists the default values of the REP parameters on the west port of a ring.

Note The details for west port is applicable only to a closed-ended ring.

Parameter	Default Value
Port Role	Preferred (Edge)
STCN	Disable
VLAN Load Balancing	Enable
Neigbor No	-1
VLB Preempt Delay (in seconds)	15
Retries (in seconds)	5
Ageout Timer (in milliseconds)	5000

Understanding REP Administrative VLAN

To avoid the delay introduced by relaying messages related to link-failure or VLAN-blocking notification during VLAN load balancing, REP floods packets at the HFL to a regular multicast address. HFL packets are used for fast transmission of failure notification across a REP ring by flooding a BPA on a VLAN. These messages are flooded to the whole network, not just the REP segment. You can control flooding of these messages by configuring an administrative VLAN for the whole domain.

Follow these guidelines when configuring the REP administrative VLAN:

- If you do not configure an administrative VLAN, the default VLAN is VLAN 1. The default VLAN 1 is always configured.
- There can be only one administrative VLAN on a router and on a segment.

The administrative VLAN is configured at the system level. Whenever the administrative VLAN is changed, the corresponding EFP must also be manually configured to match the outer encapsulation for tagged control packets. The EFP must be associated with a bridge domain used exclusively for administrative VLAN EFPs. The VLAN marked as administrative VLAN must not be used for any other service or data traffic.

NTP-J12 Configure REP Administrative VLAN

Purpose	This procedure configures REP Administrative VLAN.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J29 Configure REP Administrative VLAN Using Cisco IOS Commands, on page 504
- DLP-J30 Configure REP Administrative VLAN Using CTC, on page 505

Stop. You have completed this procedure.

DLP-J29 Configure REP Administrative VLAN Using Cisco IOS Commands

Purpose	This procedure configures REP administrative VLAN using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**rep admin vlan** *vlan-id* **Example:** Router(config)# rep admin vlan 100	Configures an REP administrative VLAN. The range of the REP administrative VLAN is from 2 to 4094. The default value is VLAN 1.

	Command or Action	Purpose
Step 4	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 5	**show interface** [*interface-id*] **rep detail** **Example:** Router# show interface TenGigabitEthernet4/1 rep detail	Displays the REP configuration and status for a specified interface.
Step 6	Return to your originating procedure (NTP).	—

Example: Configure REP Administrative VLAN

The following example shows how to configure the administrative VLAN as VLAN 100.

```
Router> enable
Router# configure terminal
Router(config)# rep admin vlan 100
Router(config)# end
```

DLP-J30 Configure REP Administrative VLAN Using CTC

Purpose	This procedure configures REP administrative VLAN using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to configure the REP administrative VLAN.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Provisioning** tab.

Step 5 From the left pane, click **REP**.

Step 6 Click the **Admin VLAN Configuration** tab.

Step 7 From the VLAN drop–down list, choose a VLAN. The range of the REP administrative VLAN is from 2 to 4094. The default value is VLAN 1.

Step 8 Click **Apply**.

Step 9 Return to your originating procedure (NTP).

NTP-J13 Configure REP

Purpose	This procedure configures REP.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J31 Enable REP on a Port Using Cisco IOS Commands, on page 507
- DLP-J32 Configure STCN on the Primary Edge Port Using Cisco IOS Commands, on page 508
- DLP-J33 Configure Preemption Delay on the Primary Edge Port Using Cisco IOS Commands, on page 509
- DLP-J34 Create a Segment Using CTC, on page 511
- DLP-J35 Edit a Segment Using CTC, on page 513

Stop. You have completed this procedure.

DLP-J31 Enable REP on a Port Using Cisco IOS Commands

Purpose	This procedure enables REP on a port using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J29 Configure REP Administrative VLAN Using Cisco IOS Commands, on page 504
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface and enters the interface configuration mode.
Step 4	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**] **Example:** Router(config-if)# rep segment 1 edge preferred	Enables REP on the interface, and identifies a segment number. The segment ID range value is from 1 to 1024. **Note** You must configure a primary and secondary edge port on each segment. The following optional keywords are available. • Enter **edge** to configure the port as an edge port. Each segment has only two edge ports. • Enter **no-neighbor** to specify that the edge port must not have a neighbor port.

	Command or Action	Purpose
		• Enter **primary** to configure the port as the primary edge port where you can configure VLAN load balancing. • Enter **preferred** to indicate that the port is the preferred alternate port or the preferred port for VLAN load balancing. **Note** Configuring a port as **preferred** does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.
Step 5	**end** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 6	**show interface** [*interface-id*] **rep detail** **Example:** Router(config)# show interface TenGigabitEthernet4/1 rep detail	Displays the REP interface configuration.
Step 7	Return to your originating procedure (NTP).	—

DLP-J32 Configure STCN on the Primary Edge Port Using Cisco IOS Commands

Purpose	This procedure configures the primary edge port to send STCNs to other segments or to an interface using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J31 Enable REP on a Port Using Cisco IOS Commands, on page 507
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Perform this procedure only on edge ports and not on regular segment ports.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface and enters interface configuration mode.
Step 4	**rep stcn** {**interface** *interface-id* | **segment** *segment-id-list*} **Example:** Router(config-if)# rep stcn segment 2-5	Configures the edge port to send STCNs to one or more segments or to an interface.
Step 5	**end** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J33 Configure Preemption Delay on the Primary Edge Port Using Cisco IOS Commands

Purpose	This procedure configures preemption time delay on the primary edge port using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J31 Enable REP on a Port Using Cisco IOS Commands, on page 507
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface and enters interface configuration mode.
Step 4	**rep preempt delay** *seconds* **Example:** Router(config-if)# rep preempt delay 60	Configures a preempt time delay. Use this command if you want VLAN load balancing to automatically trigger after a link failure and recovery. The time delay range is from 15 to 300 seconds. The default action is manual preemption with no time delay.
Step 5	**end** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

Example: Configure a REP Interface Using Cisco IOS Commands

The following example shows how to configure an interface as the primary edge port for segment 1, to send STCNs to segments 2 through 5, and to configure the alternate port as the port with port ID 0009001818D68700 to block all VLANs after a preemption delay of 60 seconds after a segment port failure and recovery.

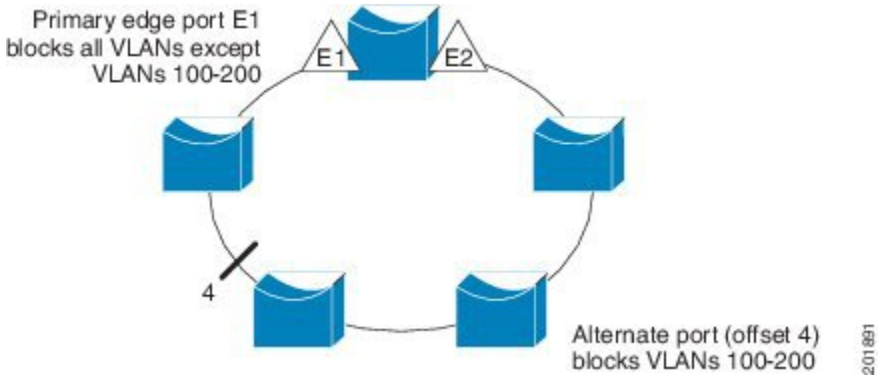
```
Router# configure terminal
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# rep segment 1 edge primary
Router(config-if)# rep stcn segment 2-5
```

```
Router(config-if)# rep block port 0009001818D68700 vlan all
Router(config-if)# rep preempt delay 60
Router(config-if)# end
```

The following example shows how to configure the VLAN blocking configuration shown in Figure 73: Example of VLAN Blocking, on page 511. The alternate port is the neighbor with neighbor offset number 4. After manual preemption, VLANs 100 to 200 are blocked at this port and all other VLANs are blocked at the primary edge port E1 (TenGigabitEthernet4/1).

```
Router# configure terminal
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# rep segment 1 edge primary
Router(config-if)# rep block port 4 vlan 100-200
Router(config-if)# end
```

Figure 73: Example of VLAN Blocking



DLP-J34 Create a Segment Using CTC

Purpose	This procedure creates a REP segment using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J30 Configure REP Administrative VLAN Using CTC, on page 505
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- You must configure two edge ports in the segment. A segment has only one primary edge port. If you configure two ports in a segment as the primary edge port, for example, ports on different switches, REP selects one of the ports to serve as the primary edge port based on port priority.
- If REP is enabled on two ports on a switch, both the ports must be either regular ports or edge ports. However, if the No-neighbor port is configured, one port can be an edge port and another port can be a regular port.

- You can also optionally configure where to send STCNs and VLAN load balancing (VLB). STCNs can be enabled on any edge port. VLB can be enabled only on primary edge ports.

Note You can create up to 32 REP segments.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to create a segment.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Provisioning** tab.

Step 5 From the left pane, click **REP**.

Step 6 Click the **Segment** tab.

Step 7 Click **Create**. The Create Segment dialog box appears.

Step 8 Enter the segment ID in the Segment No field. The range of the segment ID is 1 to 1024.

Step 9 From the Slot drop-down list, choose a slot.

Step 10 From the Port drop-drown list, choose a REP port that must belong to this segment.

Note A REP port can belong to only one segment.

Step 11 From the Port Role area, choose whether you want to configure the port as an edge port or a regular port. The options are:

a) Edge—The port is configured as an edge port.

- Check the **Primary** check box to configure the edge port as a primary edge port. Otherwise, uncheck the **Primary** check box to configure the edge port as a secondary edge port.
- Check the **Preferred** check box to configure the edge port as a preferred alternate port.
- Check the **NoNeighbor** check box if the edge port must not have a neighbor port. REP does not check for neighbor adjacency.

b) None—The port is configured as a regular port. If you choose this option, STCN and VLAN Load Balancing configurations are disabled.

- Check the **Preferred** check box to configure the edge port as a preferred alternate port.

Step 12 From the STCN area, configure the destination of STCN messages:

a) Check the **Enable** check box to enable sending STCN messages.
b) From the Port drop-down list, choose the STCN port to send STCN messages or enter the segment ID in the Segment No field to send STCN messages. The STCN port and REP port must be unique.

Step 13 From the VLAN Load Balancing area, configure VLAN load balancing on the primary edge port:

a) Check the **Enable** check box to enable VLAN load balancing.
b) Enter a single VLAN or range of VLANs in the VLAN field.
c) Choose **Preferred**, **Port Id**, or **Neighbor Id**. Complete one of the following steps:

- Choose **Preferred** to identify the preferred alternate port for VLAN load balancing.
- Choose **Port Id** and enter the REP port ID in the Rep PortId field.
- Choose **Neighbor Id** and enter the neighbor port id in the Neighbor No field.

Step 14 From the VLB Preempt Delay area, configure preemption delay on the primary edge port:
a) Check the **Enable** check box to enable preemption delay.
b) Enter the trigger delay for automatic VLB activation in the Trigger Delay field. The range is from 15 to 300 seconds.

Step 15 Enter the number of LSL retries before the REP link is disabled in the Retries field. The range is from 3 to 10 seconds.

Step 16 Enter the LSL age out timer value in the Time field. The range is from 120 to 10000 milliseconds.

Step 17 Click **Next**.

Step 18 Enter the details of the second port to add it to the segment.

Step 19 Click **Finish** to create a REP segment.
The new segment is added to the Selected Segment table.

Step 20 Return to your originating procedure (NTP).

DLP-J35 Edit a Segment Using CTC

Purpose	This procedure edits a segment using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J34 Create a Segment Using CTC, on page 511
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to edit a segment.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Provisioning** tab.

Step 5 From the left pane, click **REP**.

Step 6 Click the **Segment** tab. The list of segments appear in the Selected Segment table.

Step 7 Choose a segment from the list of segments.

Step 8 Click **Edit**. The Edit Segment dialog box appears.

Step 9 Modify the values as required and click **Finish**.

Step 10 Return to your originating procedure (NTP).

Understanding VLAN Load Balancing

REP supports VLAN load balancing, controlled by the primary edge port but occurring at any port in the segment.

You must configure two edge ports in the segment for VLAN load balancing. One edge port in the REP segment acts as the primary edge port; the other edge port as the secondary edge port.

The primary edge port always participates in VLAN load balancing in the segment. REP VLAN load balancing is achieved by blocking some VLANs at a configured alternate port and all other VLANs at the primary edge port.

Note When VLAN load balancing is configured, it does not start working until triggered by either manual intervention or a link failure and recovery.

When VLAN load balancing is triggered, the primary edge port then sends out a message to alert all interfaces in the segment about the preemption. When the message is received by the secondary edge port, it is reflected into the network to notify the alternate port to block the set of VLANs specified in the message and to notify the primary edge port to block the remaining VLANs.

You can also configure a particular port in the segment to block all VLANs. VLAN load balancing is initiated only by the primary edge port and is not possible if the segment is not terminated by an edge port on each end. The primary edge port determines the local VLAN load balancing configuration.

NTP-J14 Configure VLAN Load Balancing

Purpose	This procedure configures VLAN load balancing.
Tools/Equipment	None

Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J38 Configure VLAN Load Balancing on the Primary Edge Port Using Cisco IOS Commands, on page 515
- DLP-J39 Configure the Preemption for VLAN Load Balancing Using Cisco IOS Commands, on page 517
- DLP-J40 Activate VLAN Load Balancing Using CTC, on page 518
- DLP-J41 Deactivate VLAN Load Balancing Using CTC, on page 519

Stop. You have completed this procedure.

DLP-J38 Configure VLAN Load Balancing on the Primary Edge Port Using Cisco IOS Commands

Purpose	This procedure configures VLAN load balancing on the primary edge port using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J31 Enable REP on a Port Using Cisco IOS Commands, on page 507
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	Router> enable	
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface and enters the interface configuration mode.
Step 4	**rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**} **Example:** Router(config-if)# rep block port 0009001818D68700 vlan all	Configures VLAN load balancing on the primary edge port, identifies the REP alternate port, and configures the VLANs to be blocked on the alternate port. • Enter the **id** *port-id* to identify the alternate port by port ID. The port ID is automatically generated for each port in the segment. You can view interface port IDs by entering the **show interface** *interface-id* **rep detail** command in privileged EXEC mode. • Enter a *neighbor-offset* number to identify the alternate port as a downstream neighbor from an edge port. The range is from –256 to 256, with negative numbers indicating the downstream neighbor from the secondary edge port. A value of 0 is invalid. Enter -1 to identify the secondary edge port as the alternate port. • Enter **preferred** to select the regular segment port previously identified as the preferred alternate port for VLAN load balancing. • Enter **vlan** *vlan-list* to block one VLAN or a range of VLANs. • Enter **vlan all** to block all the VLANs.
Step 5	**end** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J39 Configure the Preemption for VLAN Load Balancing Using Cisco IOS Commands

Purpose	This procedure configures the preemption for VLAN load balancing using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J38 Configure VLAN Load Balancing on the Primary Edge Port Using Cisco IOS Commands, on page 515
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Ensure that all the other segment configuration has been completed before setting preemption for VLAN load balancing. When you enter the **rep preempt segment** *segment-id* command, a confirmation message appears before the command is executed because preemption for VLAN load balancing can disrupt the network.

If you do not enter the **rep preempt delay** *seconds* interface configuration command on the primary edge port to configure a preemption time delay, the default configuration is to manually trigger VLAN load balancing on the segment. Use the **show rep topology** privileged EXEC command to see which port in the segment is the primary edge port.

Perform these steps on the router that has the segment with the primary edge port.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**rep preempt segment** *segment-id* **Example:** Router# rep preempt segment 1	Manually triggers VLAN load balancing on the segment. **Note** Confirm the action before the command is executed.
Step 3	**show rep topology** **Example:** Router# show rep topology	Displays the REP topology information.
Step 4	Return to your originating procedure (NTP).	—

Example: Configure the Preemption for VLAN Load Balancing

The following example shows how to set the preemption for VLAN load balancing on a REP segment using Cisco IOS commands.

```
Router> enable
Router# rep preempt segment 1
```

DLP-J40 Activate VLAN Load Balancing Using CTC

Purpose	This procedure activates VLAN load balancing using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J34 Create a Segment Using CTC, on page 511
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note When VLAN load balancing is activated, the default configuration is manual preemption with the delay timer disabled.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to activate VLAN load balancing.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Provisioning** tab.

Step 5 From the left pane, click **REP**.

Step 6 Click the **Segment** tab. The list of segments appear.

Step 7 Choose a segment from the list of segments.

Step 8 Click **Activate VLB** to activate VLAN load balancing.

Step 9 Return to your originating procedure (NTP).

DLP-J41 Deactivate VLAN Load Balancing Using CTC

Purpose	This procedure deactivates VLAN load balancing using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J34 Create a Segment Using CTC, on page 511
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to deactivate VLAN load balancing.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Provisioning** tab.

Step 5 From the left pane, click **REP**.

Step 6 Click the **Segment** tab. The list of segments appear.

Step 7 Choose a segment from the list of segments.

Step 8 Click **Deactivate VLB** to deactivate VLAN load balancing.

Step 9 Return to your originating procedure (NTP).

Understanding REP Configurable Timers

The REP Configurable Timer (REP Fast Hellos) feature provides a fast reconvergence in a ring topology with higher timer granularity and quicker failure detection on the remote side. This feature also supports improved convergence of REP segments having nodes with copper based SFPs, where the link detection time varies between 300 ms to 700 ms.

With the REP Link Status Layer (LSL) ageout timer configuration, the failure detection time can be configured between a range of 120 to 10000 ms, in multiples of 40 ms. The result of this configuration is that, even if the copper pull takes about 700 ms to notify the remote end about the failure, the REP configurable timers process will detect it much earlier and take subsequent action for the failure recovery within 200 ms.

The LSL retries and LSL ageout timer is related in terms of LSL hello packet transmission. The LSL hello packet interval is measured by lsl_age_timer/lsl_retries value. The LSL hello packet interval value must be at least 40 ms.

Restrictions and Usage Guidelines

Follow these guidelines and restrictions:

- While configuring REP configurable timers, we recommend that you shut the port, configure REP and only then use the **no shut** command. This prevents the REP from flapping and generating large number of internal messages.
- If incompatible switches are neighbors, configure the correct LSL Age Out value first. In some scenarios, you might not get the expected convergence range.
- While configuring REP configurable timers, we recommend that you configure the REP LSL number of retries first and then configure the REP LSL ageout timer value.

NTP-J15 Configure REP Timers

Purpose	This procedure configures REP timers.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J42 Configure REP Link Status Layer Retries Using Cisco IOS Commands, on page 520
- DLP-J43 Configure the REP Link Status Layer Ageout Timer Using Cisco IOS Commands, on page 522

Stop. You have completed this procedure.

DLP-J42 Configure REP Link Status Layer Retries Using Cisco IOS Commands

Purpose	This procedure configures REP LSL retries at the interface configuration level using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J31 Enable REP on a Port Using Cisco IOS Commands, on page 507

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**rep lsl-retries** *no-of-retries* **Example:** Router(config-if)# rep lsl-retries 4	Configures the number of retries before the REP link is disabled. The range of retries is from 3 to 10. The default number of LSL retries is 5.
Step 5	**end** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

Example: Configure REP Link Status Layer Retries

The following example shows how to configure REP LSL retries using Cisco IOS commands.

```
Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# rep segment 2 edge primary
Router(config-if)# rep lsl-retries 4
Router(config-if)# end
```

DLP-J43 Configure the REP Link Status Layer Ageout Timer Using Cisco IOS Commands

Purpose	This procedure configures REP LSL ageout timer at the interface configuration level using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	• DLP-J31 Enable REP on a Port Using Cisco IOS Commands, on page 507 • DLP-J42 Configure REP Link Status Layer Retries Using Cisco IOS Commands, on page 520
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**rep lsl-age-timer** *lsl-age-timer* **Example:** Router(config-if)# rep lsl-age-timer 2000	Configures REP link status layer ageout timer value. The range of *lsl-age-timer* is between 120 ms and 10000 ms, in multiples of 40 ms. The default LSL ageout timer value is 5 seconds. The recommended LSL ageout timer value is 2 seconds.

	Command or Action	Purpose
Step 5	**end** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

Example: Configure the REP LSL Ageout Timer

The following example shows how to configure REP LSL ageout timer value using Cisco IOS commands.

```
Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# rep segment 1 edge primary
Router(config-if)# rep lsl-age-timer 2000
Router(config-if)# end
```

Understanding REP with EVC

REP can be integrated with an Ethernet Virtual Circuit (EVC) port using the REP over EVC feature. This feature allows you to configure and manage ports at the service instance level. An EVC port can have multiple service instances. Each service instance corresponds to a unique Ethernet Flow Point (EFP).

This feature allows you to configure an EVC port to participate in a REP segment. REP can selectively block or forward data traffic on particular VLANs. For EVC, the VLAN ID refers to the outer tag of the encapsulation that is configured on a service instance.

Note REP is supported on an EVC cross-connect and bridge domain service. REP is not supported for Ethernet Private Line and Ethernet Virtual Private Line services.

REP does not support protection or loop prevention on ring interfaces which have one of the following EFP configurations:

- **encapsulation default**
- **encapsulation untagged**
- **encapsulation xxxx any**

Though a REP ring will converge with such interfaces, traffic loop can happen depending on the EVC configuration.

Using the REP over EVC feature, you can:

- Control data traffic.
- Configure VLAN load balancing.

Restrictions and Usage Guidelines

When configuring REP over EVC, follow these guidelines and restrictions:

- It is recommended that you begin by configuring one port and then configure the contiguous ports to minimize the number of segments and the number of blocked ports.
- REP is not supported on LACP.
- If more than two ports in a segment fail when no external neighbors are configured, one port goes into a forwarding state to maintain connectivity during configuration.
- To avoid misconfiguration, you must configure all the trunk ports in the segment with the same set of allowed VLANs.
- Because REP blocks all VLANs until another REP interface sends a message to unblock it, you might lose connectivity to the port. This happens if you enable REP in a telnet session that accesses the EVC port through the same interface.
- On a router if REP is enabled on two ports for a segment, both ports must either be a regular segment ports or edge ports. REP ports follow these rules on a router:
  - If only one port is configured in a segment, the port should be an edge port.
  - If two ports belong to the same segment, both ports must be edge ports or the regular segment ports.
  - If two ports belong to the same segment and one is configured as an edge port and other as a regular segment port, the edge port is treated as a regular segment port.
  - There can be only two edge ports in a segment; if there are two edge routers in a segment, each router can have only one edge port. All the other ports on the edge router function as normal ports.
- REP interfaces come up in a blocked state and remains in a blocked state until notified that it is safe to unblock.
- REP relays all LSL Protocol Data Units (PDUs) in untagged frames and only HFL packets are relayed on the administrative VLAN.
- REP is not supported on EtherChannels. It is supported on EVC port-channels. REP is implemented on port-channels instead of its individual member links.
- REP is not supported on static port-channels.
- In case of double VLAN tagged frame, REP is implemented only on the outer VLAN tag.
- When an edge no-neighbor is configured on a router, configuring and unconfiguring an edge port is not allowed.

NTP-J16 Configure REP over EVC

Purpose	This procedure configures REP over EVC.
Tools/Equipment	None
Prerequisite Procedures	None

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

Procedure

Perform any of the following procedures as needed:

- DLP-J44 Configure REP over EVC Using a Cross–Connect Using Cisco IOS Commands, on page 525
- DLP-J45 Configure REP over EVC Using the Bridge Domain Using Cisco IOS Commands, on page 528

Stop. You have completed this procedure.

DLP-J44 Configure REP over EVC Using a Cross–Connect Using Cisco IOS Commands

Purpose	This procedure configures REP over EVC using a cross–connect at the service instance level using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters the interface configuration mode.
Step 4	**ether vlan color-block all** **Example:** Router(config-if)# ether vlan color-block all	Configures REP to block cross-connect type of service instances.
Step 5	**service instance** *id* **ethernet** [*evc-id*] **Example:** Router(config-if)# service instance 101 ethernet	Configures an Ethernet service instance on an interface and enters the service instance configuration mode.
Step 6	**encapsulation dot1q** {*any* | *vlan-id* [*vlan-id* [*-vlan-id*]]} **second-dot1q** {*any* | *vlan-id* [*vlan-id* [*-vlan-id*]]} **Example:** Router(config-if-srv)# encapsulation dot1q 100 second-dot1q 200	Configures the encapsulation. Defines the matching criteria to be used to map ingress dot1q frames on an interface to the appropriate service instance.
Step 7	**rewrite ingress tag** {**push** {**dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **pop** {**1** | **2**} | **translate** {**1-to-1** {**dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **2-to-1 dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **1-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **2-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*}} {**symmetric**} **Example:** Router(config-if-srv)# rewrite ingress tag dot1q single symmetric	Specifies the rewrite operation to be applied on the frame ingress to the service instance.
Step 8	**xconnect** *loopback_id vc_id* **encapsulation mpls** **Example:** Router(config-if-srv)# xconnect 10.0.0.2 999 encapsulation mpls	Configures the forwarding mechanism on a service instance. Ensure that the MPLS connectivity is up.
Step 9	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**] **Example:**	Configures REP over EVC. The segment ID range is from 1 to 1024. **Note** You must configure a primary and secondary edge port on each segment.

	Command or Action	Purpose
	Router(config-if)# rep segment 3 edge	The following optional keywords are available. • Enter **edge** to configure the port as an edge port. Entering **edge** without the **primary** keyword configures the port as the secondary edge port. Each segment has only two edge ports. • Enter **no-neighbor** to specify that the edge port must not have a neighbor port. • Enter **primary** to configure the port as the primary edge port where you can configure VLAN load balancing. • Enter **preferred** to indicate that the port is the preferred alternate port or the preferred port for VLAN load balancing. **Note** Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.
Step 10	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode.
Step 11	Return to your originating procedure (NTP).	—

Example: Configure REP over EVC Using Cross–Connect

The following example shows how to configure REP over EVC using cross–connect.

```
Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# service instance 10 ethernet
Router(config-srv)# encapsulation dot1q 20
Router(config-if-srv)# rewrite ingress tag push dot1q 20 symmetric
Router(config-if-srv)# xconnect 10.0.0.2 999 encapsulation MPLS
Router(config-if-srv)# exit
Router(config-if)# rep segment 2 edge
Router(config-if)# end
```

DLP-J45 Configure REP over EVC Using the Bridge Domain Using Cisco IOS Commands

Purpose	This procedure configures REP over EVC using the bridge domain at the service instance level using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**service instance** *id* **ethernet** [*evc-id*] **Example:** Router(config-if)# service instance 101 ethernet	Configures an Ethernet service instance on an interface and enters service instance configuration mode.
Step 5	**encapsulation dot1q** {*any* | *vlan-id* [*vlan-id* [*-vlan-id*]]} **second-dot1q** {*any* | *vlan-id* [*vlan-id* [*-vlan-id*]]} **Example:** Router(config-if-srv)# encapsulation dot1q 100 second dot1q 200	Configures the encapsulation. Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.

	Command or Action	Purpose
Step 6	**rewrite ingress tag** {**push** {**dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **pop** {**1** | **2**} | **translate** {**1-to-1** {**dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **2-to-1 dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **1-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **2-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*}} {**symmetric**} **Example:** Router(config-if-srv)# rewrite ingress tag push dot1q 20	Specifies the rewrite operation to be applied on the frame ingress to the service instance.
Step 7	**bridge-domain** *bridge-id* [**split-horizon**] **Example:** Router(config-if-srv)# bridge-domain 10	Configures the bridge domain to add another VLAN tag of type bridge-domain to the incoming packet.
Step 8	**exit** **Example:** Router(config-if-srv)# exit	Exits service instance configuration mode.
Step 9	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**] **Example:** Router(config-if)# rep segment 2 edge primary	Configures REP over EVC. The segment ID range is from 1 to 1024. **Note** You must configure a primary and secondary edge port on each segment. The following optional keywords are available. • Enter **edge** to configure the port as an edge port. Entering **edge** without the **primary** keyword configures the port as the secondary edge port. Each segment has only two edge ports. • Enter **no-neighbor** to specify that the edge port must not have a neighbor port. • Enter **primary** to configure the port as the primary edge port where you can configure VLAN load balancing. • Enter **preferred** to indicate that the port is the preferred alternate port or the preferred port for VLAN load balancing.

	Command or Action	Purpose
		Note Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.
Step 10	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode.
Step 11	Return to your originating procedure (NTP).	—

Example: Configure REP over EVC Using the Bridge Domain

The following example shows how to configure REP over EVC using the bridge domain.

```
Router# enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag push dot1q 10 symmetric
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# exit
Router(config-if)# rep segment 2 edge
Router(config-if)# end
```

Verify REP with EVC Configuration Using Cisco IOS Commands

You can use the **show rep topology**, **show rep topology detail** and **show interface rep** commands to verify REP over EVC configuration.

Example of the show rep topology Command

```
Router# show rep topology
```

```
REP Segment 1
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
10.64.106.63     Te5/4      Pri  Open
10.64.106.228    Te3/4           Open
10.64.106.228    Te3/3           Open
10.64.106.67     Te4/3           Open
10.64.106.67     Te4/4           Alt
10.64.106.63     Te4/4      Sec  Open

REP Segment 3
```

```
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
10.64.106.63     Gi50/1     Pri  Open
SVT_3400_2       Gi0/3           Open
SVT_3400_2       Gi0/4           Open
10.64.106.68     Gi40/2          Open
10.64.106.68     Gi40/1          Open
10.64.106.63     Gi50/2     Sec  Alt
```

Example of the show rep topology detail Command

```
Router# show rep topology detail
```

```
REP Segment 1
10.64.106.63, Te5/4 (Primary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 1 / [-6]
10.64.106.228, Te3/4 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 2 / [-5]
10.64.106.228, Te3/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 00E
  Port Priority: 000
  Neighbor Number: 3 / [-4]
10.64.106.67, Te4/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1800
  Port Number: 008
  Port Priority: 000
  Neighbor Number: 4 / [-3]
10.64.106.67, Te4/4 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 0005.9b2e.1800
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 5 / [-2]
10.64.106.63, Te4/4 (Secondary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 6 / [-1]
```

Example of the show interface rep detail Command

```
Router# show interface TenGigabitEthernet4/1 rep detail
```

```
TenGigabitEthernet4/1 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

REP with Other Features

REP supports up to 32 segments in each node. REP supports up to 5 segments or 10 ports on a single card or CPT 50 panel.

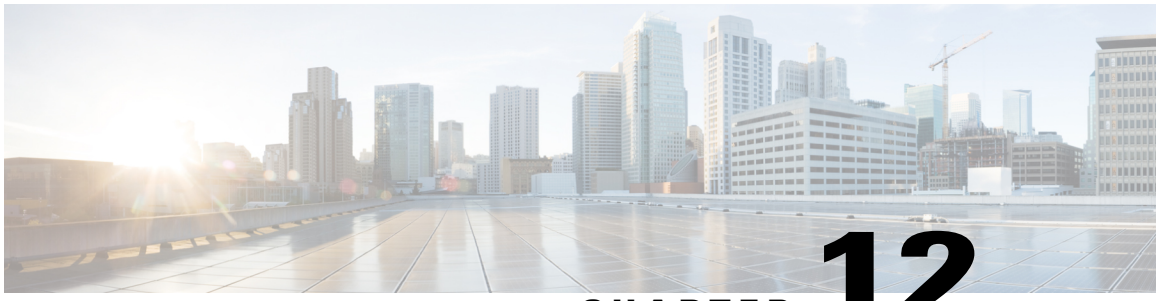
REP with High Availability

When the active fabric card fails, REP supports hot switchover to the standby fabric card. There might be momentary loss of traffic when the standby fabric card takes over as the active fabric card.

REP with Multicast

In a REP ring, the multicast traffic may not flow across all the elements on the ring; the traffic depends on the path taken from the multicast router to the client. The elements that do not form the multicast path do not become members of the multicast group.

When there is a failure in a REP ring, it is possible that the new path between the multicast router and the client may traverse elements which were previously not part of the multicast traffic path. These elements do not forward multicast traffic till they see a query from multicast router and a join from the client. A multicast router may only send query after long intervals, which results in a large traffic hit. All the ports that are enabled with REP must be configured as static mrouter ports to solve this issue.



CHAPTER 12

Configuring Link Aggregation Group and Link Aggregation Control Protocol

This chapter describes Link Aggregation Group, Link Aggregation Control Protocol, and manual load balancing. This chapter also describes the configuration procedures.

This chapter includes the following topics.

Understanding IEEE 802.3ad Link Bundling

The IEEE 802.3ad Link Bundling feature provides a method for aggregating multiple Ethernet links into a single logical channel based on the IEEE 802.3ad standard. This feature helps improve the cost effectiveness of a device by increasing cumulative bandwidth without necessarily requiring hardware upgrades. In addition, the IEEE 802.3ad Link Bundling feature provides a capability to dynamically provision, manage, and monitor various aggregated links and enables interoperability between various Cisco devices and devices of third-party vendors.

Benefits of Link Bundling

The IEEE 802.3ad Link Bundling feature provides the following benefits:

- Increased network capacity without changing physical connections or upgrading hardware.

- Cost savings resulting from use of existing hardware and software for additional functions.
- A standard solution that enables interoperability of network devices.
- Port redundancy without user intervention when an operational port fails.

Link Aggregation Group and Link Aggregation Control Protocol Configuration Procedures

The following procedures can be performed using Cisco IOS commands to configure Link Aggregation Group (LAG) and Link Aggregation Control Protocol (LACP):

- DLP-J5 Configure and Retrieve a Port Channel Using Cisco IOS Commands, on page 536
- DLP-J6 Configure LACP over Port Channel Using Cisco IOS Commands, on page 537
- DLP-J7 Monitor LACP Status Using Cisco IOS Commands, on page 538
- DLP-J8 Set LACP System Priority Using Cisco IOS Commands, on page 540
- NTP-J4 Configure LACP 1:1 Redundancy with Fast Switchover Using Cisco IOS Commands, on page 542
- DLP-J11 Configure a Channel Group with LACP Using Cisco IOS Commands, on page 545
- DLP-J12 Configure a Channel Group Without LACP Using Cisco IOS Commands, on page 546
- DLP-J13 Add and Remove Interfaces from a Channel Group Using Cisco IOS Commands, on page 548
- DLP-J14 Set a Minimum and Maximum Threshold of Active Links Using Cisco IOS Commands, on page 549
- DLP-J17 Configure Manual Load Balancing Using Cisco IOS Commands, on page 555

The following procedures can be performed using CTC to configure LAG and LACP:

- DLP-J9 Set LACP System Priority Using CTC, on page 541
- DLP-J15 Create a Channel Group Using CTC, on page 551
- DLP-J16 Edit a Channel Group Using CTC, on page 552
- DLP-J18 Configure Manual Load Balancing Using CTC, on page 557

Understanding LACP

The LACP is part of the IEEE802.3ad standard that enables you to bundle several physical ports together to form a single logical channel. LACP enables a network device, such as a switch, to negotiate an automatic bundling of links by sending LACP packets to the peer device. The LACP is a control protocol over LAG to check for any LAG misconfigurations.

LACP enables you to form a single Layer 2 link automatically from two or more Ethernet links. This protocol ensures that both ends of the Ethernet link are functional and agree to be members of the aggregation group. LACP must be enabled at both ends of the link to be operational.

For more information on LACP, see the IEEE802.3ad standard document.

LACP Advantages

LACP provides high reliability and redundancy. If a port fails, traffic continues on the remaining ports.

LACP Functions

LACP performs the following functions in the system:

- Maintains configuration information to control aggregation.
- Exchanges configuration information with other peer devices.
- Attaches or detaches ports from the LAG based on the exchanged configuration information.

LACP Modes

LACP can be configured in the following modes:

- Active—In this mode, the ports send LACP packets at regular intervals to the partner ports.
- Passive—In this mode, the ports do not send LACP packets until the partner port sends LACP packets. After receiving the LACP packets from the partner port, the ports send LACP packets to the partner port.

Note When you enable LACP on the channel group, LACP exchanges Protocol Data Units (PDU) of size 128 bytes. Hence, if the Maximum Transmission Unit (MTU) size of the channel group is set to a value less than 128 bytes, the protocol data units are dropped and the channel group interface goes down.

NTP-J2 Manage LACP

Purpose	This procedure configures LACP and monitors LACP status.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J5 Configure and Retrieve a Port Channel Using Cisco IOS Commands, on page 536
- DLP-J6 Configure LACP over Port Channel Using Cisco IOS Commands, on page 537
- DLP-J7 Monitor LACP Status Using Cisco IOS Commands, on page 538

Stop. You have completed this procedure.

DLP-J5 Configure and Retrieve a Port Channel Using Cisco IOS Commands

Purpose	This procedure configures and retrieves a port channel using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You must manually create a port channel logical interface. Configuring the IP address on the port channel interface is not supported.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface port-channel** *channel-number* **Example:** Router(config)# interface port-channel 10	Identifies the interface port channel and enters interface configuration mode.
Step 4	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Router(config-if)# end	
Step 5	**show running-config interface port-channel** *channel-number* **Example:** Router# show running-config interface port-channel 10	Displays the port channel configuration.
Step 6	**end** **Example:** Router# end	Ends the current configuration session.
Step 7	Return to your originating procedure (NTP).	—

Example: Verify the Port Channel Configuration

The following example shows how to verify the port channel configuration using Cisco IOS commands.

```
Router# show running-config interface port-channel 100

Building configuration...

Current configuration : 139 bytes
!
interface Port-channel100
 no ip address
 carrier-delay msec 0
 l2protocol peer cdp lacp
 l2protocol forward stp vtp dtp pagp dot1x
end
```

DLP-J6 Configure LACP over Port Channel Using Cisco IOS Commands

Purpose	This procedure configures LACP using port channel using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface port-channel** *channel-number* **Example:** Router(config)# interface port-channel 10	Identifies the interface port channel and enters interface configuration mode.
Step 4	**exit** **Example:** Router(config-if)# exit	Returns to interface configuration mode.
Step 5	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure and enters interface configuration mode.
Step 6	**channel-group** *channel-number* **mode {active | passive}** **Example:** Router(config-if)# channel-group 10 mode active	Configures the interface in a channel group and sets the lacp mode.
Step 7	**exit** **Example:** Router(config-if)# exit	Returns to privileged EXEC mode.
Step 8	Return to your originating procedure (NTP).	—

DLP-J7 Monitor LACP Status Using Cisco IOS Commands

Purpose	This procedure monitors LACP activity in the network using Cisco IOS commands.
Tools/Equipment	None

Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

For examples of **show lacp** commands, see Show Commands, on page 558.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show lacp** {*channel-group-number* | **counters** | **internal [detail]** | **neighbor [detail]** | **sys-id**} **Example:** Router# show lacp internal	Displays LACP information.
Step 3	**end** **Example:** Router# end	Ends the current configuration session.
Step 4	Return to your originating procedure (NTP).	—

Understanding LACP Priority

LACP uses the following parameters to control aggregation:

- LACP system priority—The system priority can be configured automatically or through the CLI. LACP uses the system priority with the device MAC address to form the system ID and also during negotiations with other systems. The range of LACP system priority is from 0 to 65535. The default value is 32768.
- LACP port priority—The port priority can be configured automatically or through the CLI. LACP uses the port priority to decide which ports must be placed first in aggregation. LACP also uses the port priority with the port number to form the port identifier. The range of LACP port priority is from 0 to 65535. The default value is 32768.
- LACP administrative key—LACP automatically configures an administrative key value on each port configured to use LACP. The administrative key defines the ability of a port to aggregate with other ports. The ability of the port to aggregate with the other ports is determined by the following:

- Port physical characteristics such as data rate, duplex capability, and point-to-point or shared medium.
- Configuration restrictions that you establish.

NTP-J3 Set LACP Priority

Purpose	This procedure sets LACP priority.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J8 Set LACP System Priority Using Cisco IOS Commands, on page 540
- DLP-J9 Set LACP System Priority Using CTC, on page 541

Stop. You have completed this procedure.

DLP-J8 Set LACP System Priority Using Cisco IOS Commands

Purpose	This procedure sets the LACP system priority using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**lacp system–priority** *priority* **Example:** Router(config)# lacp system-priority 200	Sets the system priority. The range of the LACP system priority is from 0 to 65535. The default value is 32768.
Step 4	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 5	**show lacp** {*channel-group-number* | **counters** | **internal [detail]** | **neighbor [detail]** | **sys-id**} **Example:** Router# show lacp sys-id	Displays the LACP information.
Step 6	**end** **Example:** Router# end	Ends the current configuration session.
Step 7	Return to your originating procedure (NTP).	—

DLP-J9 Set LACP System Priority Using CTC

Purpose	This procedure sets LACP system priority using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to set the LACP system priority.

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

Step 3 Right–click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Provisioning** tab.

Step 5 From the left pane, click **LACP**.

Step 6 Enter the priority in the System Priority field.
The range of the LACP system priority is from 0 to 65535. The default value is 32768.

Step 7 Click **Apply** to set the LACP system priority.

Step 8 Return to your originating procedure (NTP).

Understanding LACP 1:1 Redundancy

The LACP 1:1 redundancy feature provides an EtherChannel configuration with one active link and fast switchover to a hot standby link.

To use the LACP 1:1 redundancy feature, configure the LACP EtherChannel with two ports (one active and one standby). If the active link goes down, the EtherChannel stays up and the system performs fast switchover to the hot standby link. When the failed link becomes operational again, the EtherChannel performs another fast switchover to revert to the original active link.

For the LACP 1:1 redundancy feature to work correctly, especially the fast switchover capability, the feature needs to be enabled at both ends of the link.

NTP-J4 Configure LACP 1:1 Redundancy with Fast Switchover Using Cisco IOS Commands

Purpose	This procedure configures LACP 1:1 redundancy with fast switchover using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

For the LACP 1:1 redundancy feature, the channel group must contain two links, of which only one is active. The link with the lower port priority number (and therefore a higher priority) will be the active link, and the other link will be in a hot standby state. The maximum number of active member ports (**lacp max–bundle**) must be set to 1.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface port-channel** *channel-number* **Example:** Router(config)# interface port-channel 10	Identifies the interface port channel and enters interface configuration mode.
Step 4	**lacp fast-switchover** **Example:** Router(config-if)# lacp fast-switchover	Enables the fast switchover feature for this channel group.
Step 5	**lacp max-bundle** *number* **Example:** Router(config-if)# lacp max-bundle 1	Sets the maximum number of active member ports in the channel group to 1.
Step 6	**end** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 7	**show running-config interface port-channel** *channel-number* **Example:** Router# show running-config interface port-channel 10	Displays the port channel configuration.
Step 8	**end** **Example:** Router# end	Ends the current configuration session.

Example: Configure LACP 1:1 Redundancy with Fast Switchover

The following example shows how to configure the LACP channel group with 1:1 redundancy using Cisco IOS commands. Because the Ten Gigabit Ethernet port 4/1 is configured with a higher port priority number (and therefore a lower priority) than the default value of 32768, it will be the standby port.

```
Router> enable
Router# configure terminal
Router(config)# lacp system-priority 33000
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# channel-group 1 mode active
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# lacp port-priority 33000
Router(config)# interface port-channel 1
Router(config-if)# lacp fast-switchover
Router(config-if)# lacp max-bundle 1
Router(config-if)# end
Router(config)# show run interface port-channel 1
```

Understanding LAG

The LAG or an EtherChannel, bundles individual Ethernet links into a single logical link that provides the aggregate bandwidth of up to eight physical links. When an Ethernet Flow Point is configured on LAG, the EFP is protected against link failures.

When a link within an EtherChannel fails, the traffic previously carried over the failed link switches to the remaining links within that EtherChannel.

LAG supports manual load balancing and platform default load balancing. LAG supports Ethernet services. LAG can be an attachment circuit for MPLS services.

The LACP is a control protocol that is supported on the LAG.

Restrictions of LAG in CPT

The following restrictions apply to LAG in CPT:

- All the member links of LAG must be connected to the same CPT system and must be of the same interface type (10GE or 1GE). For example, one member link can be present in one CPT 50 and another member link can be present in another CPT 50. These two CPT 50 panels must be connected to the same CPT system.
- All the member links of LAG must operate at the same link speed and in full-duplex mode. LACP does not support the half-duplex mode.
- If you configure a physical port as part of LAG, you cannot configure Ethernet Virtual Circuits (EVCs) under that physical port.
- The number of LAGs supported in the CPT system is 128 with 8 member links per LAG. A member link cannot belong to more than one LAG at the same time.
- No MPLS-TP port can be created as LAG.

NTP-J5 Manage a Channel Group

Purpose	This procedure manages a channel group.

Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J11 Configure a Channel Group with LACP Using Cisco IOS Commands, on page 545
- DLP-J12 Configure a Channel Group Without LACP Using Cisco IOS Commands, on page 546
- DLP-J13 Add and Remove Interfaces from a Channel Group Using Cisco IOS Commands, on page 548
- DLP-J14 Set a Minimum and Maximum Threshold of Active Links Using Cisco IOS Commands, on page 549
- DLP-J15 Create a Channel Group Using CTC, on page 551
- DLP-J16 Edit a Channel Group Using CTC, on page 552

Stop. You have completed this procedure.

DLP-J11 Configure a Channel Group with LACP Using Cisco IOS Commands

Purpose	This procedure configures a channel group with LACP using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
	Router> enable	
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface port-channel** *channel-number* **Example:** Router(config)# interface port-channel 5	Identifies the interface port channel.
Step 4	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Configures a member interface and enters interface configuration mode.
Step 5	**channel-group** *channel-number* **mode** {**active** | **passive**} **Example:** Router(config-if)# channel-group 5 mode active	Configures the channel group with the LACP.
Step 6	**exit** **Example:** Router(config-if)# exit	Returns to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

Example: Configure a Channel Group with LACP

The following example shows how to configure the channel group number 5 using Cisco IOS commands.

```
Router> enable
Router# configure terminal
Router(config)# interface port-channel5
Router(config)# interface TenGigabitEthernet 7/1
Router(config-if)# channel-group 5 mode active
Router(config-if)# exit
```

DLP-J12 Configure a Channel Group Without LACP Using Cisco IOS Commands

Purpose	This procedure configures a channel group without LACP using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface port-channel** *channel-number* **Example:** Router(config)# interface port-channel 5	Identifies the interface port channel.
Step 4	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Configures a member interface and enters interface configuration mode.
Step 5	**channel-group** *channel-number* **link** *link-id* **Example:** Router(config-if)# channel-group 5 link 1	Configures the channel group without using LACP.
Step 6	**exit** **Example:** Router(config-if)# exit	Returns to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

Example: Configure a Channel Group Without Using LACP

The following example shows how to configure the channel group number 5 using Cisco IOS commands.

```
Router> enable
Router# configure terminal
Router(config)# interface port-channel5
Router(config)# interface TenGigabitEthernet 7/1
Router(config-if)# channel-group 5 link 1
Router(config-if)# exit
```

DLP-J13 Add and Remove Interfaces from a Channel Group Using Cisco IOS Commands

Purpose	This procedure adds and removes interfaces from a channel group using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J5 Configure and Retrieve a Port Channel Using Cisco IOS Commands, on page 536
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Configures a member interface and enters the interface configuration mode.
Step 4	**channel-group** *channel-group-number* **mode** {**active** | **passive**} **Example:** Router(config-if)# channel-group 5 mode active	Adds a Ten Gigabit Ethernet interface to a channel group.
Step 5	**no channel-group** **Example:** Router(config-if)# no channel-group	Removes the Ten Gigabit Ethernet interface from the channel group.

	Command or Action	Purpose
Step 6	**exit** **Example:** Router(config-if)# exit	Returns to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

Example: Add and Remove Interface from a Channel Group

The following example shows how to add an interface to a channel group using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 5/0
Router(config-if)# channel-group 5 mode active
Router(config-if)# exit
```

The following example shows how to remove an interface from a channel group using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 5/0
Router(config-if)# no channel-group
Router(config-if)# exit
```

DLP-J14 Set a Minimum and Maximum Threshold of Active Links Using Cisco IOS Commands

Purpose	This procedure sets a minimum and maximum threshold of active links allowed in the LACP bundle using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *port-channel channel-number* **Example:** Router(config)# interface port-channel 1	Creates a port channel virtual interface and enters interface configuration mode.
Step 4	**lacp min-bundle** *min-bundle-number* **Example:** Router(config-if)# lacp min-bundle 5	Sets the minimum threshold of active member links allowed in the LACP bundle. The range is 1 to 8.
Step 5	**lacp max-bundle** *max-bundle-number* **Example:** Router(config-if)# lacp max-bundle 7	Sets the maximum threshold of active member links allowed in the LACP bundle. The range is 1 to 8. The maximum threshold value must be greater than or equal to the minimum threshold value.
Step 6	**end** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

Set a Minimum Threshold of Active Links

The following example shows how to set a minimum threshold of active member links using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# interface port-channel 1
Router(config-if)# lacp min-bundle 5
Router(config-if)# end
```

DLP-J15 Create a Channel Group Using CTC

Purpose	This procedure creates a channel group using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to create a channel group.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Provisioning** tab.

Step 5 In the left pane, click **Channel Groups**.

Step 6 Click **Create**. The Channel Group Creation dialog box appears.

Step 7 Enter the name of the channel group in the Name field.

Step 8 From the ID drop-down list, choose an ID for this channel group. The IDs range from 1 to 128.

Step 9 From the Standalone list, choose the ports that will belong to this channel group and click the right arrow button to move the selected ports to the Bundled list.

Step 10 To create a channel group by configuring LACP:

a) Check the **LACP** check box to configure the channel group using LACP.

b) Enter the MTU value in the MTU field. The default value is 9600.

c) Check the **Remote Link Failure Notify** check box to enable the remote link failure notify feature for this channel group.

d) Enter the minimum number of ports that need to be active for the channel group in the Minimum bundle field. The default value is 1.

e) Enter the maximum number of ports to be bundled in a channel group in the Maximum bundle field. The default value is 8.

f) Check the **Fast Switchover** check box to enable the fast switchover feature for this channel group.

g) Click **Configure/Edit** in the Port LACP area of the port to configure the LACP mode for each port. The LACP Configuration dialog box appears.
The Port column lists all the ports that are added to the channel group.

- From the LACP Config drop-down list, choose **Active** or **Passive** for each port.
- Enter the LACP priority in the Priority field for each port. The default value is 32768. The range of LACP port priority is from 0 to 65535.

- Click **Apply**.

h) Click **Configure/Edit** in the Layer 2 action area to configure the actions for each Layer 2 protocol. The L2 Protocol Config dialog box appears.

- From the Action drop-down list, choose **Drop**, **Forward**, or **Peer** for each Layer 2 protocol.
- Click **Apply**.

i) Click **Create**. A new channel group is added in the Channel Group table.

Step 11 To create a channel group without configuring LACP:

a) Enter the MTU value in the MTU field. The default value is 9600.

b) Click **Configure/Edit** in the Layer 2 action area to configure the actions for each Layer 2 protocol. The L2PT Config dialog box appears.

- From the Action drop-down list, choose **Drop**, **Forward**, or **Peer** for each Layer 2 protocol.
- Click **Apply**.

c) Click **Create**. A new channel group is added in the Channel Group table.

Step 12 To delete a channel group, choose a channel group and click **Delete**.

Step 13 Return to your originating procedure (NTP).

DLP-J16 Edit a Channel Group Using CTC

Purpose	This procedure edits a channel group using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J15 Create a Channel Group Using CTC, on page 551
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to edit a channel group.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Provisioning** tab.

Step 5 In the left pane, click **Channel Groups**.

Step 6 Choose a channel group from the existing channel groups.

Step 7 Click **Edit**. The Edit Channel Group dialog box appears.
You can modify all the parameters of the channel group except the name and ID.

Step 8 To add ports to an existing channel group, choose the required ports from the Standalone list. Click the right arrow button to move the selected ports to the Bundled list.

Step 9 To remove ports from an existing channel group, choose the required ports from the Bundled list. Click the left arrow button to move the selected ports to the Standalone list.

Step 10 Modify the other parameters of the channel group, such as LACP mode of the channel group, soak time, minimum bundle, maximum bundle, LACP mode of ports, and Layer 2 action configuration as required.

Step 11 Click **Apply** to edit the channel group.

Step 12 Return to your originating procedure (NTP).

Understanding Load Balancing

Manual load balancing enables you to manually specify which member link a service instance must use for its egress traffic. This allows you, who has knowledge about the type of traffic traversing an EFP, to equally distribute EFPs.

Note The ingress traffic for any EFP can arrive on any member link of the LAG. All the egress traffic for the EFP must use only one of the member links.

EFPs can be configured on a channel group. The traffic, carried by the EFPs, is load balanced across the member links. Ingress traffic for a single EVC can arrive on any member of the bundle. All egress traffic for an EFP uses only one of the member links. The load balancing is achieved by distributing EFPs between the member links. The EFPs on a channel group are grouped and each group is associated with a member link. The manual load balancing mechanism can be used to control the EFP grouping.

Note CPT supports manual load balancing and platform default load balancing. CPT does not support weighted load balancing in this release. When manual load balancing is not configured and applied to the service instance, the default platform load balancing mechanism is used.

Default Load Balancing

In the default load balancing mechanism, the EFP traffic is distributed based on a hashing algorithm that is determined by the service instance ID and the number of active members in the channel group. The default load balancing algorithm is explained below.

(Service-instance ID) ÷ max_num_links

The maximum number of member links (max_num_links) supported in CPT is 8. Hence, (Service-instance ID) ÷ max_num_links value provides a hash bit value from 0 to 7. This value is then compared with the load share of each member link.

The load share is allocated for each active member link based on the number of active member links in the channel group. The member link whose load share contains the hash bit is selected as the egress link.

The load share derivation is as follows:

The default load share allocation algorithm allocates the load share bits sequentially to the member links.

Let us consider that we have 4 active links as follows. The load share calculation varies based on the link ids defined.

Member-1:4/1- 0 0 0 1 0 0 0 1 = 0x11

Member-2:4/2- 0 0 1 0 0 0 1 0 = 0x22

Member-3:4/3- 0 1 0 0 0 1 0 0 = 0x44

Member-4:4/4- 1 0 0 0 1 0 0 0 = 0x88

1. Create a channel group and add 4 member links (4/1, 4/2, 4/3, and 4/4)
2. The load share is calculated for the active member links.
3. Create a service with id 10 on the channel group. In CTC, the service instance id is automatically generated and can be obtained from the configuration pane (Layer-2 -> Carrier Ethernet).
4. On applying the algorithm: (Service-instance ID) ÷ max_num_links, we get 10 ÷ 8 == 2 (hash bit).
5. In the loadshare derived above, the hash bit = 2 is set for the port 4/3 and hence 4/3 is chosen as the egress port for the service 10.
6. The same procedure is repeated when services are added to obtain the egress port.

NTP-J6 Configure Manual Load Balancing

Purpose	This procedure configures manual load balancing.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J17 Configure Manual Load Balancing Using Cisco IOS Commands, on page 555
- DLP-J18 Configure Manual Load Balancing Using CTC, on page 557

Stop. You have completed this procedure.

DLP-J17 Configure Manual Load Balancing Using Cisco IOS Commands

Purpose	This procedure configures manual load balancing on the member links of the LAG using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J11 Configure a Channel Group with LACP Using Cisco IOS Commands, on page 545
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface port-channel 10	Creates a port channel virtual interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**service instance** *id* **ethernet** **Example:** Router(config-if)# service instance 100 ethernet	Configures an Ethernet service instance on an interface and enters service instance configuration mode.
Step 5	**encapsulation untagged, dot1q** {**any** | *vlan-id*} **second-dot1q** {**any** | *vlan-id*} **Example:** Router(config-if-srv)# encapsulation dot1q 100	Defines the matching criteria that maps the ingress dot1q, QinQ, or untagged frames on an interface to the appropriate service instance.
Step 6	**bridge-domain** *bridge-id* **Example:** Router(config-if-srv)# bridge-domain 100	Binds the Ethernet service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance.
Step 7	**exit** **Example:** Router(config-if-srv)# exit	Exits the service instance configuration mode.
Step 8	**port-channel load-balance** {**link** *link-id*} **Example:** Router(config-if)# port-channel load-balance link 1	Configures the primary load balanced link.
Step 9	**backup link** *link-id* **Example:** Router(config-if-lb)#backup link 2,3,4	Configures the back up links under the primary link.
Step 10	**service-instance** *id* **Example:** Router(config-if-lb)#service-instance 100	Assigns a service instance to a member link for manual load balancing
Step 11	**exit** **Example:** Router(config-if-lb)#exit	Returns to interface configuration mode.
Step 12	**end** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 13	Return to your originating procedure (NTP).	—

Example: Configure Manual Load Balancing

The following example shows how the service instances 100 and 101 are manually assigned to link 1 on Ten Gigabit Ethernet interface 5/2. The service instances are also assigned backup links 2, 3, and 4.

```
Router# configure terminal
Router(config)# interface port-channel 10
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# exit
Router(config-if)# service instance 101 ethernet
Router(config-if-srv)# encapsulation dot1q 101
Router(config-if-srv)# bridge-domain 101
Router(config-if-srv)# exit
Router(config-if)# port-channel load-balance link 1
Router(config-if-lb)# backup link 2,3,4
Router(config-if-lb)# service-instance 100,101
Router(config-if-lb)# exit

Router(config)# interface TenGigabitEthernet 5/2
Router(config-if)# channel-group 10 mode active link 1
Router(config-if)# exit
```

DLP-J18 Configure Manual Load Balancing Using CTC

Purpose	This procedure configures manual load balancing on the ports of the channel group using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J15 Create a Channel Group Using CTC, on page 551
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to configure manual load balancing.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Provisioning** tab.

Step 5 From the left pane, click **Channel Groups**.

Step 6 Click the **Load Balancing** tab.

Step 7 From the LAG drop-down list, choose a channel group.

Step 8 Click **Create** to configure manual load balancing on the ports of the channel group. The Manual Load Balancing dialog box appears.

Step 9 From the Primary Loadbalanced Link list, choose a port.

Step 10 From the Available Ports list, choose the required ports and click the right arrow button to move the ports to the Selected Ports list.
The selected ports serve as the backup ports for the primary load balanced port.

Step 11 Click **Apply**.
See DLP-J2 Create an EVC Circuit Using CTC, on page 143 to choose a channel group as the EFP and configure manual load balancing on the channel group.

Step 12 Return to your originating procedure (NTP).

Show Commands

Display Port Channel Statistics

The following example shows how to view port channel statistics.

```
Router# show interfaces stats
```

```
GigabitEthernet0/1
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
Processor          108470    31042570     82259      14255449
Route cache             0           0         0             0
Total              108470    31042570     82259      14255449
GigabitEthernet0/2
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
Processor           15979    19073260     15192      1325713
Route cache             0           0         0             0
Total              15979     19073260     15192      1325713
Port-channel15
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
Processor               0           0         0             0
```

```
Route cache          0           0           0           0
Total                0           0           0           0
```

```
Router# show interfaces port-channel 2 stats
```

```
Port-channel2
          Switching path    Pkts In   Chars In   Pkts Out    Chars Out
               Processor  570546645 295127854241  557694541 291427545417
            Route cache          0          0          0          0
                  Total  570546645 295127854241  557694541 291427545417
```

Display Port Channel Interface

The following example shows how to view the information for a port channel interface. *channel-id* is an integer value between 1 to 128.

```
Router# show interfaces port-channel channel-id
```

```
Router# show interfaces port-channel 20
```

```
Port-channel20 is up, line protocol is up
Hardware is GEChannel, address is 0002.0415.0002 (bia 0000.0000.0000)
  MTU 9600 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of active members in this channel: 1
        Member 0 : TenGigabitEthernet4/2 , Full-duplex, 10000Mb/s
    No. of passive members in this channel: 0
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     37 packets input, 7820 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     39 packets output, 8088 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

Display EFP Statistics

The following example shows how to view EFP statistics.

```
Router> show ethernet service instance stats
```

```
System maximum number of service instances: 32768
Service Instance 2, Interface TenGigabitEthernet3/1
Pkts In     Bytes In      Pkts Out      Bytes Out
   0           0             0             0
Service Instance 2, Interface Port-channel15
Pkts In     Bytes In      Pkts Out      Bytes Out
   0           0             0             0
```

Note The **show ethernet service instance stats** command does not display the EFP statistics for a pseudowire. Use the **show mpls l2transport vc [vcid] [detail]** command to view the EFP statistics for a pseudowire.

Display LACP Activity

The following examples show how to view LACP activity in the network.

```
Router# show lacp internal
```

```
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode


Channel group 20
                        LACP port   Admin   Oper  Port      Port
Port      Flags State   Priority    Key     Key   Number    State
Te4/2      SA    bndl    32768      0x5     0x5   0x42      0x3D
```

```
Router# show lacp 20 counters
```

```
            LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err

---------------------------------------------------------------------
Channel group 20
Te4/2      21     18        0      0        0      0         0
```

```
Router# show lacp 20 internal
```

```
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 20
                        LACP port   Admin   Oper  Port      Port
Port      Flags State   Priority    Key     Key   Number    State
Te4/2      SA    bndl    32768      0x5     0x5   0x42      0x3D
```

```
Router# show lacp 20 neighbor
```

```
Flags:  S - Device is requesting Slow LACPDUs
```

```
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 20 neighbors

Partner's information:

     Partner Partner LACP Partner  Partner   Partner  Partner     Partner
Port  Flags   State   Port Priority Admin Key Oper Key Port Number Port
State

Te4/2  SA     32768   0011.2026.7300  11s      0x1       0x14       0x3C
```

```
Router# show lacp 20 counters
```

```
             LACPDUs       Marker    Marker Response    LACPDUs
Port            Sent   Recv   Sent   Recv     Sent   Recv      Pkts  Err
--------------------------------------------------------------------------------
Channel group: 20
Te4/2           26      31     0      0        0      0         0
```

```
Router# show lacp sys-id
```

```
32768,0005.9b2e.18e0
```

Display Manual Load Balancing Configuration

```
Router# show ethernet service instance load-balance
```

```
Manually Assigned Load-Balancing Status for Port-channel1

 Link ID 1: TenGigabitEthernet4/1 (Active)
  Backup: Link ID 2 TenGigabitEthernet3/2
  Service instances: 10

 Link ID 2: TenGigabitEthernet3/2 (Active)
  Backup: Link ID 1 TenGigabitEthernet4/1
  Service instances: 20
```

```
Router# show ethernet service instance platform
```

Displays the port channel EFPs that are currently using the manual or platform load balancing and the egress link.

```
EFP id: 10 Interface Port-channel1
        Load balancing type: Manual
        Associated Egress Interface: TenGigabitEthernet4/1
EFP id: 20 Interface Port-channel1
        Load balancing type: Manual
        Associated Egress Interface: TenGigabitEthernet3/2
EFP id: 10 Interface Port-channel2
        Load balancing type: Manual
        Associated Egress Interface: TenGigabitEthernet5/1
EFP id: 20 Interface Port-channel2
```

```
        Load balancing type: Platform
        Associated Egress Interface: TenGigabitEthernet5/1
```

Interactions of LAG with Other Features

LAG interacts with the following features:

- EVC
- MPLS
- QoS
- IGMP Snooping
- REP

LAG with EVC

EFPs can be configured on a channel group. The traffic, carried by the EFPs, is load balanced across the member links. Ingress traffic for a single EVC can arrive on any member of the bundle. All egress traffic for an EFP uses only one of the member links. The load balancing is achieved by distributing EFPs between the member links. The EFPs on a channel group are grouped and each group is associated with a member link. In the default load balancing mechanism, there is no control over how the EFPs are distributed together, and sometimes the EFP distribution is not ideal. The manual load balancing mechanism can be alternatively used to control the EFP grouping.

When you configure a physical port as part of a channel group, you cannot configure EVCs under that physical port.

LAG can be configured for both point–to–point and point–to–multipoint bridge domains.

LAG with MPLS

LAG can be an attachment circuit for MPLS services.

The following example shows how the Ethernet LAG can connect to MPLS.

```
Router# enable
Router# configure terminal
Router(config)# interface port-channel 10
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# xconnect 10.0.0.2 999 encapsulation MPLS
Router(config-if-srv)# exit
```

LAG with QoS

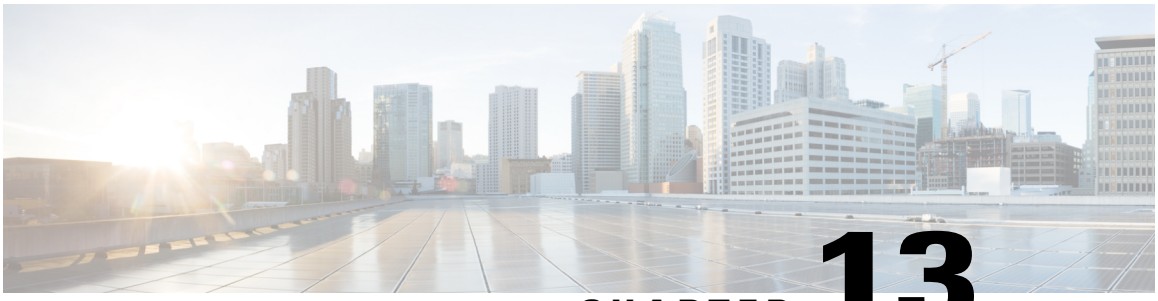
See QoS Support on Port-Channel, on page 460.

LAG with IGMP Snooping

See IGMP Snooping Interaction with LAG, on page 631.

LAG with REP

REP is not supported on member links that are part of a channel group.



CHAPTER 13

Configuring Span

This chapter describes port and EFP span. This chapter also describes procedures to configure port and EFP span.

Understanding Span

Span

Span is a technique of replicating the ingress or egress frames in a specific port to a specified list of destination ports. It is a monitoring feature used to monitor the traffic that is coming in and out of a port, channel group, or an Ethernet Flow Point (EFP). The monitored traffic can be used to debug the network and can also be used by law enforcement agencies.

The span can be configured to monitor ingress traffic, egress traffic, or both. The span source can be a physical port, channel group, or an EFP. The span destination can be a physical port or a channel group.

CPT supports two span modes:

- Port Span—In this configuration, the ingress or egress traffic on all the Ethernet Virtual Circuits (EVCs) in the source port or channel group is captured on the destination port or channel group. The pseudowire or tunnel port is not supported as a span destination.
- EFP Span—In this configuration, the ingress or egress traffic on the specified EFPs on a particular port or channel group is captured on the destination port or channel group. All types of services such as Multiprotocol Label Switching (MPLS), Virtual Private LAN Service (VPLS), Virtual Private Wire Service (VPWS), xconnect can be monitored. The pseudowire or tunnel port is not supported as a span destination.

Span Session

A span session is a collection of span source and destination ports, where traffic from each source port (based on their span direction) is replicated to the destination ports. Both the egress and ingress spans can be configured in a single session. A span destination port must not be a source of another span session. A span destination port cannot be shared among different sessions. CPT supports up to 50 span sessions.

Limitations and Restrictions of Port and EFP Span in CPT

- CPT supports only local span and not remote span. Therefore, the destination port or channel group can be any port or channel group on the same card or on different card on the same node.
- A port on the CPT 50 fanned out from a fabric card can be a destination span port only if the source span port is also on the same CPT 50.
- A span source port on a CPT 50 fanned out from a line card and a span destination port on another CPT 50 fanned out from another line card is not supported. If traffic is affected due to this issue, remove the span and reload the line card that has the fanout of the destination CPT 50 span.
- For egress span of the line card, only Ethernet Virtual Private LAN (EVPLAN) traffic is supported. The operations, administration, and maintenance (OAM) control traffic is not replicated.
- The span destination can only be a port or a channel group and not an EFP. The span source can be a port, channel group, or an EFP.
- If a channel group is selected as a destination port, the member ports of the channel group cannot be selected as destination ports.
- The egress span for the line card is supported only for point-to-multipoint traffic.
- The EFP, Resilient Ethernet Protocol (REP), Ethernet in the first mile (EFM) loopback, Link Aggregation Control Protocol (LACP), and Quality of Service (QoS) cannot be configured on the span destination port. No service can be associated with the span destination port as well.
- For port span, two egress span destinations and three ingress span destinations for each card is supported.
- For EFP span, one egress span destination for each card is supported.
- For EFP span, three ingress span destinations for each card is supported. When you add the fourth destination port to the span, the traffic is not received on the three destination ports.
- The maximum egress span bandwidth traffic is 10 Gbps for each card; the maximum egress span bandwidth traffic for the line card is 16 Gbps for the CPT system.
- CPT can monitor up to 256 EFPs for each fabric card, line card (ingress), and CPT 50 panel.
- CPT can monitor up to 150 EFPs in the entire CPT system for line card egress span.
- If there are multiple source ports, the traffic sent by each source port is not equally shared on the destination port.
- If QoS policy is attached to a port, span destination port cannot be configured on that.
- If a port is MPLS-TP core port, span destination port cannot be configured on that.
- If a port is FOG port, span destination port cannot be configured on that.

NTP-J119 Configure a Span Using Cisco IOS Commands

Purpose	This procedure configures a span using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J359 Configure a Port Span Using Cisco IOS Commands, on page 565
- DLP-J360 Configure an EFP Span Using Cisco IOS Commands, on page 567
- DLP-J362 Restrict the Destination Ports for a Span Using Cisco IOS Commands, on page 569
- DLP-J361 Verify the Span Configuration Using Cisco IOS Commands, on page 570

Stop. You have completed this procedure.

DLP-J359 Configure a Port Span Using Cisco IOS Commands

Purpose	This procedure configures a port span using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Router> enable	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**monitor session** *local_span_session_number* type *span-type* **Example:** Router(config)# monitor session 3 type local	Configures a monitor session using a SPAN session number and enters the SPAN session configuration mode. The *local_span_session_number* values range from 1 to 50. Only local span type is supported.
Step 4	**source interface** *type number direction* **Example:** Router(config-mon-local)# source interface TenGigabitEthernet 4/1 rx	Configures a port span for the source port and selects the traffic direction to be monitored. The *direction* accepts the following values: • **both—**Monitors received and transmitted traffic (both ingress and egress). • **rx—**Monitors received traffic (ingress). • **tx—**Monitors transmitted traffic (egress).
Step 5	**destination interface** *type number* **Example:** Router(config-mon-local)# destination interface TenGigabitEthernet 5/1	Configures a port span for the destination port.
Step 6	**exit** **Example:** Router(config-mon-local)# exit	Returns to global configuration mode.
Step 7	Return to your originating procedure (NTP).	—

Example: Configure a Port Span

The following example shows how to configure a port span using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# monitor session 3 type local
Router(config-mon-local)# source interface TenGigabitEthernet 4/1 rx
Router(config-mon-local)# destination interface TenGigabitEthernet 5/1
Router(config-mon-local)# exit
```

DLP-J360 Configure an EFP Span Using Cisco IOS Commands

Purpose	This procedure configures an EFP span using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**service instance** *id* **ethernet** [*evc-id*] **Example:** Router(config-if)# service instance 101 ethernet	Configures an Ethernet service instance on an interface and enters service instance configuration mode.
Step 5	**encapsulation dot1q** {*any* | *vlan-id* [*vlan-id* [*-vlan-id*]]} **second-dot1q** {*any* | *vlan-id* [*vlan-id* [*-vlan-id*]]} **Example:** Router(config-if-srv)# encapsulation dot1q 100 second dot1q 200	Defines the matching criteria that maps the ingress dot1q, QinQ, or untagged frames on an interface to the appropriate service instance.
Step 6	**rewrite ingress tag** {**push** {**dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **pop** {**1** | **2**} | **translate** {**1-to-1** {**dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **2-to-1 dot1q**	Specifies the rewrite operation to be applied on the frame ingress to the service instance.

	Command or Action	Purpose
	vlan-id | **dot1ad** *vlan-id*}| **1-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **2-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*}} {**symmetric**} **Example:** Router(config-if-srv)# rewrite ingress tag push dot1q 20	
Step 7	exit **Example:** Router(config-if-srv)# exit	Exits to global configuration mode.
Step 8	**monitor session** *local_span_session_number* type *span-type* **Example:** Router(config)# monitor session 3 type local	Configures a monitor session using a SPAN session number and enters the SPAN session configuration mode. The *local_span_session_number* values range from 1 to 50. Only local span type is supported.
Step 9	**source service instance** *EFP_number type number* **direction** **Example:** Router(config-mon-local)# source service instance 1 – 512 TenGigabitEthernet 4/1 rx	Configures an EFP span for the source port and selects the traffic direction to be monitored. The *EFP_number* can be a specific EFP or a range of EFPs. The range is from 1 to 32768. The *direction* values are as follows: • **both—**Monitors received and transmitted traffic (both ingress and egress). • **rx—**Monitors received traffic (ingress). • **tx—**Monitors transmitted traffic (egress).
Step 10	**destination interface** *type number* **Example:** Router(config-mon-local)# destination interface TenGigabitEthernet 5/1	Configures an EFP span for the destination port.
Step 11	**end** **Example:** Router(config-mon-local)# end	Exits configuration mode.
Step 12	Return to your originating procedure (NTP).	—

Example: Configure an EFP Span

The following example shows how to configure an EFP span for a channel group using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# interface port-channel 11
Router(config-if)# service instance 101 ethernet
Router(config-if-srv)# encapsulation dot1q 13
Router(config-if-srv)# rewrite ingress tag push dot1q 20 symmetric
Router(config-if-srv)# exit
Router(config)# monitor session 3 type local
Router(config-mon-local)# source service instance 2 - 200 Port-channel 1 both
Router(config-mon-local)# destination interface TenGigabitEthernet 5/1
Router(config-mon-local)# end
```

DLP-J362 Restrict the Destination Ports for a Span Using Cisco IOS Commands

Purpose	This procedure enables you to restrict the destination ports that can be used for a span session using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**monitor permit-list destination interface** *type number* **Example:**	Restricts the destination ports that can be used for a span session.

	Command or Action	Purpose
	Router(config)# monitor permit-list destination interface TenGigabitEthernet 4/1	
Step 4	**exit** **Example:** Router(config)# exit	Returns to privileged EXEC mode.
Step 5	Return to your originating procedure (NTP).	—

DLP-J361 Verify the Span Configuration Using Cisco IOS Commands

Purpose	This procedure verifies the span configuration using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**show monitor session all**
	
	Example:
	Router# show monitor session all
		Displays the configuration of all the span sessions.
		
		`Session 1`
		`---------`
		`Type : Local Session`
		`Status : Admin Disabled`
		`Source Ports :`
		`RX Only : Te5/1`
		`Destination Ports : Gi55/26,Gi55/44`
		
		`Session 5`
		`---------`
		`Type : Local Session`
		`Status : Admin Disabled`
		`Source EFPs :`
		`RX Only : Te5/1: 1`
		`Destination Ports : Te5/4`

	Command or Action	Purpose

Step 3	**show monitor permit-list**
	
	Example:
	Router# show monitor permit-list
		Displays the destination ports that can be used for a span session.
		
		`SPAN Permit-list :Admin Disabled`
		`Permit-list ports :Te3/2`

Step 4	Return to your originating procedure (NTP).	—

NTP-J118 Configure a Span Using CTC

Purpose	This procedure configures a span using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J357 Configure a Port or EFP Span Using CTC, on page 571
- DLP-J358 Restrict the Destination Ports for a Span Using CTC, on page 573

Stop. You have completed this procedure.

DLP-J357 Configure a Port or EFP Span Using CTC

Purpose	This procedure enables you to configure a port or EFP span using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J2 Create an EVC Circuit Using CTC, on page 143
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The span destination can only be a port or a channel group and not an EFP. The span source can be a port, channel group, or an EFP.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to configure a span.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

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

Step 4 Click **Create**. The Create Span dialog box appears.

Step 5 From the Span type drop-down list, choose **Port** or **EFP**.

Step 6 To set the port span type:

a) In the Source Information area, click **Add** to add the source ports or channel groups.
b) In the Add Source dialog box, choose **Slot/Port** or **CHGRP** as an interface type.
c) (For Slot/Port interface type) From the Slot drop-down list, choose a slot.
d) From the Available Ports/Available CHGRPS list, choose the required source ports or channel groups and click the right arrow to move them to the Selected Ports/Selected CHGRPS list.
e) Choose **Ingress**, **Egress**, or **Both** for the direction of the span.
f) Click **OK** to close the Add Source dialog box.
The specified details appear in the Source Information area in the Create Span dialog box.
g) In the Destination Information area, click **Add** to add the destination ports or channel groups.
h) In the Add Destination dialog box, choose **Slot/Port** or **CHGRP** as an interface type.
i) (For Slot/Port interface type) From the Slot drop-down list, choose a slot.
j) From the Available Ports/Available CHGRPS list, choose the required destination ports or channel groups and click the right arrow to move them to the Selected Ports/Selected CHGRPS list.
A port or channel group cannot be specified as a destination port if it carries traffic and has a service ID configured.
k) Click **OK** to close the Add Destination dialog box.
The specified details appear in the Destination Information area in the Create Span dialog box.

Step 7 To set the EFP span type:

a) In the Source Information area, click **Add** to add the source EFPs.
b) In the Add Source dialog box, choose **Slot/Port** or **CHGRP** as an interface type.
c) Enter the Service ID of the EFP in the Service ID field.
If a proper service ID is not specified, the span configuration does not work.
d) (For Slot/Port interface type) From the Slot drop-down list, choose a slot.
e) (For Slot/Port interface type) From the Port drop-down list, choose a port.
f) (For CHGRP interface type) From the CHGRP drop-down list, choose a channel group.

g) Choose **Ingress**, **Egress**, or **Both** for the direction of the span.
h) Click **OK** to close the Add Source dialog box.
The specified details appear in the Source Information area in the Create Span dialog box.
i) In the Destination Information area, click **Add** to add the destination ports or channel groups.
j) In the Add Destination dialog box, choose **Slot/Port** or **CHGRP** as an interface type.
k) (For Slot/Port interface type) From the Slot drop-down list, choose a slot.
l) From the Available Ports/Available CHGRPS list, choose the required destination ports or channel groups and click the right arrow to move them to the Selected Ports/Selected CHGRPS list.
A port or channel group cannot be specified as a destination port if it carries traffic and has a service ID configured.
m) Click **OK** to close the Add Destination dialog box.
The specified details appear in the Destination Information area in the Create Span dialog box.

Step 8 Click **Add** to create a port or EFP span.
You can also edit or delete a port or EFP span from the Span tab. The span type cannot be changed while editing a span.

Step 9 Return to your originating procedure (NTP).

DLP-J358 Restrict the Destination Ports for a Span Using CTC

Purpose	This procedure enables you to restrict the destination ports that can be used for a span session using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Only the ports in the Permit List tab can be specified as a destination port while creating a span session. If the Permit List tab is empty, all the ports can be specified as destination ports for the span session except the source span ports.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to restrict the destination ports for a span session.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** > **Span** > **Permit List** tabs.

Step 4 Click **Add**. The Add Source dialog box appears.

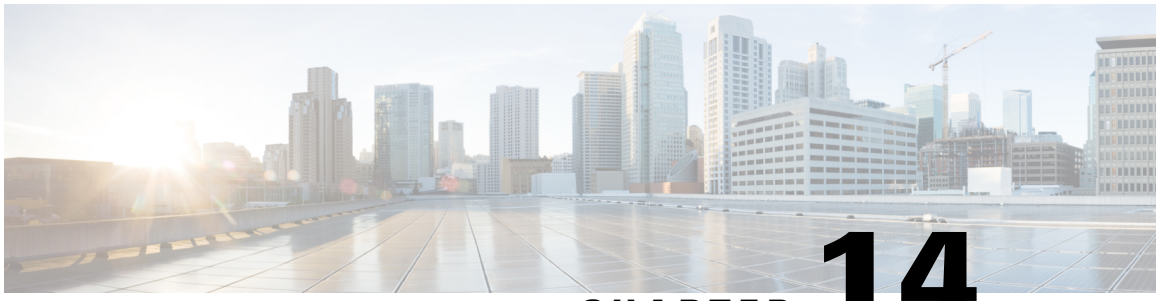
Step 5 In the Add Source dialog box, choose **Slot/Port** or **CHGRP** as an interface type.

Step 6 (For Slot/Port interface type) From the Slot drop-down list, choose a slot.

Step 7 From the Available Ports/Available CHGRPS list, choose the required destination ports or channel groups and click the right arrow to move them to the Selected Ports/Selected CHGRPS list.

Step 8 Click **OK** to close the Add Source dialog box.
The ports that can be specified as destination ports appear in the Permit List tab.

Step 9 Return to your originating procedure (NTP).



CHAPTER 14

Configuring MAC Learning

This chapter describes MAC learning, MAC address limiting, and static MAC address. This chapter also describes the configuration procedures.

Understanding MAC Learning

The Carrier Packet Transport (CPT) system is a distributed system with fabric cards, line cards, and CPT 50 panels. The MAC addresses learned on one line card needs to be learned or distributed on the other line cards. The MAC learning feature enables the distribution of the MAC addresses learned on one line card to the other line cards.

A software MAC address table is maintained on the fabric cards. This MAC address table contains the MAC addresses learned on all the line cards. This MAC address table is used to distribute the MAC addresses when the line card reboots or goes through Online Insertion and Removal (OIR).

Note By default, MAC address learning is enabled only for point–to–multipoint bridge domains and can also be disabled. See NTP-J7 Enable or Disable MAC Learning on a Bridge Domain, on page 578.

MAC Address Aging

Dynamically learned MAC addresses are deleted after the MAC address age out value. This frees up unused addresses from the MAC address table for other active subscribers. In CPT, the default value for MAC address aging is 300 seconds and cannot be changed. The expected MAC address age out timer is between 300 to 600 seconds depending on the number of MAC addresses learned.

Dynamic MAC Address Learning

Dynamic MAC address learning occurs when the bridging data path encounters an ingress frame whose source address is not present in the MAC address table for the ingress service instance. The learned MAC addresses are distributed to the other cards with Ethernet Flow Points (EFPs) in the same bridge domain.

MAC Move

A MAC move occurs when the same MAC address is re-learned on a different port. When a MAC move is detected, a transient event is generated to inform the user about the MAC move.

MAC Learning on LAG

MAC learning is enabled on the LAG interface, if the Link Aggregation Group (LAG) interface is part of the point–to–multipoint bridge domain. The MAC addresses are learned on the LAG interface instead of the physical interface.

MAC Learning Actions

The following table describes the various scenarios and the actions taken on MAC addresses for each scenario.

Table 28: MAC Learning Actions

Scenario	Action
A bridge domain is created.	The MAC learning is enabled by default in point–to–multipoint bridge domains. The MAC learning is not supported in point–to–point bridge domains.
A bridge domain is deleted.	The MAC addresses learned on the bridge domain are removed from the software MAC address table that is maintained on the fabric cards. These MAC addresses are also removed from the line card hardware.
An EFP is added and is the first EFP on a bridge domain on a card.	All the MAC addresses learned on the bridge domain are sent to this new card.
An EFP is added and is not the first EFP on a bridge domain.	Nothing needs to be done as the MAC addresses learned on the bridge domain are already present.
An EFP is deleted.	All the MAC addresses learned on that EFP are deleted.
An EFP admin state is UP.	When the EFP is the first EFP on the bridge domain on the card, all the MAC addresses learned on the bridge domain are sent to this new card. When the EFP is not the first EFP on the bridge domain on the card, nothing needs to be done as the MAC addresses learned on the bridge domain are already present.

Scenario	Action
An EFP admin state is DOWN.	All the MAC addresses learned on that EFP are deleted.
The port goes down.	All the MAC addresses learned on the port on all the bridge domains are deleted.
The active fabric card is reset.	The standby fabric card becomes active and the software MAC address table on the new active card is used.
The standby fabric card is reset.	The standby fabric card is updated with the software MAC address table during the bulk synchronization process.
The line card comes up after the line card is reset (soft reset).	The active fabric card sends the MAC addresses learned on the bridge domains that are configured on the line card.
The line card goes through Online Insertion and Removal (OIR).	The active fabric card sends the MAC addresses learned on the bridge domains that are configured on the line card.

MAC Learning Configuration Procedures

The following procedures can be performed using Cisco IOS commands to configure MAC learning and MAC address limiting:

- DLP-J19 Re–enable or Disable MAC Learning on a Bridge Domain Using Cisco IOS Commands, on page 578
- DLP-J21 Configure MAC Address Limit on a Bridge Domain Using Cisco IOS Commands, on page 581
- DLP-J23 Configure a Static MAC Address on a Service Instance Using Cisco IOS Commands, on page 584
- DLP-J25 Remove a MAC Address Using Cisco IOS Commands, on page 588
- DLP-J27 Display Information About the MAC Address Table Using Cisco IOS Commands, on page 591

The following procedures can be performed using CTC to configure MAC learning and MAC address limiting:

- DLP-J20 Re-enable or Disable MAC Learning on a Bridge Domain Using CTC, on page 580
- DLP-J22 Configure the MAC Address Limit on a Bridge Domain Using CTC, on page 582
- DLP-J24 Configure a Static MAC Address on a Service Instance Using CTC, on page 586
- DLP-J26 Remove a MAC Address Using CTC, on page 589
- DLP-J28 Display Information About the MAC Address Table Using CTC, on page 593

NTP-J7 Enable or Disable MAC Learning on a Bridge Domain

Purpose	This procedure enables or disables MAC learning on a bridge domain.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J19 Re–enable or Disable MAC Learning on a Bridge Domain Using Cisco IOS Commands, on page 578
- DLP-J20 Re-enable or Disable MAC Learning on a Bridge Domain Using CTC, on page 580

Stop. You have completed this procedure.

DLP-J19 Re–enable or Disable MAC Learning on a Bridge Domain Using Cisco IOS Commands

Purpose	This procedure re-enables or disables MAC learning on the bridge domain using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note MAC learning is enabled on the point–to–multipoint bridge domains by default.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**bridge-domain** *bridge-id* **Example:** Router(config)# bridge-domain 100	Configures components on a bridge domain and enters bridge domain configuration mode.
Step 4	**mac learning** **Example:** Router(config-bdomain)# mac learning	Re-enables MAC learning on this bridge domain.
Step 5	**no mac learning** **Example:** Router(config-bdomain)# no mac learning	Disables MAC learning on this bridge domain.
Step 6	**end** **Example:** Router(config-bdomain)# end	Exits bridge domain configuration mode and returns to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

Example: Re–enable or Disable MAC Learning on a Bridge Domain

The following example shows how to re-enable MAC learning on a bridge domain using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# bridge-domain 100
Router(config-bdomain)# mac learning
Router(config-bdomain)# end
```

The following example shows how to disable MAC learning on a bridge domain using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# bridge-domain 100
Router(config-bdomain)# no mac learning
Router(config-bdomain)# end
```

DLP-J20 Re-enable or Disable MAC Learning on a Bridge Domain Using CTC

Purpose	This procedure re-enables or disables MAC learning on the bridge domain using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J2 Create an EVC Circuit Using CTC, on page 143 of EVC type Ethernet Private LAN or Ethernet Virtual Private LAN.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note MAC learning is enabled on the point–to–multipoint bridge domains by default.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to re-enable or disable MAC learning.

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

Step 3 Click the **Layer2+** tab.

Step 4 Click **Carrier Ethernet**.

Step 5 From the list of EVC circuits, choose an EVC circuit to edit.

Step 6 Click **Edit**. The Edit Circuit dialog box appears.

Step 7 Click the **MAC Learning** tab.

Step 8 Re-enable or disable MAC learning on the Network Element. Complete one of the following steps:

a) Check the **MAC Learning** check box to re-enable MAC learning on this Network Element.

b) Uncheck the **MAC Learning** check box to disable MAC learning on this Network Element.

Step 9 Click **Apply**.

Step 10 Return to your originating procedure (NTP).

Understanding MAC Address Limiting

The MAC Address Limiting for bridge domains provides the capability to control the MAC addresses learnt on the bridge domain. You can configure an upper limit on the number of MAC addresses that can be learnt in a bridge domain. If an Ethernet frame with an unknown MAC address is received, it is flooded in the bridge domain. The MAC address limiting commands are configured under the bridge domain.

Note The maximum MAC address limit on a bridge domain is 128000.

NTP-J8 Configure MAC Address Limit on a Bridge Domain

Purpose	This procedure configures MAC address limit on a bridge domain.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J21 Configure MAC Address Limit on a Bridge Domain Using Cisco IOS Commands, on page 581
- DLP-J22 Configure the MAC Address Limit on a Bridge Domain Using CTC, on page 582

Stop. You have completed this procedure.

DLP-J21 Configure MAC Address Limit on a Bridge Domain Using Cisco IOS Commands

Purpose	This procedure configures an upper limit on the number of MAC addresses that reside in a bridge domain using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**bridge-domain** *bridge-id* **Example:** Router(config)# bridge-domain 100	Configures components on a bridge domain and enters bridge domain configuration mode.
Step 4	**mac limit maximum addresses** *maximum-addresses* **Example:** Router(config-bdomain)# mac limit maximum addresses 200	Sets an upper limit on the number of MAC addresses that reside in a bridge domain. **Note** Enter the **no mac limit** command to restore the default MAC address limit.
Step 5	**end** **Example:** Router(config-bdomain)# end	Exits bridge domain configuration mode and returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

Example: Configure MAC Address Limit on a Bridge Domain

The following example shows how to configure MAC address limiting on a bridge domain using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# bridge-domain 100
Router(config-bdomain)# mac limit maximum addresses 1000
Router(config-bdomain)# end
```

DLP-J22 Configure the MAC Address Limit on a Bridge Domain Using CTC

Purpose	This procedure configures the MAC address limit on a bridge domain using CTC.
Tools/Equipment	None

Prerequisite Procedures	DLP-J2 Create an EVC Circuit Using CTC, on page 143 of EVC type Ethernet Private LAN or Ethernet Virtual Private LAN.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to configure the MAC address limit.

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

Step 3 Click the **Layer2+** tab.

Step 4 Click **Carrier Ethernet**.

Step 5 From the list of EVC circuits, select an EVC circuit to edit.

Step 6 Click **Edit**. The Edit Circuit dialog box appears.

Step 7 Click the **MAC Learning** tab.

Step 8 Enter the upper limit on the number of MAC addresses that reside in a bridge domain in the Limit field. You need to change the MAC address limit value on each node where the bridge domain is configured.

Step 9 Click **Apply**.

Step 10 Return to your originating procedure (NTP).

Understanding the Static MAC Address

You can configure static MAC addresses on a service instance. Static MAC address configuration on service instances eliminates the need for MAC address learning, which is required for traffic forwarding. Without MAC address learning, MAC address table resources can be conserved and network resources can be optimized.

Note Static MAC address configuration does not apply to the MVR bridge domain.

Benefits

Static MAC address support on service instances provides the following benefits:

- Facilitates optimization of network resources.
- Conserves MAC table resources when used for upstream traffic.

Restrictions

- Multicast static MAC addresses are not allowed in MAC address configurations. Unicast MAC addresses can be statically configured.

NTP-J9 Configure a Static MAC Address on a Service Instance

Purpose	This procedure configures a static MAC address on a service instance.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J23 Configure a Static MAC Address on a Service Instance Using Cisco IOS Commands, on page 584
- DLP-J24 Configure a Static MAC Address on a Service Instance Using CTC, on page 586

Stop. You have completed this procedure.

DLP-J23 Configure a Static MAC Address on a Service Instance Using Cisco IOS Commands

Purpose	This procedure configures a static MAC address on a service instance using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J1 Configure an Ethernet Service Instance Using Cisco IOS Commands, on page 141
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Enter the **no mac static address mac-addr** command to remove the statically added unicast MAC address.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Configures a Ten Gigabit Ethernet interface and enters interface configuration mode.
Step 4	**service instance** *id* **ethernet** *[evc-id]* **Example:** Router(config-if)# service instance 1 ethernet	Configures an Ethernet service instance on an interface and enters service instance configuration mode.
Step 5	**mac static address** *mac-address* **Example:** Router(config-if-srv)# mac static address 0000.bbbb.cccc	Configures a static MAC address on a service instance.
Step 6	**exit** **Example:** Router(config-if-srv)# exit	Returns to interface configuration mode.
Step 7	**end** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 8	Return to your originating procedure (NTP).	—

Example: Configure a Static MAC Address on a Service Instance

The following example shows how to configure a static MAC address on a service instance using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac static address 0000.bbbb.cccc
Router(config-if-srv)# exit
Router(config-if)# end
```

DLP-J24 Configure a Static MAC Address on a Service Instance Using CTC

Purpose	This procedure configures a static MAC address on a service instance using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J2 Create an EVC Circuit Using CTC, on page 143 of EVC type Ethernet Private LAN or Ethernet Virtual Private LAN.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to configure a static MAC address.

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

Step 3 Click the **Layer2+** tab.

Step 4 Click **Carrier Ethernet**.

Step 5 From the list of EVC circuits, select an EVC circuit to edit.

Step 6 Click **Edit**. The Edit Circuit dialog box appears.

Step 7 Click the **MAC Learning** tab.

Step 8 Click **EFP Static MAC Address Configuration** to enter static MAC addresses for each EFP. The EFP Static MAC Address Configuration dialog box appears.

Step 9 From the EFP drop-down list, choose an EFP.

Step 10 Enter one or more static MAC addresses for this EFP in the MAC Address field and click **Add**. The added MAC addresses appear in the Entered MAC Addresses area.

Step 11 Click **Apply** and close the EFP Static MAC Address Configuration dialog box.

Step 12 Return to your originating procedure (NTP).

NTP-J10 Remove a MAC address

Purpose	This procedure removes a MAC address from the MAC address table.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J25 Remove a MAC Address Using Cisco IOS Commands, on page 588
- DLP-J26 Remove a MAC Address Using CTC, on page 589

Stop. You have completed this procedure.

DLP-J25 Remove a MAC Address Using Cisco IOS Commands

Purpose	This procedure removes a dynamic MAC address from the MAC address table using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure removes only dynamically added MAC addresses. To remove the statically added MAC addresses, enter the **no mac static address mac-addr** command.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**clear mac-address-table** [**address** *mac-address*] [**interface** *type number*] [**bridge-domain** *bridgedomain-id*] **Example:** Router# clear mac-address-table address 0000.bbbb.cccc interface TenGigabitEthernet 4/1 bridge-domain 100	Removes the dynamic MAC address from the MAC address table on a bridge domain. The *bridgedomain-id* is the bridge domain number.
Step 4	**exit** **Example:** Router# exit	Exits global configuration mode.
Step 5	Return to your originating procedure (NTP).	—

Example: Remove a MAC Address

The following example shows how to remove a MAC address from the MAC address table on a bridge domain using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router# clear mac-address-table address
0000.bbbb.cccc interface TenGigabitEthernet 4/1 bridge-domain 100
Router# exit
```

The following example shows how to remove a MAC address from the MAC address table on all the bridge domains using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router# clear mac-address-table address 0000.bbbb.cccc
Router# exit
```

DLP-J26 Remove a MAC Address Using CTC

Purpose	This procedure removes a specific MAC address from the MAC address table using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J2 Create an EVC Circuit Using CTC, on page 143 of EVC type Ethernet Private LAN or Ethernet Virtual Private LAN.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to remove specific MAC addresses from the MAC address table.

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

Step 3 Click the **Layer2+** tab.

Step 4 Click **Carrier Ethernet**.

Step 5 From the list of EVC circuits, select an EVC circuit to edit.

Step 6 Click **Edit**. The Edit Circuit dialog box appears.

Step 7 Click the **MAC Learning** tab.

Step 8 Click **Clear MAC Addresses**. The Clear MAC Addresses dialog box appears.

Step 9 To remove a specific MAC address from the MAC address table, select that MAC address in the MAC Addresses to clear area and click **Clear**.

Step 10 Close the Clear MAC Addresses dialog box.

Step 11 Return to your originating procedure (NTP).

NTP-J11 Display Information About the MAC Address Table

Purpose	This procedure displays information about the MAC address table.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J27 Display Information About the MAC Address Table Using Cisco IOS Commands, on page 591
- DLP-J28 Display Information About the MAC Address Table Using CTC, on page 593

Stop. You have completed this procedure.

DLP-J27 Display Information About the MAC Address Table Using Cisco IOS Commands

Purpose	This procedure displays information about the MAC address table using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show mac-address-table address** *mac-addr* **Example:** Router# show mac-address-table address 0050.3e8d.6400	Displays information about the MAC address table for a specific MAC address. The *mac-addr* is a 48–bit MAC address and the valid format is H.H.H.
Step 3	**show mac-address-table bridge-domain** *bridgedomain-id* **Example:** Router# show mac-address-table bridge-domain 100	Displays information about the MAC address table for a specific bridge domain. The *bridgedomain-id* is the bridge domain number.
Step 4	**show mac-address-table interface** *type number* **Example:** Router# show mac-address-table interface TenGigabitEthernet 4/1	Displays information about the MAC address table for a specific interface.
Step 5	Return to your originating procedure (NTP).	—

Example: Display Information About the MAC Address Table

The following example shows how to display the MAC address table information:

```
Router# show mac-address-table
```

```
BD Index   MAC Address     Type    Ports
-----------------------------------------
2          0000.1000.001e   dynamic   Te4/2
2          0000.1000.001d   dynamic   Te4/2
2          0000.1000.001c   dynamic   Te4/2
200        0050.3e8d.6400   static    Te4/1
100        0050.3e8d.6400   static    Te4/1
5          0050.3e8d.6400   static    Te4/1
4          0050.3e8d.6400   static    Te4/1
1          0050.3e8d.6400   static    Te4/1
```

The following example shows how to display the MAC address table information for a specific MAC address:

```
Router# show mac-address-table address 0000.1000.0001
```

```
BD Index   MAC Address     Type     Ports
-----------------------------------------
 2         0000.1000.0001  dynamic   Te4/2
```

The following example shows how to display the MAC address table information for a specific bridge domain:

```
Router# show mac-address-table bridge-domain 2
```

```
BD Index   MAC Address     Type    Ports
-----------------------------------------
2         0000.1000.001e   dynamic  Te4/2
2         0000.1000.001d   dynamic  Te4/2
2         0000.1000.001c   dynamic  Te4/2
2         0000.1000.001b   dynamic  Te4/2
2         0000.1000.001a   dynamic  Te4/2
2         0000.1000.0019   dynamic  Te4/2
```

The following example shows how to display the MAC address table information for a specific interface:

```
Router# show mac-address-table interface tenGigabitEthernet4/2
```

```
BD Index   MAC Address     Type    Ports
-----------------------------------------
2         0000.1000.001e  dynamic    Te4/2
2         0000.1000.001d  dynamic    Te4/2
2         0000.1000.001c  dynamic    Te4/2
2         0000.1000.001b  dynamic    Te4/2
2         0000.1000.001a  dynamic    Te4/2
2         0000.1000.0019  dynamic    Te4/2
```

The following example shows how to display the MAC address table information for a LAG interface (Po9):

```
Router# show mac-address-table
```

```
BD index   MAC Address     Type    Ports
-----------------------------------------
2          0000.0300.0900  dynamic  Te4/1
2          0000.0300.1000  dynamic  Po9
```

DLP-J28 Display Information About the MAC Address Table Using CTC

Purpose	This procedure displays information about the MAC address table using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to display information about the MAC address table.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 Click the **Maintenance** tab.

Step 5 From the left pane, click **MAC Learning**.

Step 6 To display information about the MAC address table for a specific MAC address:

a) Click the **MAC Addresses** subtab.
b) Enter the MAC address in the MAC address field.
c) Click **Show** to display information about the MAC address table for this MAC address.

Step 7 To display information about the MAC address table for a specific interface:

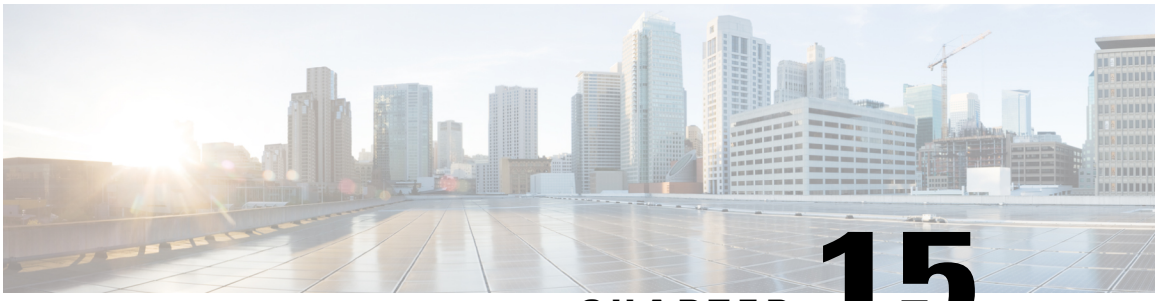
a) Click the **Interface** subtab.
b) From the Interface type drop-down list, choose **ONE_GE**, **TEN_GE**, or **PORT_CHANNEL**.
c) Enter the interface number in the Interface Number field.
d) Click **Show** to display information about the MAC address table for this interface.

Step 8 To display information about the MAC address table for a specific EFP:

a) From the View menu, choose **Go to Home View**
b) Click the **Layer2+** tab.
c) Click **Carrier Ethernet**.

d) From the list of EVC circuits, select an EVC circuit to edit.
e) Click **Edit**. The Edit Circuit dialog box appears.
f) Click the **MAC Learning** tab.
g) Click **Display MAC Address(es)** to display the configured static MAC addresses for each EFP. The Configured EFP Static MAC Addresses dialog box appears.
h) From the EFP drop-down list, choose an EFP.
i) The MAC addresses configured on the EFP appear in the Configured MAC Addresses area.
j) Close the Configured EFP Static MAC Addresses dialog box.

Step 9 Return to your originating procedure (NTP).



CHAPTER 15

Configuring Multicast VLAN Registration

This chapter describes Multicast VLAN Registration and procedures to configure Multicast VLAN Registration.

Using MVR in a Multicast Television Application

In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is an EFP configured as the MVR receiver. Figure 74: Multicast Bridge-Domain Registration Example, on page 597 is an example configuration. The DHCP assigns an IP address to the set-top box or the PC. When a subscriber selects a channel, the set-top box or PC sends an IGMP report to the CPT node (CPT 200 or CPT 600 along with CPT 50) to join the appropriate multicast. If the IGMP report matches one of the configured IP multicast group addresses, the CPT system modifies the hardware address table to include this receiver EFP and bridge-domain as a forwarding destination of the specified multicast stream when it is received from the multicast bridge-domain.

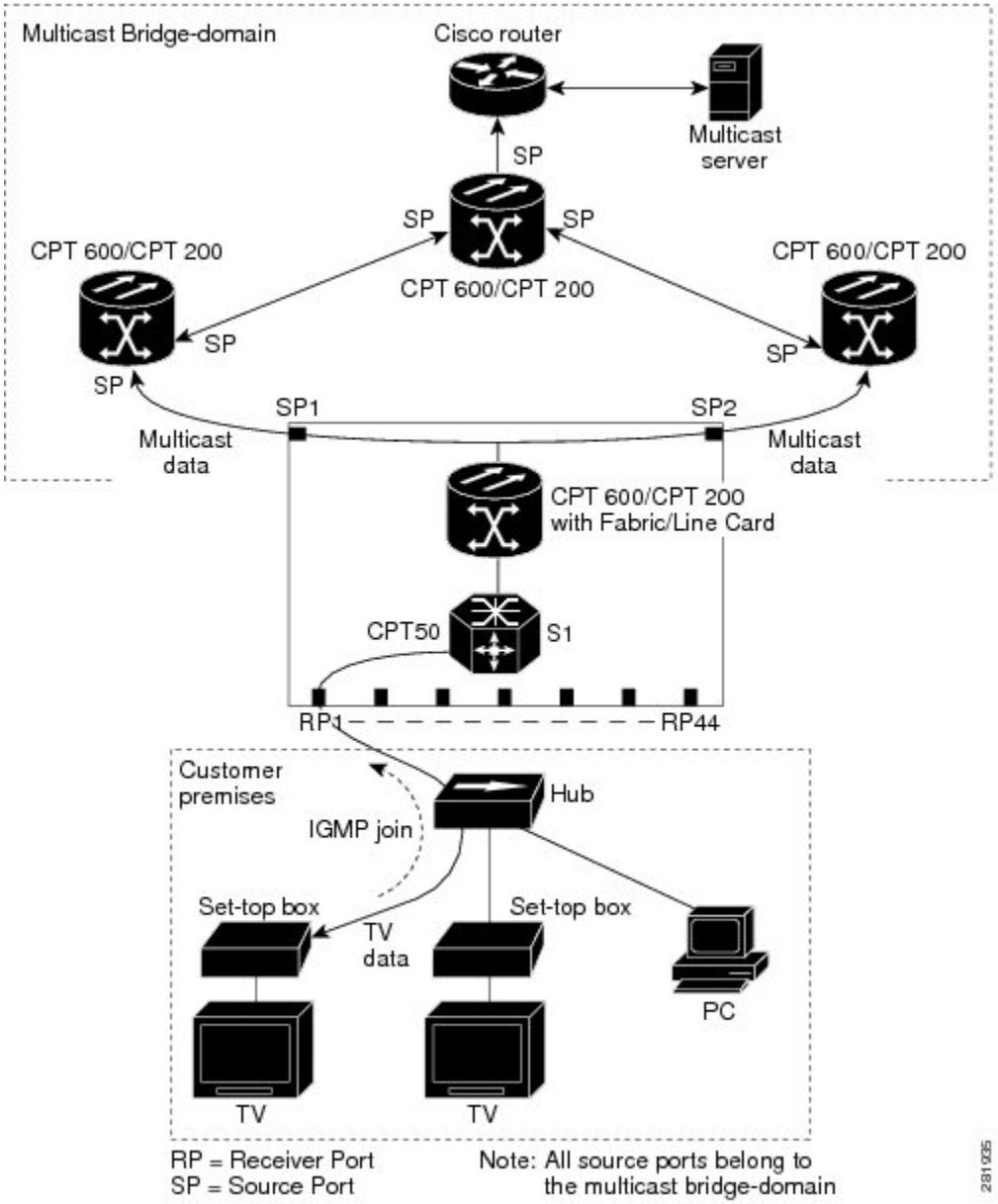
When a subscriber changes channels or turns off the television, the set-top box sends an IGMP leave message for the multicast stream. The CPT system sends a MAC-based general query through the receiver EFP bridge-domain. If there is another set-top box in the bridge-domain still subscribing to this group, that set-top box must respond within the maximum response time specified in the query. If the CPT system does not receive a response, it eliminates the receiver EFP as a forwarding destination for this group.

If the Immediate Leave feature is enabled on a receiver EFP, the EFP leaves a multicast group more quickly. Without Immediate Leave, when the CPT system receives an IGMP leave message from a subscriber on a receiver EFP, it sends out an IGMP group specific query on that EFP and waits for the IGMP group membership reports. If no reports are received in a configured time period, the receiver EFP is removed from the multicast group membership. With Immediate Leave, an IGMP query is not sent from the receiver EFP where the IGMP leave was received. As soon as the leave message is received, the receiver EFP is removed from the multicast group membership, which speeds up leave latency. Enable the Immediate Leave feature only on receiver EFPs to which a single receiver device is connected.

MVR eliminates the need to duplicate television-channel multicast traffic for subscribers in each bridge-domain. Multicast traffic for all channels is only sent around the bridge domain source EFPs —only on the multicast bridge-domain. The IGMP leave and join messages are in the bridge-domain to which the subscriber port is assigned. These messages dynamically register for streams of multicast traffic in the multicast bridge-domain on the Layer 3 device. The CPT node (CPT 200 or CPT 600 along with CPT 50) modifies the forwarding behavior to allow the traffic to be forwarded from the multicast bridge domain to the subscriber port in a different bridge-domain, thereby selectively allowing traffic to cross between the two bridge-domains.

IGMP reports are sent to the same IP multicast group address as the multicast data. The CPT node (CPT 200 or CPT 600 along with CPT 50) must capture all IGMP join and leave messages from the receiver EFPs and forward them to the multicast bridge domain of the source EFP.

Figure 74: Multicast Bridge-Domain Registration Example



Configuring Multicast VLAN Registration

This section provides MVR configuration guidelines and limitations, and procedures to configure MVR using Cisco IOS commands and CTC.

MVR Configuration Guidelines and Limitations

- Receiver EFPs on a CPT system can be in different bridge-domains, but should not belong to the multicast bridge-domain.
- The maximum number of multicast entries (MVR group addresses) that can be configured on a CPT system is 2000.
- The CPT system supports up to 20 MVR bridge-domains.
- The maximum number of receiver EFPs on an MVR bridge-domain is 128.
- Because an MVR on the CPT system uses IP multicast addresses instead of MAC multicast addresses, aliased IP multicast addresses are allowed on the CPT system.
- MVR can coexist with IGMP snooping on a CPT system.
- MVR data received on an MVR receiver EFP is not forwarded to MVR source EFPs.
- A physical port can have only one receiver EFP for a given MVR bridge domain.
- CPT system does not support MVR in point to point bridge-domains.
- Query response time is 0.5 second.
- It is mandatory to untag the packets before they enter the bridge domain:
  - For an MVR source, the packets are untagged using the **rewrite pop** configuration at the EFP level.
  - For an MVR receiver, the **rewrite pop** operation is implicit. User-defined rewrite operation is used for bridge-domains that do not have MVR enabled.
- Following configuration restrictions are applicable while configuring MVR source EFPs on the CPT system:
  - For a single tagged packet, the tag is removed using the **rewrite ingress tag pop 1 symmetric** command at the EFP level.
  - For a double tagged packet, the tag is removed using the **rewrite ingress tag pop 2 symmetric** command at the EFP level.
  - For an untagged packet, a rewrite operation is not required.

To configure MVR using Cisco IOS commands, see NTP-J69 Configuring MVR Using Cisco IOS Commands, on page 598.

To configure MVR using CTC, see NTP-J70 Configuring MVR Using CTC, on page 608.

NTP-J69 Configuring MVR Using Cisco IOS Commands

Purpose	This procedure configures MVR using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None

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

Procedure

Step 1 Complete the DLP-J210 Enabling or Disabling MVR on a Bridge Domain Using Cisco IOS Commands , on page 599.

Step 2 Complete the DLP-J211 Enabling or Disabling MVR on the Source and Receiver EFPs Using Cisco IOS Commands, on page 601.

Step 3 (Optional) Complete the DLP-J229 Viewing MVR Configuration Using Cisco IOS Commands, on page 606.
Stop. You have completed this procedure.

DLP-J210 Enabling or Disabling MVR on a Bridge Domain Using Cisco IOS Commands

Purpose	This procedure enables or disables MVR on a bridge domain using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**bridge domain** *bridge-domain value* **Example:** Router(config)# bridge-domain 22	Enters the bridge-domain configuration mode. • Enter the value of the bridge-domain.
Step 4	**[no] mvr** **Example:** Router(config-bdomain)# mvr	Enables MVR on the bridge-domain. The **no** form of the command disables MVR.
Step 5	**[no] mvr group** *ip-address count* **Example:** Router(config-bdomain)# mvr group 228.1.23.4 5	Defines a global range of IP multicast groups on which MVR must be enabled. The optional count parameter is used to configure a contiguous series of MVR group addresses (the range for count is from 1 to 2000; the default is 1). Any multicast data sent to the IP address mentioned in the command is sent to all source EFPs on the CPT system and all receiver EFPs that have elected to receive data on that multicast address. The **no** form of the deletes the multicast IP address configuration. *ip-address*—Group IP address. *count*—Group count inside the bridge domain.
Step 6	**end** **Example:** Router(config-bdomain)# end	Exits the bridge domain configuration mode and returns to privileged EXEC mode.
Step 7	**show mvr** **Example:** Router#show mvr	Verifies the configuration.
Step 8	**copy running-config startup-config** **Example:** copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Examples:

The following example shows how to enable MVR on bridge domain 22 and configure the group address.

```
Router(config)# bridge-domain 22
Router(config-bdomain)# mvr
Router(config-bdomain)# mvr group 228.1.23.4 5
Router(config-bdomain)# end
```

The following example shows how to disable MVR on bridge domain 22 and group address.

```
Router(config)# bridge-domain 22
Router(config-bdomain)# no mvr
```

```
Router(config-bdomain)# no mvr group 228.1.23.4 5
Router(config-bdomain)# end
```

The following example shows how to verify the MVR multicast group addresses on the CPT system.

```
Router# show mvr groups
```

```
MVR multicast VLAN: 20
MVR max Multicast Groups allowed: 2000
MVR current multicast groups: 20
MVR groups:

        Group start     Group end       Type  Count/Mask
        --------------- --------------- ----- ---------------
        230.1.2.3       230.1.2.22      count 20
```

DLP-J211 Enabling or Disabling MVR on the Source and Receiver EFPs Using Cisco IOS Commands

Purpose	This procedure enables or disables MVR on the source and receiver EFPs: • Step 1 through Step 9 explains MVR configuration of the source EFP. • Step 10 through Step 15 explains MVR configuration of the receiver EFP.
Tools/Equipment	None
Prerequisite Procedures	DLP-J210 Enabling or Disabling MVR on a Bridge Domain Using Cisco IOS Commands , on page 599
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Note Users must configure an MVR bridge domain before configuring the MVR source and receiver EFPs.

The **mvr type {source | receiver bridge-domain** *id* **[***vlan id***] [immediate]}** command is used to configure the EFPs, where **bridge-domain** *id* **[***vlan id***] [immediate]** is only applicable to the receiver EFPs.

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Router> enable	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TengigabitEthernet 4/1	Specifies the type and location of the interface to configure, where: • *type*—Specifies the type of the interface. • *number*—Specifies the location of the interface.
Step 4	**service instance** *id* **ethernet** **Example:** Router(config-if)# service instance 10 ethernet	Configures an Ethernet service instance on an interface.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** Router(config-if-srv)# encapsulation dot1q 10	Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.
Step 6	**rewrite ingress tag pop {1|2} symmetric** **Example:** Router(config-if-srv)# rewrite ingress tag pop 1 symmetric	Specifies the rewrite operation.
Step 7	**bridge-domain** *bridge-domain id* **Example:** Router(config-if-srv)# bridge-domain 22	Enters the bridge-domain
Step 8	**[no] mvr type source** **Example:** Router(config-if-srv)#mvr type source	Configures an MVR EFP as the source. Subscribers cannot be directly connected to the source EFPs. All source EFPs on a CPT system belong to the single multicast bridge-domain. The **no** form of the command removes the MVR source EFP configuration.
Step 9	exit **Example:** exit	Exits the service instance mode.

	Command or Action	Purpose
Step 10	**interface** *type number* **Example:** Router(config)# interface TengigabitEthernet 6/3	Specifies the type and location of the interface to configure. • *type*—Type of the interface. • *number*—Location of the interface.
Step 11	**service instance** *id* **ethernet** **Example:** Router(config-if)# service instance 100 ethernet	Configures an Ethernet service instance on an interface.
Step 12	**encapsulation dot1q** {*vlan-id* | *vlan-range*} **Example:** • Router(config-if-srv)# encapsulation dot1q 10 or • Router(config-if-srv)# encapsulation dot1q 100-1000	Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.
Step 13	**bridge-domain** *bridge-domain id* **Example:** Router(config-if-srv)# bridge-domain 100	Enters the bridge-domain
Step 14	**[no] mvr type receiver bridge-domain** *id* **[vlan** *vlan-id***] [immediate]** **Example:** • Router(config- if-srv)# mvr type receiver bridge-domain 22 immediate or • Router(config-if-srv)# mvr type receiver bridge-domain 22 vlan 200	Configures an MVR EFP (subscriber port) as the receiver to receive only multicast data. It does not receive data unless it becomes a member of the multicast group, either statically or by using IGMP leave and join messages. Receiver EFPs cannot belong to the multicast bridge-domain. The **no** form of the command removes the MVR receiver EFP configuration. **immediate—** (Optional) Enables the Immediate-Leave feature on the receiver EFP. **Note** This command applies to only receiver EFPs and should only be enabled on receiver EFPs to which a single receiver device is connected. **vlan** *vlan-id***—** (Optional) Specifies the VLAN ID to be used when the VLAN range is mentioned. This option is used only on the receiver EFP.

	Command or Action	Purpose
Step 15	end **Example:** Router(config-if-srv)# end	Returns to privileged EXEC mode.
Step 16	**show mvr** **Example:** Router(config)# show mvr	Verifies the configuration.
Step 17	**copy running-config startup-config** **Example:** copy running-config startup-config	(Optional) Saves your entries in the configuration file.

To return the CPT system to its default settings, use the **no mvr [type** *type*| **immediate | vlan** *vlan-id***]** command in the interface configuration mode.

Examples:

This example shows how to configure an EFP as a receiver and receive multicast traffic sent to the multicast group address. It also shows how to enable Immediate Leave on the receiver EFP and verify the results.

```
Router(config)# interface TengigabitEthernet 6/3
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mvr type receiver bridge-domain 22 immediate
end
Router(config)#show mvr receiver
```

This example shows how to disable MVR on the receiver EFP.

```
Router(config)# interface TengigabitEthernet 6/3
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# no mvr type receiver bridge-domain 22 immediate
Router(config-if-srv)# no service instance 100 ethernet
```

This example shows how to configure an EFP as a receiver with encapsulation range, and receive multicast traffic sent to the multicast group address. It also shows how to enable Immediate Leave on the receiver EFP.

```
Router(config)# interface gi36/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 100-1000
Router(config-if-srv)# rewrite ingress tag push dot1q 100 symmetric
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mvr type receiver bridge-domain 22 immediate vlan 200
```

This example shows how to configure an EFP as a receiver with encapsulation ID, and receive multicast traffic sent to the multicast group address. It also shows how to enable Immediate Leave on the receiver EFP.

```
Router(config)# interface gi36/2
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag push dot1q 100 symmetric
```

```
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mvr type receiver bridge-domain 22 immediate
```

This example shows how to enable MVR on the source EFP.

```
Router(config)# TengigabitEthernet 6/3
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 12
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 22
Router(config-if-srv)# mvr type source
```

This example shows how to disable MVR on the source EFP.

```
Router(config)# TengigabitEthernet 6/3
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# no mvr type source
Router(config-if-srv)# no service instance 100 ethernet
```

This example shows how to enable MVR on the bridge domains and configure source MVR EFPs and receiver MVR EFPs.

```
! Enabling MVR on the bridge domain 22 and bridge domain 30.
Router(config)# bridge-domain 22
Router(config-bdomain)# mvr
Router(config-bdomain)# mvr group 225.0.0.1 5
Router(config-bdomain)# end

Router(config)# bridge-domain 30
Router(config-bdomain)# mvr
Router(config-bdomain)# mvr group 226.0.0.1 5

! Configuring source EFP on the bridge domain 22.
Router(config)# TengigabitEthernet 6/3
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 12
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 22
Router(config-if-srv)# mvr type source

! Configuring receiver EFP on the bridge domain 50.
Router(config)# interface TengigabitEthernet 5/3
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 50
Router(config-if-srv)# mvr type receiver bridge-domain 22 immediate


! Configuring source EFP on the bridge domain 30.
Router(config)# TengigabitEthernet 4/3
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 12
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 30
Router(config-if-srv)# mvr type source

! Configuring receiver EFP on the bridge domain 60.
Router(config)# interface TengigabitEthernet 2/3
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag push dot1q 100 symmetric
Router(config-if-srv)# bridge-domain 60
Router(config-if-srv)# mvr type receiver bridge-domain 30 immediate

! Configuring receiver EFP on the bridge domain 60 encapsulation range.
Router(config)# interface TengigabitEthernet 2/4
Router(config-if)# service instance 200 ethernet
Router(config-if-srv)# encapsulation dot1q 10-1000
```

```
Router(config-if-srv)# bridge-domain 60
Router(config-if-srv)# mvr type receiver bridge-domain 30 immediate vlan 20
```

DLP-J229 Viewing MVR Configuration Using Cisco IOS Commands

Purpose	This procedure explains how to view MVR configuration using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show mvr [source-ports] [receiver-ports] [groups]** **Example:** Router# show mvr	Displays MVR status and values for all the bridge-domains where MVR is enabled. It provides the number of groups configured per bridge domain and displays all receiver and source EFPs.
Step 3	**show ip igmp snooping [groups] [querier]** **Example:** Router# show ip igmp snooping	(Optional) Displays the querier and snooping information.

Examples

This example shows how to view MVR receiver port configuration.

```
Router# show mvr receiver-ports
```

```
Joins: v1,v2,v3 counter shows total IGMP joins
       v3 counter shows IGMP joins received with both MVR and non-MVR
groups
Port       VLAN   Status            Immediate             Joins
                                    Leave          (v1,v2,v3)    (v3)
```

```
---------  ----   -------------     ----------     ---------- ----------
Po10        100   ACTIVE  /UP       DISABLED                0          0
Gi40/2      100   ACTIVE  /UP       DISABLED                0          0
Po10        200   ACTIVE  /UP       DISABLED                0          0
Gi40/2      101   ACTIVE  /UP       DISABLED                0          0
```

This example shows how to view MVR source port configuration.

```
Router# show mvr source-ports
```

```
Joins: v1,v2,v3 counter shows total IGMP joins
       v3 counter shows IGMP joins received with both MVR and non-MVR
groups
Port       VLAN   Status            Immediate             Joins
                                    Leave          (v1,v2,v3)    (v3)
---------  ----   -------------     ----------     ---------- ----------
Gi36/2        1   ACTIVE  /UP       DISABLED                0          0
Gi36/2        2   ACTIVE  /UP       DISABLED                0          0
```

This example shows how to view MVR group details.

```
Router#  show mvr groups
```

```
MVR multicast VLAN: 1
MVR max Multicast Groups allowed: 2000
MVR current multicast groups: 60
MVR groups:

        Group start     Group end       Type  Count/Mask
        --------------- --------------- ----- ---------------
        224.1.1.1       224.1.1.20      count 20
        225.1.1.1       225.1.1.20      count 20
        229.1.1.1       229.1.1.10      count 10
        230.1.1.1       230.1.1.10      count 10

MVR multicast VLAN: 2
MVR max Multicast Groups allowed: 2000
MVR current multicast groups: 60
MVR groups:

        Group start     Group end       Type  Count/Mask
        --------------- --------------- ----- ---------------
        224.1.1.1       224.1.1.20      count 20
        225.1.1.1       225.1.1.20      count 20
        229.1.1.1       229.1.1.10      count 10
        230.1.1.1       230.1.1.10      count 10
```

This example shows how to view snooping details.

```
Router# show ip igmp snooping groups
```

```
Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode

Vlan      Group/source             Type        Version     Port List
------------------------------------------------------------------------
1         229.1.1.1                I           v3          Po10 Gi40/2
```

```
1          229.1.1.2                  I            v3           Po10 Gi40/2
1          229.1.1.3                  I            v3           Po10 Gi40/2
1          229.1.1.4                  I            v3           Po10 Gi40/2
1          229.1.1.5                  I            v3           Po10 Gi40/2
1          229.1.1.6                  I            v3           Po10 Gi40/2
1          229.1.1.7                  I            v3           Po10 Gi40/2
1          229.1.1.8                  I            v3           Po10 Gi40/2
1          229.1.1.9                  I            v3           Po10 Gi40/2
1          229.1.1.10                 I            v3           Po10 Gi40/2
```

This example shows how to view querier details.

```
Router# show ip igmp snooping querier
```

```
Vlan      IP Address               IGMP Version   Port
-----------------------------------------------------------------
1         12.12.12.12              v3             Gi36/2
```

This example shows how to view generic MVR details.

```
Router# show mvr
```

```
MVR Running: TRUE
MVR multicast VLAN: 2
MVR Max Multicast Groups: 2000
MVR Current multicast groups: 100
MVR Global query response time: 5 (tenths of sec)
```

NTP-J70 Configuring MVR Using CTC

Purpose	This procedure explains how to enable MVR on the bridge domain, create a source MVR EFP, a receiver MVR EFP, and disable MVR.
Tools/Equipment	None

Prerequisite Procedures	Create an Ethernet Virtual Private LAN EVC circuit with the following conditions: • Type of VLAN Tagging: ◦ Double Tagged ◦ Single Tagged ◦ Untagged • Rewrite Operation: ◦ POP 1 for Single Tagged ◦ POP 2 for Double Tagged ◦ N/A for Untagged **Note** While creating an EVPLAN circuit, the source EFP and the receiver EFP of the same MVR bridge domain cannot be present on the same physical port. To create an EVC circuit, seeDLP-J2 Create an EVC Circuit Using CTC, on page 143 .
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Note An MVR source is configured on the EVPLAN circuit that has MVR enabled; however, an MVR receiver is configured on the EVPLAN circuit that does not have MVR enabled.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to enable MVR.

Step 2 In the node view, click the **Layer2+** tab.

Step 3 Click **Carrier Ethernet.**

Step 4 From the list of Ethernet Virtual Circuits (EVCs), select an Ethernet Virtual Private LAN EVC circuit to enable MVR.

Step 5 Click **Edit**. The Edit Circuit dialog box appears. In the **MVR** tab, specify the multicast settings for the bridge domain as described in the subsequent steps.

Step 6 To enable MVR on the bridge domain, do the following:

a) Check the **MVR** check box to enable MVR for this bridge domain.

Note To disable MVR, uncheck the **MVR** check box.

b) Click **Apply**.

Step 7 To add multicast IP addresses for the bridge domain, do the following:

a) Check **Multicast IP Address Configuration**. The Multicast IP Addresses dialog box appears.

b) Enter one or more multicast IP address in the IP Address field and click **Add**. The added multicast addresses appear in the IP Addresses area.

Note When the EVPLAN circuit spans across more than one node in the network, the Multicast IP address configuration must be performed on all those nodes.

c) Click **Apply**.

Step 8 To create an MVR source EFP, do the following:

a) From the MVR Type drop-down list, choose **Source** for each EFP.

Note Choose **None** to remove the MVR type from the EFP.

b) Enter one or more multicast IP address in the IP Address field and click **Add**. The added multicast addresses appear in the IP Addresses area.

c) Click **Apply** and close the Multicast IP Addresses dialog box.

Step 9 To create an MVR receiver EFP, do the following:

a) From the MVR Type drop-down list, choose **Receiver** for each EFP.

Note Choose **None** to remove the MVR type from the EFP.

b) Click the Source Service ID field and select an MVR enabled service.

c) Check the **Immediate Leave** check box. When you enable Immediate Leave, MVR immediately removes a port when it detects a leave message on that port.

Note In case of VLAN range in the MVR receiver configuration, specify the Egress VLAN ID.

d) Click **Apply**.

Step 10 To disable MVR on the bridge-domain, source MVR EFP, or receiver MVR EFP, do the following:

a) Choose **None** to remove the MVR type from the EFP.

b) Delete the multicast IP address configuration.

c) Uncheck the **MVR** check box.

Step 11 To view the MVR configuration, refer to the procedure explained in DLP-J56 Open the Cisco IOS Configuration Mode and View the Feature Configuration Details Using CTC, on page 10.

MVR Interaction with LAG

We can add a LAG interface to a bridge domain which has MVR enabled.

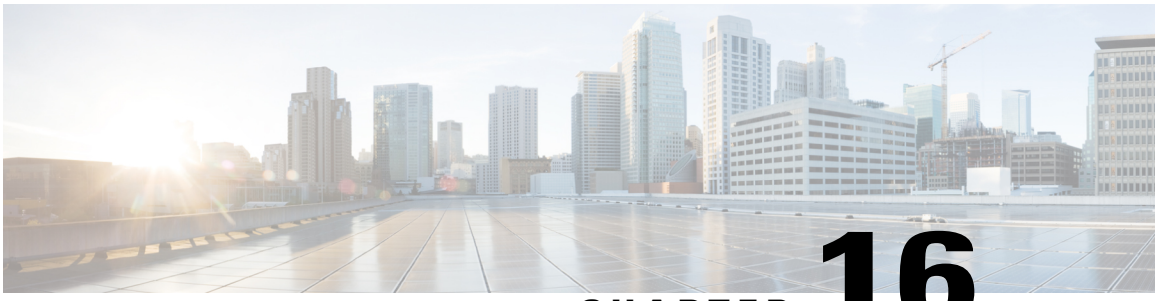
The following example shows the source EFP configuration, which is part of the LAG interface that is a member of the MVR-enabled bridge domain.

```
! Enabling MVR on the bridge domain.
Router(config)# bridge-domain 30
Router(config-bdomain)# mvr
Router(config-bdomain)# mvr group 239.0.0.1 10

! Configuring source EFP on the bridge domain 30.
Router(config)# interface port-channel 10
```

```
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# bridge-domain 30
Router(config-if-srv)# mvr type source
Router(config-if-srv)# exit

! Adding members to the port channel interface.
Router(config)# interface ten 6/1
Router(config-if)# channel-group 10

Router(config)# interface ten 6/2
Router(config-if)# channel-group 10

! Configuring receiver EFP on the bridge domain 100.
Router(config)# interface gi36/5
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mvr type receiver bridge-domain 30

! Configuring receiver EFP on the bridge domain 200.
Router(config)# interface gi36/6
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# rewrite ingress tag push dot1q 100 symmetric
Router(config-if-srv)# bridge-domain 200
Router(config-if-srv)# mvr type receiver bridge-domain 30
```

The following example shows the receiver EFP configuration, which is part of the LAG interface.

```
! Enabling MVR on the bridge domain.
Router(config)# bridge-domain 30
Router(config-bdomain)# mvr
Router(config-bdomain)# mvr group 228.1.23.4 5
Router(config-bdomain)# end

! Configuring the source EFP.
Router(config)# interface ten 6/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10 second-dot1q 30
Router(config-if-srv)# bridge-domain 30
Router(config-if-srv)# mvr type source

! Configuring the receiver EFP.
Router(config)# interface port-channel 10
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mvr type receiver bridge-domain 30

! Adding members to the port channel interface.
Router(config)# interface gi36/5
Router(config-if)# channel-group 10

Router(config)# interface gi36/6
Router(config-if)# channel-group 10

! Configuring the receiver EFP.
Router(config)# interface gi36/6
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# rewrite ingress tag push dot1q 100 symmetric
Router(config-if-srv)# bridge-domain 200
Router(config-if-srv)# mvr type receiver bridge-domain 30
```



CHAPTER 16

Configuring IGMP Snooping

This chapter describes IGMP Snooping and procedures to configure IGMP Snooping.

Understanding IGMP Snooping

As networks increase in size, multicast routing becomes critically important as a means to determine which segments require multicast traffic and which do not. IP multicasting enables IP traffic to be propagated from one source to a number of destinations, or from many sources to many destinations. Rather than sending one packet to each destination, one packet is sent to the multicast group identified by a single IP destination group address.

Internet Group Management Protocol (IGMP) snooping restricts flooding of multicast traffic by sending multicast traffic only to the interfaces that are subscribed to a particular multicast group.

The Carrier Packet Transport (CPT) system can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the CPT system to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups

and member ports. When the CPT system receives an IGMP report from a host for a particular multicast group, the CPT system adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

Note For more information on IP multicast and IGMP, see RFC 1112, RFC 2236, and RFC 3376.

The CPT system forwards periodic general queries received from the multicast router in the bridge domain where IGMP snooping is enabled. All hosts interested in this multicast group send join requests and are added to the forwarding table entry. The CPT system creates one entry per bridge domain in the IGMP snooping IP multicast forwarding table for each group from which it receives an IGMP join request.

The IP multicast groups learned through IGMP snooping are dynamic.

If a port interface, EFP, and bridge domain state changes, the IGMP snooping-learned multicast groups from this port, EFP, and bridge domain in the bridge domain are deleted.

IGMP Versions

The CPT system supports IGMP version 1, IGMP version 2, and IGMP version 3 on a bridge domain level. The CPT system does snooping using L2 multicast address and not L3 IP address.

Note The CPT system supports IGMPv3 snooping based only on the destination multicast MAC address and not on the the source IP address or on proxy reports.

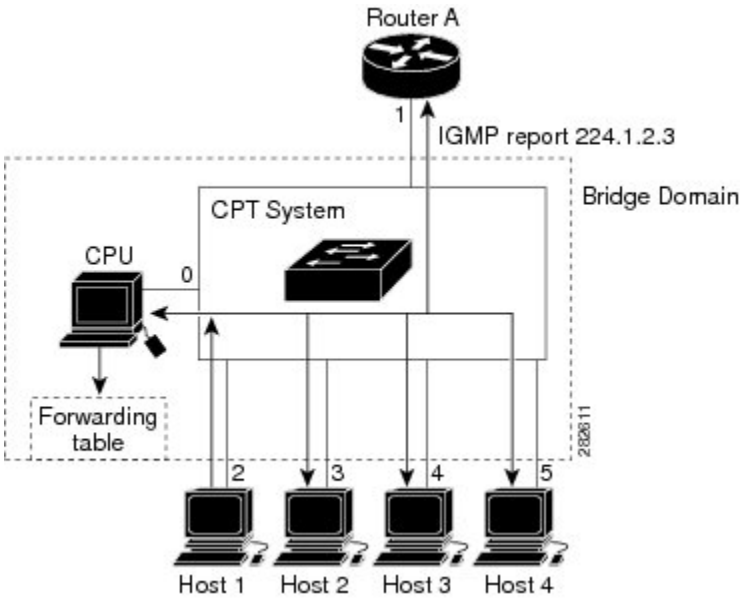
An IGMPv3 CPT system provides Basic IGMPv3 Snooping Support (BISS), which includes support for the snooping features on IGMPv1 and IGMPv2 switches and for IGMPv3 membership report messages. BISS constrains the flooding of multicast traffic when the network includes IGMPv3 hosts. It constrains traffic to approximately the same set of ports as the IGMP snooping feature on IGMPv1 or IGMPv2 hosts.

Joining a Multicast Group

When a host connected to the CPT system wants to join an IP multicast group and it is an IGMP version 2 or version 3 client, it sends an unsolicited IGMP join message, specifying the IP multicast group to join. Alternatively, when the CPT system receives a general query from the router, it forwards the query to all the EFPs in the bridge domain. IGMP hosts wanting to join the multicast group respond by sending a join message to the CPT system. The CPT system CPU creates a multicast forwarding-table entry for the group if it is not already present. The CPU also adds the interface where the join message was received to the forwarding-table

entry. The host associated with that interface receives multicast traffic for that multicast group. See Figure 75: Initial IGMP Join Message , on page 615.

Figure 75: Initial IGMP Join Message



Router A sends a general query to the CPT system, which forwards the query to ports 2 through 5, which have EFPs configured in the same bridge domain. Host 1 wants to join multicast group 224.1.2.3 and multicasts an IGMP membership report (IGMP join message) to the group. The CPT system CPU uses the information in the IGMP report to set up a forwarding-table entry as shown in Table 29: IGMP Snooping Forwarding Table, on page 615, which includes the port numbers connected to Host 1 and the router.

Table 29: IGMP Snooping Forwarding Table

Destination Address	Type of Packet	Ports
224.1.2.3	IGMP	1, 2

The CPT system hardware can distinguish IGMP information packets from other packets for the multicast group. The information in the table enables the switching engine to send frames addressed to the 224.1.2.3 multicast IP address, which are not IGMP packets, to the router and to the host that has joined the group.

If another host (for example, Host 4) sends an unsolicited IGMP join message for the same group (Figure 76: Second Host Joining a Multicast Group , on page 616) the CPU receives that message and adds the port number of Host 4 to the forwarding table as shown in Table 30: Updated IGMP Snooping Forwarding Table, on page

616. Note that because the forwarding table directs IGMP messages only to the CPU, the message is not flooded to other ports on the CPT system. Any known multicast traffic is forwarded to the group and not to the CPU.

Figure 76: Second Host Joining a Multicast Group

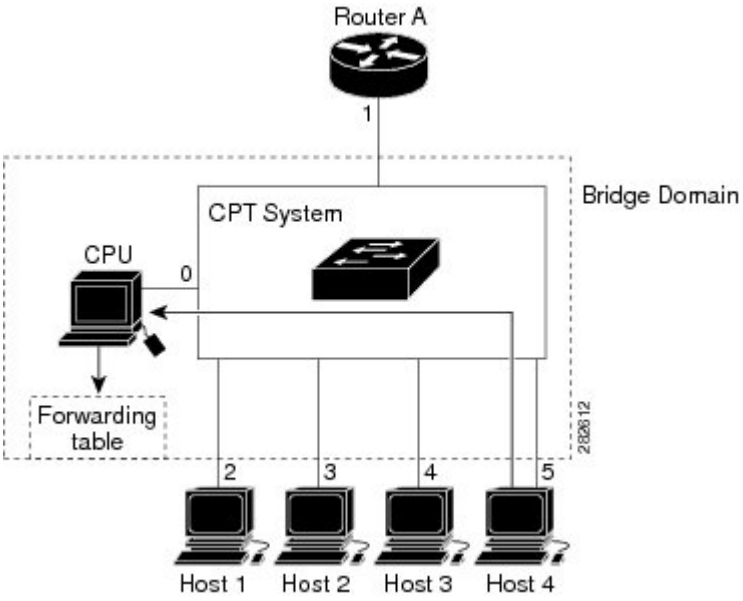


Table 30: Updated IGMP Snooping Forwarding Table

Destination Address	Type of Packet	Ports
224.1.2.3	IGMP	1, 2, 5

IGMP Snooping Configuration Guidelines and Restrictions

- On a CPT system, IGMP snooping can be configured at the bridge domain level.
- **IGMP immediate-leave** and **IGMP report-suppression** commands can be configured at the bridge domain level.
- Static multicast router can be configured at the EFP level.
- It is mandatory to untag the packets before they enter the bridge domain. This is achieved using the **rewrite pop** configuration at the EFP level.
- Following configuration restrictions are applicable while configuring the IGMP snooping on the CPT system:
  - For a single tagged packet, the tag is removed using the **rewrite ingress tag pop 1 symmetric** command at the EFP level.
  - For a double tagged packet, the tag is removed using the **rewrite ingress tag pop 2 symmetric** command at the EFP level.
  - For an untagged packet, a rewrite operation is not required.

NTP-J64 Configuring IGMP Snooping Using Cisco IOS Commands

Purpose	This procedure configures IGMP snooping using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

Step 1 Complete DLP-J217 Enabling or Disabling IGMP Snooping Using Cisco IOS Commands, on page 617.

Step 2 Complete the following tasks as necessary:

- DLP-J218 Enabling or Disabling IGMP Immediate Leave Using Cisco IOS Commands, on page 620
- DLP-J219 Disabling IGMP Report Suppression Using Cisco IOS Commands , on page 622
- DLP-J220 Configuring a Static Multicast Router Port Using Cisco IOS Commands , on page 623

Step 3 (Optional) Complete the DLP-J230 Viewing IGMP Configuration Using Cisco IOS Commands, on page 626.

Stop. You have completed this procedure.

DLP-J217 Enabling or Disabling IGMP Snooping Using Cisco IOS Commands

Purpose	This procedure enables or disables IGMP snooping using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**bridge domain** *bridge-domain value* **Example:** Router(config)# bridge-domain 22	Enters the bridge-domain. • Enter the value of the bridge-domain.
Step 4	**[no] ip igmp snooping** **Example:** Router(config-bdomain)# ip igmp snooping	Enables IGMP snooping on the bridge-domain. The **no** form of the command disables IGMP snooping.
Step 5	end **Example:** Router(config-bdomain)# end	Returns to the privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Examples:

The following example shows how to enable IGMP snooping on untagged Ethernet traffic on the bridge domain and how to configure the source and host ports:

```
! Configuration on the bridge-domain
Router(config)# bridge-domain 30
Router(config-bdomain)# ip igmp snooping

! Configuration on port 1
Router(config)# interface gi 36/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation untagged
Router(config-if-srv)# bridge-domain 30

! Configuration on port 2
Router(config)# interface gi 36/5
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation untagged
Router(config-if-srv)# bridge-domain 30
```

```
! Configuration on port 3
Router(config)# interface gi 36/10
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation untagged
Router(config-if-srv)# bridge-domain
```

The following example shows how to enable IGMP snooping on single and double tagged Ethernet traffic on the bridge domain and how to configure the source and host ports:

```
! Configuration on the bridge-domain
Router(config)# bridge-domain 30
Router(config-bdomain)# ip igmp snooping

! Configuration on port 1
Router(config)# interface gi 36/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 50 second-dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 2 symmetric
Router(config-if-srv)# bridge-domain 30

! Configuration on port 2
Router(config)# interface gi 36/2
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 200
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 30

! Configuration on port 3
Router(config)# interface gi 36/5
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 30
```

The following example shows how to enable IGMP snooping on double tagged Ethernet traffic on the bridge domain and how to configure the source and host ports::

```
! Configuration on the bridge-domain
Router(config)# bridge-domain 30
Router(config-bdomain)# ip igmp snooping

! Configuration on port 1
Router(config)# interface gi 36/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10 second-dot1q 20
Router(config-if-srv)# rewrite ingress tag pop 2 symmetric
Router(config-if-srv)# bridge-domain 30

! Configuration on port 2
Router(config)# interface gi 36/5
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 100 second-dot1q 20
Router(config-if-srv)# rewrite ingress tag pop 2 symmetric
Router(config-if-srv)# bridge-domain 30

! Configuration on port 3
Router(config)# interface gi 36/6
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 101 second-dot1q 20
Router(config-if-srv)# rewrite ingress tag pop 2 symmetric
Router(config-if-srv)# bridge-domain 30
```

Leaving a Multicast Group

The router sends periodic multicast general queries, and the CPT system forwards these queries through all ports in the bridge domain. Interested hosts respond to the queries. If at least one host in the bridge domain wants to receive multicast traffic, the router continues forwarding the multicast traffic to the bridge domain. The CPT system forwards multicast group traffic only to those hosts listed in the forwarding table for that IP multicast group maintained by IGMP snooping.

When hosts want to leave a multicast group, they can leave without sending a message, or they can send a leave message. When the CPT system receives a leave message from a host, it sends a group-specific query to learn if any other devices connected to that interface are interested in traffic for the specific multicast group. The CPT system then updates the forwarding table for that MAC group so that only those hosts interested in receiving multicast traffic for the group are listed in the forwarding table. If the router receives no reports from a bridge domain, it removes the group for the bridge domain from its IGMP cache.

Immediate Leave

The Immediate Leave feature is only supported on IGMP version 2 hosts. The CPT system uses IGMP Snooping Immediate Leave feature to remove an interface from the forwarding table, which sends a leave message without the CPT system sending group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. The Immediate Leave feature ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are simultaneously in use.

Note You should only use the Immediate Leave feature on bridge domains where a single host is connected to each port. If this feature is enabled on bridge domains where more than one host is connected to a port, some hosts might get dropped.

DLP-J218 Enabling or Disabling IGMP Immediate Leave Using Cisco IOS Commands

When you enable the IGMP Immediate Leave feature, the CPT system immediately removes a port when it detects an IGMP version 2 leave message on that port. You should use the Immediate Leave feature only when there is a single receiver present on every port in the bridge domain.

Note The Immediate Leave feature is supported only on IGMP version 2 hosts.

Purpose	This procedure enables or disables IGMP Immediate Leave feature using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J217 Enabling or Disabling IGMP Snooping Using Cisco IOS Commands, on page 617
Required/As Needed	As needed

Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**bridge domain** *bridge-domain value* **Example:** Router(config)# bridge-domain 22	Enters the bridge domain configuration mode. • Enter the value of the bridge-domain.
Step 4	**[no] ip igmp snooping immediate-leave** **Example:** Router(config-bdomain)# ip igmp snooping immediate-leave	Enables the IGMP Immediate Leave feature on the bridge domain. The **no** form of the command disables IGMP snooping immediate-leave.
Step 5	end **Example:** Router(config-bdomain)# end	Returns to the privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** copy running-config startup-config	(Optional) Saves your entries in the configuration file.

To disable the IGMP Immediate Leave feature on a bridge domain, use the **no ip igmp snooping immediate-leave** global configuration command.

Examples:

The following example shows how to enable IGMP Immediate Leave feature for bridge-domain130:

```
Router# configure terminal
Router(config)# bridge-domain 130
Router(config-bdomain)# ip igmp snooping immediate-leave
Router(config-bdomain)# end
```

IGMP Report Suppression

Note IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The CPT system uses IGMP report suppression to forward only one IGMP report per multicast router query, to multicast devices. When IGMP router suppression is enabled (the default), the CPT system sends the first IGMP report from all hosts for a group, to all the multicast routers. The CPT system does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the CPT system forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all the multicast routers.

If the multicast router query also includes requests for IGMPv3 reports, the CPT system forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression, all IGMP reports are forwarded to the multicast routers.

DLP-J219 Disabling IGMP Report Suppression Using Cisco IOS Commands

Note IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

IGMP report suppression is enabled by default. When it is enabled, the CPT system forwards only one IGMP report per multicast router query. When report suppression is disabled, all IGMP reports are forwarded to the multicast routers. To re-enable IGMP report suppression, use the **ip igmp snooping report-suppression** command in the bridge domain configuration mode.

Purpose	This procedure disables IGMP report suppression using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J217 Enabling or Disabling IGMP Snooping Using Cisco IOS Commands, on page 617
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**bridge domain** *bridge-domain value* **Example:** Router(config)# bridge-domain 22	Enters the bridge domain configuration mode. • Enter the value of the bridge domain.
Step 4	**no ip igmp snooping report-suppression** **Example:** Router(config-bdomain)# no ip igmp snooping report-suppression	Disables IGMP report suppression.
Step 5	end **Example:** Router(config-bdomain)# end	Returns to the privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Examples:

The following example shows how to re-enable IGMP report suppression for bridge-domain 130:

```
Router# configure terminal
Router(config-bdomain)# bridge-domain 130
Router(config-bdomain)# ip igmp snooping report-suppression
Router(config-bdomain)# end
```

DLP-J220 Configuring a Static Multicast Router Port Using Cisco IOS Commands

To add a static connection to a multicast router port, use the **ip igmp snooping mrouter** EFP configuration command on the CPT system. To remove a static multicast router port from the bridge domain, use the **no ip igmp snooping mrouter** configuration command.

Note Static connections to multicast routers are supported only at the EFP.

Purpose	This procedure enables a static connection to a multicast router using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J217 Enabling or Disabling IGMP Snooping Using Cisco IOS Commands, on page 617
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TengigabitEthernet 4/1	Specifies the type and location of the interface to configure, where: • *type*—Specifies the type of interface. • *number*—Specifies the location of the interface. The interface can be a physical interface or a port channel. The port-channel range is 1 to 128.
Step 4	**service instance** *id* **ethernet** **Example:** Router(config-if)# service instance 10 ethernet	Configures an Ethernet service instance on an interface.
Step 5	**encapsulation dot1q** *id* **Example:** Router(config-if)# encapsulation dot1q 10	Defines the encapsulation format as IEEE 802.1Q (**dot1q**) and specifies the identifier. The identifier indicates the CVLAN with which the packet is received on the interface.

	Command or Action	Purpose
		• Enter the value of the identifier.
Step 6	**rewrite ingress tag pop 1 symmetric** **Example:** Router(config-if-srv)# **rewrite ingress tag pop 1 symmetric**	Specifies the rewrite operation.
Step 7	**bridge domain** *bridge-domain value* **Example:** Router(config-if-srv)# bridge-domain 22	Specifies the multicast router bridge domain ID. The bridge domain ID range is from 1 to 16384 • Enter the value of the bridge domain.
Step 8	**[no] ip igmp snooping mrouter** **Example:** Router(config-if-srv)# ip igmp snooping mrouter	Adds a static connection to the multicast router. The **no** form of the command removes the static multicast router port from the bridge domain.
Step 9	end **Example:** Router(config-if-srv)# end	Returns to the privileged EXEC mode.

Examples:

The following example shows how to enable a static connection to a multicast router:

```
Router(config)# interface TenGigabitEthernet4/2
Router(config-if)# service instance 20 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 20
Router(config-if-srv)# ip igmp snooping mrouter
```

The following example shows how to disable a static connection to a multicast router:

```
Router(config)# interface TenGigabitEthernet4/2
Router(config-if)# service instance 20 ethernet
Router(config-if-srv)# no ip igmp snooping mrouter
```

Note To add a static multicast router port to the EFP using CTC, see Step 6.e of NTP-J68 Configuring IGMP Snooping Using CTC, on page 629.

DLP-J230 Viewing IGMP Configuration Using Cisco IOS Commands

Purpose	This procedure explains how to view IGMP configuration using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip igmp snooping [groups [count | vlan** *bridge-domain ID* **[** *ip-address* **| count |dynamic [count] | user [count]]]] | mrouter [vlan** *bridge-domain ID***] querier | vlan** *bridge-domain ID***]** **Example:** Router# show ip igmp snooping	Displays the IGMP snooping information. • **groups—**(Optional) Displays group information. • **count—**(Optional) Displays the number of multicast groups learned by IGMP snooping. • **vlan** *bridge-domain ID***—**(Optional) Specifies a bridge domain. • *bridge-domain ID***—** Bridge domain ID. Valid values are from 1 to 16384. • *ip-address***—**(Optional) Displays information about the specified group. • **count—**(Optional) Displays the group count inside a bridge domain. • **dynamic—**(Optional) Displays dynamic entries learned through IGMP snooping. • **count—**(Optional) Displays the number of dynamic entries. • **user—**(Optional) Displays only the user-configured multicast entries. • **count—**(Optional) Displays the number of user-configured multicast entries.

	Command or Action	Purpose
		• **mrouter—**(Optional) Displays information about dynamically learned and manually configured multicast router ports. • **querier—**(Optional) Displays IGMP querier information.
Step 3	**show ip igmp snooping querier [vlan** *bridge-domain ID* **] [detail]** **Example:** Router# show ip igmp snooping querier	Displays information about the IP address and the receiving port for the recently received IGMP query messages. • **vlan** *bridge-domain ID* **—**(Optional) Specifies a bridge domain. • *bridge-domain ID***—** Bridge domain ID. Valid values are from 1 to 16384. • **detail—**Specifies the configuration and operational state of the IGMP snooping querier in the bridge domain.

Examples

The following example displays the output of the **show ip igmp snooping [vlan** *bridge-domain ID* **]** command.

```
Router# show ip igmp sn vlan 2

Global IGMP Snooping configuration:
----------------------------------------
IGMP snooping Oper State     : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000
Check TTL=1                  : No
Check Router-Alert-Option    : No

Vlan 2
----------------------
IGMP snooping Admin State          : Enabled
IGMP snooping Oper State           : Enabled
IGMPv2 immediate leave             : Disabled
Report suppression                 : Enabled
Robustness variable                : 2
Last member query count            : 2
Last member query interval         : 1000
Check TTL=1                        : Yes
Check Router-Alert-Option          : Yes
Query Interval                     : 0
Max Response Time                  : 10000
```

The following example displays the output of the **show ip igmp snooping groups** command.

```
Router# show ip igmp snooping groups

Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode

Vlan      Group/source             Type        Version     Port List
------------------------------------------------------------------------------
2         224.1.1.1                I           v2          Te7/4 Te5/2
Gi41/1 Gi41/44 Gi51/1 Gi51/44 Te4/2
```

The following example displays the output of the **show ip igmp snooping groups vlan** command.

```
Router# show ip igmp snooping groups vlan 2

Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode

Vlan      Group/source             Type        Version     Port List
------------------------------------------------------------------------------
2         224.1.1.1                I           v2          Te7/4 Te5/2
Gi41/1 Gi41/44 Gi51/1 Gi51/44 Te4/2
```

The following example displays the output of the **show ip igmp snooping groups vlan** *bridge-domain ID* **[***ip_address***]** command.

```
Router# show ip igmp snooping groups vlan 2 224.1.1.1

Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode

Vlan      Group/source             Type        Version     Port List
------------------------------------------------------------------------------
2         224.1.1.1                I           v2          Te7/4 Te5/2
Gi41/1 Gi41/44 Gi51/1 Gi51/44 Te4/2
```

The following example displays the output of the **show ip igmp snooping mrouter** command.

```
Router# show ip igmp snooping mrouter

Vlan    ports
----    -----
   2    Te4/4(dynamic)
```

The following example displays the output of the **show ip igmp snooping mrouter vlan 2** command.

```
Router# show ip igmp snooping mrouter

Vlan    ports
----    -----
   2    Te4/4(dynamic)
```

The following example shows the output of the **show ip igmp snooping querier** command.

```
Router# show ip igmp snooping querier

Vlan      IP Address               IGMP Version   Port
------------------------------------------------------------
2         10.10.10.1               v2             Te4/4
```

The following example shows the output of the **show ip igmp snooping querier [vlan** *bridge-domain ID* **]** command.

```
Router# show ip igmp snooping querier vlan 2

IP address                : 10.10.10.1
IGMP version              : v2
Port                      : Te4/4
Max response time         : 10s
```

NTP-J68 Configuring IGMP Snooping Using CTC

Purpose	This procedure explains how to configure IGMP Snooping, Immediate Leave, Report Suppression, and IGMP Static Router Port using CTC.
Tools/Equipment	None
Prerequisite Procedures	Create an Ethernet Virtual Private LAN EVC circuit with the following conditions: • Type of VLAN Tagging: ◦ Double Tagged ◦ Single Tagged ◦ Untagged • Rewrite Operation: ◦ POP 1 for Single Tagged ◦ POP 2 for Double Tagged ◦ N/A for Untagged To create an EVC circuit, see DLP-J2 Create an EVC Circuit Using CTC, on page 143.
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	None

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to configure IGMP snooping.

Step 2 In node view, click the **Layer2+** tab.

Step 3 Click **Carrier Ethernet.**

Step 4 From the list of Ethernet Virtual Circuits (EVCs), select an Ethernet Virtual Private LAN EVC circuit to configure IGMP snooping.

Step 5 Click **Edit**. The Edit Circuit dialog box appears.

Step 6 In the IGMP Snooping tab, specify the settings for the bridge domain.

a) Select a bridge domain from the list.

b) Check the **IGMP Snooping** check box to enable IGMP snooping on this bridge domain.

c) Check the **Immediate Leave** check box. When you enable IGMP immediate leave, IGMP snooping immediately removes a port when it detects a leave message on that port.

d) Check the **Report Suppression** check box. When you enable report suppression, the bridge domain forwards only one IGMP report for each multicast query.

e) Check the **IGMP Static Router Port** check box to add a static router to the EFP.

Note To disable IGMP Snooping, Immediate Leave, Report Suppression, or IGMP Static Router Port, uncheck the checkbox against each one of them.

f) Click **Apply**.

Step 7 To view the IGMP configuration, refer to the procedure explained in DLP-J56 Open the Cisco IOS Configuration Mode and View the Feature Configuration Details Using CTC, on page 10.

IGMP Proxy Reporting

IGMP supports proxy reporting for IGMPv1 and IGMPv2 messages to handle group-specific queries. These queries are not sent downstream, but the CPT system does respond to them directly. When the CPT system receives a group-specific query, the CPT system terminates the query and sends an IGMP proxy report if there is a receiver for the group. There is no proxy reporting for IGMPv3 messages. For IGMPv3, a group-specific query or a group source-specific query is flooded to all VLAN member ports. The database for the IGMPv3 membership report is built based on the reports received.

Host reports responding to a specific query can be suppressed by the report suppression feature. Report suppression is supported for IGMPv1, IGMPv2 and IGMPv3 messages. With report suppression enabled (by default), when the CPT system receives a general query, the CPT system starts a suppression cycle for reports from all hosts to each group or channel. Only the first report to the discovered multicast routers are forwarded; the rest of the reports are suppressed. For IGMPv1 and IGMPv2, the time of suppression is the report response time indicated in the general query message. For IGMPv3, suppression occurs for the entire general query interval.

Note

- Source-based filtering for IGMP version 3 reports is not supported in hardware. The states are maintained only in software and used for explicit host tracking and statistics collection. The source-only entries are deleted every 5 minutes and relearned to ensure that they are still valid.
- Turning off explicit host tracking disables fast-leave processing and proxy reporting.

L2 Address Aliasing Issue

The IGMP snooping forwarding table is based on L2 address. Since multiple IP addresses can map to the same L2 address, an L2 address aliasing can occur. For example, IP addresses 225.1.1.1 and 226.1.1.1 map to the same MAC address 01005E010101 which results in L2 address aliasing.

IGMP Snooping Interaction with LAG

A link aggregation (LAG) interface can be added to a bridge domain, which has IGMP snooping enabled.

The following example shows how to configure the source port, which is part of the LAG interface that is a member of the bridge domain that has IGMP snooping enabled.

```
Configuration on the bridge-domain
Router(config)# bridge-domain 30
Router(config-bdomain)# ip igmp snooping

Configuration on port 1
Router(config)# interface  port-channel 10
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 30
Router(config)# interface ten 6/1
Router(config-if)# channel-group 10
Router(config)# interface ten 6/2
Router(config-if)# channel-group 10

Configuration port 2
Router(config)# interface gi36/2
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 20 second-dot1q 30
Router(config-if-srv)# rewrite ingress pop 2 symmetric
Router(config-if-srv)# bridge-domain 30

Configuration on port 3
Router(config)# interface gi36/3
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation  dot1q 40
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 30
```

The following example shows how to configure the receiver port, which is part of the LAG interface that is a member of the bridge domain that has IGMP snooping enabled.

```
Configuration on the bridge-domain
Router(config)# bridge-domain 30
Router(config-bdomain)# ip igmp snooping
```

```
Configuration on port 1
Router(config)# interface ten 6/1
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10 second-dot1q 30
Router(config-if-srv)# rewrite ingress pop 2 symmetric
Router(config-if-srv)# bridge-domain 30

Configuration port 2
Router(config)# interface port-channel 10
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 30

Router(config)# interface gi36/1
Router(config-if)# channel-group 10

Router(config)# interface gi36/2
Router(config-if)# channel-group 10

Configuration on port 3
Router(config)# interface gi36/5
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation  dot1q 40
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 30
```

High Availability

The multicast group tables are synchronized between the active and standby fabric cards. If an active fabric reloads, then the standby fabric card becomes active. Since, the multicast group tables are already synchronized, there is no traffic loss, unless the source or the receiver is not present on the card that reloaded.

Note The IGMP snooping feature does not interact with REP.

IGMP Statistics and Counters

An entry in a counter contains multicasting statistical information for the IGMP snooping capable CPT system. The equivalent IOS command to retrieve statistical information is **show ip igmp snooping counters**.

This information can be stored in the following counters:

- Tx General Queries—Number of general queries transmitted through an interface.
- Tx Group Specific Queries—Total group specific queries transmitted through an interface.
- Tx Reports—Total membership reports transmitted through an interface.
- Tx Leaves—Total leave messages transmitted through an interface.
- Rx General Queries—Total general queries received at an interface.
- Rx Group Specific Queries—Total group specific queries received at an interface.
- Rx Reports—Total membership reports received at an interface.
- Rx Leaves—Total leave messages received at an interface.

- Rx Valid Packets—Total valid IGMP packets received at an interface.
- Rx Invalid Packets—Total number of invalid IGMP packets that are received at an interface.

The following example shows the statistical information using the **show ip igmp snooping counters** command.

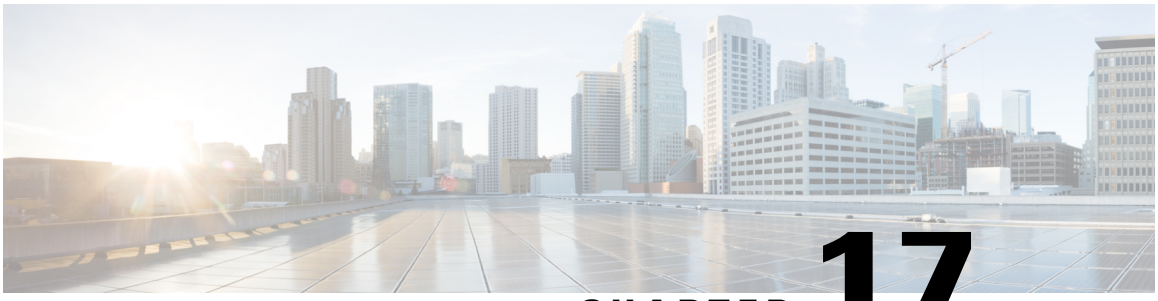
```
Router> show ip igmp snooping counters
```

```
packet queue maximum size:               20000
packet queue current size:               0
packet queue peak size:                  0
packet queue drop count:                 0
----
Vlan   1
----

Counters of group "IGMP snooping  counters                              "
overall there are 15   counters
 Type                                              | Value      | Ovr |
Und
--------------------------------------------------+------------+-----+----
RX processed Query Count                          | 0          |     |

RX processed Group Specific Query                 | 0          |     |

RX processed Join                                 | 787120     |     |

RX processed Leave                                | 0          |     |

RX processed Total Valid Packets                  | 782        |     |

RX processed Other Packets                        | 0          |     |

RX Packets dropped for sanity errors              | 0          |     |

RX Packets dropped for checksum errors            | 0          |     |

RX Packets dropped for header length errors       | 0          |     |

RX Packets dropped for other errors               | 0          |     |

RX processed Topology change notification         | 0          |     |

TX processed Query Count                          | 0          |     |

TX processed Group Specific Query                 | 0          |     |

TX processed Join                                 | 0          |     |

TX processed Leave                                | 0          |     |


Counters of group "IGMP snooping  V3 counters                           "
overall there are 18   counters
RX processed V3 AllOW NEW                         | 0          |     |

RX processed V3 BLOCK OLD                         | 0          |     |

 Type                                             | Value      | Ovr |
```

```
Und
-------------------------------------------------+-----------+-----+----
RX processed V3 MODE IS INCLUDE                  | 0         |     |

RX processed V3 MODE IS EXCLUDE                  | 0         |     |

RX processed V3 CHANGE TO INCLUDE                | 0         |     |

RX processed V3 CHANGE TO EXCLUDE                | 0         |     |

RX processed V3 Query                            | 782       |     |

RX processed V3 Group Specific Query             | 0         |     |

RX processed V3 GSS Query                        | 0         |     |

TX processed V3 ALLOW NEW                        | 0         |     |

TX processed V3 BLOCK OLD                        | 0         |     |

TX processed V3 MODE IS INCLUDE                  | 0         |     |

TX processed V3 MODE IS EXCLUDE                  | 0         |     |

TX processed V3 CHANGE TO INCLUDE                | 0         |     |

TX processed V3 CHANGE TO EXCLUDE                | 0         |     |

TX processed V3 Query                            | 0         |     |

TX processed V3 Group Specific Query             | 0         |     |

TX processed V3 GSS Query                        | 0         |     |
```

Alarms

The MCAST-MAC-TABLE-FULL condition is raised from IGMP snooping at the card level. The CPT system supports a maximum of 2000 multicast groups. The MCAST-MAC-TABLE-FULL condition is raised when the multicast table is full and a new join request is received. This table is cleared when at least one entry gets cleared from the multicast table after the alarm is raised.



CHAPTER 17

Configuring Ethernet OAM, Connectivity Fault Management, and Y.1731

This chapter describes Ethernet OAM, Connectivity Fault Management (CFM), and Y.1731 features. This chapter also describes procedures to configure Ethernet OAM, CFM, and Y.1731.

This chapter includes the following topics:

Ethernet Link OAM Overview

Ethernet Link Operations, Administration, and Maintenance (OAM) is a protocol for installing, monitoring, and troubleshooting Ethernet metropolitan-area networks (MANs) and Ethernet WANs. It relies on an optional sublayer in the data link layer of the Open Systems Interconnection (OSI) model, as specified in IEEE 802.3ah-2004 Clause 57.

Ethernet Link OAM enables service providers to monitor and troubleshoot a single physical (or emulated) Ethernet link. It supports link level verification, monitoring, and troubleshooting between two Ethernet devices. It is particularly valuable in the 'first mile' connection to the customer demarcation.

Understanding Ethernet Link OAM

Ethernet link OAM can be implemented on any full-duplex point-to-point or emulated point-to-point Ethernet link. A system-wide implementation is not required; OAM can be deployed for part of a system; that is, on specific interfaces.

Normal link operation does not require Ethernet link OAM. OAM frames, called OAM protocol data units (PDUs), use the slow protocol destination MAC address 0180.c200.0002. They are intercepted by the MAC sublayer and cannot propagate beyond a single hop within an Ethernet network.

Ethernet link OAM is a relatively slow protocol with modest bandwidth requirements. The frame transmission rate is limited to a maximum of 10 frames per second; therefore, the impact of OAM on normal operations is negligible. However, when link monitoring is enabled, the CPU must poll error counters frequently. In this case, the required CPU cycles will be proportional to the number of interfaces that have to be polled.

Two major components, the OAM client and the OAM sublayer, make up Ethernet Link OAM. The following two sections describe these components.

OAM Client

The OAM client is responsible for establishing and managing Ethernet link OAM on a link. It also enables and configures the OAM sublayer. During the OAM discovery phase, the OAM client monitors OAM PDUs received from the remote peer and enables OAM functionality on the link based on the local and remote state as well as configuration settings. After the discovery phase (at steady state), the OAM client is also responsible for managing the rules of response to OAM PDUs and the OAM remote loopback mode.

OAM Sublayer

The OAM sublayer presents two standard IEEE 802.3 MAC service interfaces: one facing the superior sublayers, which include the MAC client (or link aggregation), and the other interface facing the subordinate MAC control sublayer. The OAM sublayer provides a dedicated interface for passing OAM control information and OAM PDUs to and from a client. The OAM sublayer is made up of three components: control block, multiplexer, and packet parser (p-parser).

The control block provides the interface between the OAM client and other blocks internal to the OAM sublayer. The control block runs the discovery process, which detects the existence and capabilities of remote OAM peers. It also includes the transmit process that governs the transmission of OAM PDUs to the multiplexer and a set of rules that govern the receipt of OAM PDUs from the p-parser.

The multiplexer manages frames generated (or relayed) from the MAC client, control block, and p-parser. The multiplexer passes through frames generated by the MAC client untouched. It passes OAM PDUs generated by the control block to the subordinate sublayer; such as the MAC sublayer. Similarly, the multiplexer passes loopback frames from the p-parser to the same subordinate sublayer when the interface is in OAM remote loopback mode.

The p-parser classifies frames as OAM PDUs, MAC client frames, or loopback frames and then dispatches each class to the appropriate entity. OAM PDUs are sent to the control block; MAC client frames are passed to the superior sublayer; and loopback frames are dispatched to the multiplexer.

Benefits of Ethernet Link OAM

Ethernet Link OAM provides the following benefits:

- Competitive advantage for service providers.
- Standardized mechanism to monitor the health of a link and perform diagnostics.

NTP-J114 Configure EFM Using Cisco IOS Commands

Purpose	This procedure configures EFM using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J320 Enable or Disable Ethernet Link OAM on an Interface Using Cisco IOS Commands, on page 638
- DLP-J321 Enable or Disable Link Monitoring Support on an Interface Using Cisco IOS Commands, on page 642
- DLP-J322 Enable or Disable Link Monitoring on an Interface Using Cisco IOS Commands, on page 644

- DLP-J323 Configure Link Monitoring Parameters on an Interface Using Cisco IOS Commands, on page 646
- DLP-J325 Configure the Port for Remote Link Failure Indication Using Cisco IOS Commands, on page 651
- DLP-J367 Set Up Remote Loopback Timeout Period on an Interface Using Cisco IOS Commands, on page 654
- DLP-J324 Enable Remote Loopback on an Interface Using Cisco IOS Commands, on page 655

Stop. You have completed this procedure.

NTP-J115 Configure EFM Using CTC

Purpose	This procedure configures EFM using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J314 Enable or Disable Ethernet Link OAM on a Port Using CTC, on page 639
- DLP-J315 Enable or Disable Link Monitoring Support on an Interface Using CTC, on page 643
- DLP-J316 Enable or Disable Link Monitoring on an Interface Using CTC, on page 645
- DLP-J317 Configure Link Monitoring Parameters on an Interface Using CTC, on page 648
- DLP-J319 Configure the Port for Remote Link Failure Indication Using CTC, on page 652
- DLP-J318 Enable Remote Loopback on an Interface Using CTC, on page 656

Stop. You have completed this procedure.

DLP-J320 Enable or Disable Ethernet Link OAM on an Interface Using Cisco IOS Commands

Purpose	This procedure enables or disables Ethernet Link OAM on an interface using Cisco IOS commands.

Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**ethernet oam** [**max-rate** *oampdus* | **min-rate** *num-seconds*| **mode** {**active** | **passive**} | **timeout** *seconds*] **Example:** Router(config-if)# ethernet oam	Enables Ethernet Link OAM on the interface. The **no** form of this command disables Ethernet Link OAM on the interface.
Step 5	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
Step 6	Return to your originating procedure (NTP).	

DLP-J314 Enable or Disable Ethernet Link OAM on a Port Using CTC

Purpose	This procedure enables or disables Ethernet link OAM on a port using CTC.

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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to enable or disable Ethernet link OAM on a port.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**.

Step 3 The Packet Transport System View dialog box appears. Click the **Provisioning** > **EFM** > **Configuration** tabs.

Step 4 In the Configuration area, expand the appropriate slot and select the port where you want to enable the Ethernet link OAM.

Step 5 From the EFM State drop-down list, choose **Enabled** to enable Ethernet link OAM on the selected port. Choose **Disabled** to disable Ethernet link OAM on the selected port.

Note Ethernet link OAM is disabled by default on a port.

Step 6 In the Configuration area, expand the appropriate slot and modify any of the parameters as described in the following table.

Table 31: Ethernet Link OAM Parameters

Parameter	Description	Options
Port	(Display only) Displays the port number (n-n) and rate.	—
Mode	(Optional) Sets the OAM client mode on the interface.	• Active—Sets the OAM client mode to active on the interface which was previously in passive mode. Active is the default mode. • Passive—Sets the OAM client mode to passive on the interface. In passive mode, a device cannot initiate discovery, inquire about variables, or set loopback mode.

Parameter	Description	Options
Transmission Rate Minimum	(Optional) Sets the minimum rate, in seconds, at which OAM PDUs are transmitted. That is, the number of seconds during which at least one OAM PDU must be transmitted.	The valid values range from 1 to 10 seconds.
Transmission Rate Maximum	(Optional) Sets the maximum rate, in seconds, at which OAM PDUs are transmitted. That is, the number of seconds during which OAM PDUs must be transmitted.	The valid values range from 1 to 10 seconds.The default is 10 seconds.
Session Timer	(Optional) Specifies the amount of time, in seconds, after which a device declares its OAM peer to be nonoperational and resets its state machine. That is, the number of seconds a device waits for its OAM peer to respond.	The valid values range from 2 to 30 seconds.The default is 5 seconds.

Step 7 Return to your originating procedure (NTP).

Ethernet Link OAM Features

The Cisco CPT supports the following Ethernet link OAM features:

- Discovery, on page 641
- Link Monitoring, on page 642
- Remote Failure Indication, on page 651
- Remote Loopback, on page 653

Discovery

Discovery is the first phase of Ethernet link OAM where it identifies the devices in the network and their OAM capabilities. Discovery uses information OAM PDUs. During the discovery phase, the following information is advertised within periodic information OAM PDUs:

- OAM mode—Conveyed to the remote OAM entity. The mode can be either active or passive and can be used to determine device functionality.

- OAM configuration (capabilities)—Advertises the capabilities of the local OAM entity. With this information a peer can determine what functions are supported and accessible; for example, loopback capability.
- OAM PDU configuration—Includes the maximum OAM PDU size for receipt and delivery. This information along with the rate limiting of 10 frames per second can be used to limit the bandwidth allocated to the OAM traffic.
- Platform identity—Specifies a combination of an organization unique identifier (OUI) and 32-bits of vendor-specific information. OUI allocation, controlled by the IEEE, is typically the first three bytes of a MAC address.

Discovery includes an optional phase in which the local station can accept or reject the configuration of the peer OAM entity. For example, a node may require its partner support loopback capability to be accepted in the management network. These policy decisions may be implemented as vendor-specific extensions.

Link Monitoring

Link monitoring in Ethernet Link OAM detects and indicates link faults under a variety of conditions. Link monitoring uses the event notification OAM PDU and sends events to the remote OAM entity when there are problems detected on the link. The error events include the following:

- Error Frame (error frames per second)—The number of frame errors detected during a specified period that exceed a threshold.
- Error Frame Period (error frames per *n* frames)—The number of frame errors within the last *n* frames that exceed a threshold.
- Error Frame Seconds Summary (error seconds per *m* seconds)—The number of error seconds (1-second intervals with at least one frame error) within the last *m* seconds that exceed a threshold.

Because IEEE 802.3ah OAM does not provide a guaranteed delivery of any OAM PDU, the event notification OAM PDU may be sent multiple times to reduce the probability of a lost notification. A sequence number is used to recognize duplicate events.

DLP-J321 Enable or Disable Link Monitoring Support on an Interface Using Cisco IOS Commands

Purpose	This procedure enables or disables link monitoring support on an interface using Cisco IOS Commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**ethernet oam link-monitor supported** **Example:** Router(config-if)# ethernet oam link-monitor supported	Enables link monitoring support on the interface. The **no** form of this command disables link monitoring support on the interface.
Step 5	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.

DLP-J315 Enable or Disable Link Monitoring Support on an Interface Using CTC

Purpose	This procedure enables or disables support for link monitoring on an interface using CTC. This procedure helps establish an OAM session for performing OAM functions, such as remote loopback. For example, if the device is connected to a third-party device that does not support link monitoring, then link monitoring support must be disabled on the device to establish an OAM session with the third-party device.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to enable or disable link monitoring support on an interface.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**.

Step 3 The Packet Transport System View dialog box appears. Click the **Provisioning** > **EFM** > **Link Monitoring** tabs

Step 4 In the Link Monitoring area, expand the appropriate slot and select the port where you want to enable link monitoring.

Step 5 From the Support drop-down list, choose **Support** to enable link monitoring support or choose **No support** to disable link monitoring support on the interface.

Step 6 Return to your originating procedure (NTP).

DLP-J322 Enable or Disable Link Monitoring on an Interface Using Cisco IOS Commands

Purpose	This procedure enables or disables link monitoring on an interface using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	Router# configure terminal	
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**ethernet oam** [**max-rate** *oampdus* | **min-rate** *num-seconds*| **mode** {**active** | **passive**} | **timeout** *seconds*] **Example:** Router(config-if)# ethernet oam	Enables Ethernet OAM on the interface.
Step 5	**ethernet oam link-monitor on** **Example:** Router(config-if)# ethernet oam link-monitor on	Enables link monitoring on the interface. The **no** form of this command disables link monitoring on the interface.
Step 6	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.

DLP-J316 Enable or Disable Link Monitoring on an Interface Using CTC

Purpose	This procedure enables or disables link monitoring on an interface using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Link monitoring is enabled by default when Ethernet Link OAM is enabled on a interface.

When link monitoring is enabled, the interface sends event OAM PDUs when errors occur and interprets event OAM PDUs from the remote peer. Link monitoring can be effective only if both the local client and remote peer agree to support it.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to enable or disable link monitoring on an interface.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**.

Step 3 The Packet Transport System View dialog box appears. Click the **Provisioning** > **EFM** > **Link Monitoring** tabs

Step 4 In the Link Monitoring area, expand the appropriate slot and select the port where you want to enable link monitoring.

Step 5 From the Enable drop-down list, choose **Enabled** to enable link monitoring or choose **Disabled** to disable link monitoring on the interface.

Step 6 Return to your originating procedure (NTP).

DLP-J323 Configure Link Monitoring Parameters on an Interface Using Cisco IOS Commands

Purpose	This procedure configures link monitoring parameters on an interface using Cisco IOS Commands. **Note** Perform this optional task to specify link monitoring parameters. Steps 4 through 11 can be performed in any sequence.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**ethernet oam** [**max-rate** *oampdus* | **min-rate** *num-seconds*| **mode** {**active** | **passive**} | **timeout** *seconds*] **Example:** Router(config-if)# ethernet oam	Enables Ethernet link OAM on the interface.
Step 5	**ethernet oam link-monitor high-threshold action error-disable-interface** **Example:** Router(config-if)# ethernet oam link-monitor high-threshold action error-disable-interface	Sets the interface to the blocking or disabled state when a high threshold for an error is exceeded.
Step 6	**ethernet oam link-monitor frame** {**threshold** {**high** { **none** | *high-frames*} | **low** *low-frames*} | **window** *milliseconds*} **Example:** Router(config-if)# ethernet oam link-monitor frame window 399	Configures, in milliseconds, the number for error frames that trigger an action when reached.
Step 7	**ethernet oam link-monitor frame-period** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *frames*} **Example:** Router(config-if)# ethernet oam link-monitor frame-period threshold high 599	Configures the number of frames to be polled. The frame period is a user-defined parameter.
Step 8	**ethernet oam link-monitor frame-seconds** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *milliseconds*} **Example:** Router(config-if)# ethernet oam link-monitor frame-seconds window 699	Configures a period of time, in milliseconds, during which error frames are counted.
Step 9	**ethernet oam link-monitor receive-crc** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *milliseconds*} **Example:** Router(config-if)# ethernet oam link-monitor receive-crc window 99	Configures an Ethernet OAM interface to monitor ingress frames with cyclic redundancy check (CRC) errors for a period of time.

	Command or Action	Purpose
Step 10	**ethernet oam link-monitor transmit-crc** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *milliseconds*} **Example:** Router(config-if)# ethernet oam link-monitor transmit-crc threshold low 199	Configures an Ethernet OAM interface to monitor egress frames with CRC errors for a period of time (in milliseconds).
Step 11	**ethernet oam link-monitor symbol-period** {**threshold** {**high** {**none** | *high-symbols*} | **low** *low-symbols*} | **window** *symbols*} **Example:** Router(config-if)# ethernet oam link-monitor symbol-period threshold high 299	Configures a threshold or window for error symbols, in number of symbols.
Step 12	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.

DLP-J317 Configure Link Monitoring Parameters on an Interface Using CTC

Purpose	This procedure configures the link monitoring parameters on an interface using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to configure link monitoring parameters on an interface.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**.

Step 3 The Packet Transport System View dialog box appears. Click the **Provisioning** > **EFM** > **Link Monitoring** tabs

Step 4 In the Link Monitoring area, expand the appropriate slot and modify any of the parameters as described in the following table.

Table 32: Link Monitoring Parameters

Parameter	Description	Options
Port	(Display only) Displays the port number (n-n) and rate.	—
FT Min	Frame Threshold Minimum–Sets a low error frame threshold in number of frames.	The valid values range from 0 to 65535 seconds or frames per second. The default is 1 second.
FT Max	Frame Threshold Maximum–Sets a high error frame threshold in number of frames.	Integer in the range of 1 to 65535 that is the high threshold in number of frames.
Frame Window	Sets a window and period of time during which error frames are counted.	Sets a window and period of time during which error frames are counted. Integer in the range of 10 to 600 that represents a number of milliseconds in a multiple of 100. The default is 100.
FPT Min	Frame Period Threshold Minimum–Sets a low threshold for the error frame period in number of frames.	Integer in the range of 0 to 65535 that is the low threshold in number of frames. The default is 1.
FPT Max	Frame Period Threshold Maximum–Sets a high threshold for the error frame period in number of frames.	Integer in the range of 1 to 65535 that is the high threshold in number of frames. There is no default. The high threshold must be configured.
FP Window	Frame Period Window–Sets a polling window and window size.	Integer in the range of 1 to 65535 that is the window size in number of frames. Each value is a multiple of 10000. The default is 1000.
FST Min	Frame Seconds Threshold Minimum–Sets a low error frame-seconds threshold in number of seconds.	Integer in the range of 1 to 900 that sets the low threshold in number of frames. The default is 1.

Parameter	Description	Options
FST Max	Frame Seconds Threshold Maximum–Sets a high error frame-seconds threshold in number of seconds.	Integer in the range of 1 to 900 that is the high threshold in number of frames. There is no default. The high threshold must be configured.
FS Window	Frame Seconds Window–Sets a polling window during which error frames are counted.	Integer in the range of 100 to 9000 that represents a number of milliseconds in a multiple of 100. The default is 1000.
SPT Min	Symbol Period Threshold Minimum–Sets a low threshold for the period in number of error symbols.	Integer in the range of 0 to 65535 that is the low threshold in number of symbols.
SPT Max	Symbol Period Threshold Maximum–Sets a high threshold for the period in number of error symbols.	Integer in the range of 1 to 65535 that is the high threshold in number of symbols. There is no default. The high threshold must be configured.
SP Window	Symbol Period Window-Sets a window and window size.	Integer in the range of 1 to 65535 that is the window size in number of symbols. Each value represents one million.
RCRCT Min	Receive CRC Threshold Minimum–Sets a low threshold.	Integer in the range of 0 to 65535 that sets the low threshold in number of frames. The default is 10.
RCRCT Max	Receive CRC Threshold Maximum–Sets a high threshold in number of frames.	Integer in the range of 1 to 65535 that is the high threshold in number of frames.
RCRC Window	Receive CRC Window–Sets a window and period of time during which frames with CRC errors are counted.	Integer in the range of 10 to 1800 that represents a number of milliseconds in a multiple of 100. The default is 1000.
TCRCT Min	Transmit CRC Threshold Minimum–Sets a low threshold.	Integer in the range of 0 to 65535 that sets the low threshold in number of frames. The default is 10.
TCRCT Max	Transmit CRC Threshold Maximum-Sets a high threshold in number of frames.	Integer in the range of 1 to 65535 that is the high threshold in number of frames.
TCRC Window	Transmit CRC Window-Sets a window and period of time during which frames with transmit CRC errors are counted.	Integer in the range of 10 to 1800 that represents a number of milliseconds in a multiple of 100. The default is 100.

Parameter	Description	Options
HT Action	High Threshold Action–Provides an automatic failover of traffic from one port in an EtherChannel to another port in the same EtherChannel when one of the ports in the channel exceeds the high threshold for an error within the specified interval. The port failover occurs only if at least one operational port is in the EtherChannel. If the failed port is the last port in the EtherChannel, the port is moved into error-disable state and continues to pass traffic regardless of the types of errors received.	• NONE • Error Disable

Step 5 Return to your originating procedure (NTP).

Remote Failure Indication

Faults in Ethernet connectivity that are caused by slowly deteriorating quality are difficult to detect. Ethernet Link OAM provides a mechanism for an OAM entity to convey these failure conditions to its peer via specific flags in the OAM PDU. The following failure conditions can be communicated:

- Link Fault–Loss of signal is detected by the receiver. A link fault is sent every second in the information OAM PDU. Link fault applies only when the physical sublayer is capable of independently transmitting and receiving signals.
- Dying Gasp–An unrecoverable condition has occurred; for example, a power failure. This type of condition is vendor specific. A notification about the condition may be sent immediately and continuously.
- Critical Event–An unspecified critical event has occurred. This type of event is vendor specific. A critical event may be sent immediately and continuously.

DLP-J325 Configure the Port for Remote Link Failure Indication Using Cisco IOS Commands

Purpose	This procedure configures the port for remote link failure indication using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**ethernet oam remote-failure** {**critical-event** | **dying-gasp** | **link-fault**} **action** {**error-block-interface** | **error-disable-interface**} **Example:** Router(config-if)# ethernet oam remote-failure critical-event action **error-disable-interface**	Sets the interface to disabled state when a critical event occurs.
Step 5	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.

DLP-J319 Configure the Port for Remote Link Failure Indication Using CTC

Purpose	This procedure configures the port for remote link failure indication using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to configure the port for remote link failure indication.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**.

Step 3 The Packet Transport System View dialog box appears. Click the **Provisioning** > **EFM** > **Configuration** tabs

Step 4 In the Configuration area, expand the appropriate slot and modify any of the parameters as described in the following table.

Table 33: Remote Link Failure Indication Parameters

Parameter	Description	Options
Link Fault	Detects the loss of signal by the receiver.	• None • Error Block • Error Disable
Critical Event	Sends the critical event notification when an unspecified critical event has occurred.	• None • Error Disable
Dying Gasp	Sends the notification when an unrecoverable condition has occurred; for example, a power failure.	• None • Error Block • Error Disable

Step 5 Return to your originating procedure (NTP).

Remote Loopback

An OAM entity can put its remote peer into loopback mode using the loopback control OAM PDU. Loopback mode helps an administrator ensure the quality of links during installation or when troubleshooting. In loopback mode, every frame received is transmitted back on the same port except for OAM PDUs and pause frames. The periodic exchange of OAM PDUs must continue during the loopback state to maintain the OAM session.

The **loopback** command is acknowledged by responding with an information OAM PDU with the loopback state indicated in the State field. This acknowledgement allows an administrator, for example, to estimate if a network segment can satisfy a service-level agreement. Acknowledgement makes it possible to test delay, jitter, and throughput.

When an interface is set to the remote loopback mode the interface no longer participates in any other Layer 2 or Layer 3 protocols; for example Spanning Tree Protocol (STP) or Open Shortest Path First (OSPF). This is because when two connected ports are in a loopback session, no frames other than the OAM PDUs are sent to the CPU for software processing. The non-OAM PDU frames are either looped back at the MAC level or discarded at the MAC level.

From a user perspective, an interface in a loopback mode is in a link-up state.

DLP-J367 Set Up Remote Loopback Timeout Period on an Interface Using Cisco IOS Commands

Purpose	This procedure sets up remote loopback timeout period on an interface using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**ethernet oam remote-loopback** {**supported** | **timeout** *seconds*} **Example:** Router(config-if)# ethernet oam remote-loopback supported	Sets a remote loopback timeout period, in seconds, on an interface.

	Command or Action	Purpose
Step 5	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.

DLP-J324 Enable Remote Loopback on an Interface Using Cisco IOS Commands

Purpose	This procedure enables remote loopback on an interface using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-J367 Set Up Remote Loopback Timeout Period on an Interface Using Cisco IOS Commands, on page 654
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ethernet oam remote-loopback** {**start** | **stop**} {**interface** *type number*} **Example:** Router# ethernet oam remote-loopback start interface TenGigabitEthernet4/1	Enables remote loopback on an interface.
Step 4	**exit** **Example:**	Exits interface configuration mode and returns to EXEC mode.

	Command or Action	Purpose
	Router(config-if)# exit	

DLP-J318 Enable Remote Loopback on an Interface Using CTC

Purpose	This procedure enables remote loopback on an interface using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to enable remote loopback on an interface.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**.

Step 3 The Packet Transport System View dialog box appears. Click the **Provisioning** > **EFM** > **Remote Loopback** tabs

Step 4 In the Remote Loopback area, expand the appropriate slot and modify any of the parameters as described in the following table.

Table 34: Remote Loopback Parameters

Parameter	Description	Options
Port	(Display only) Displays the port number (n-n) and rate.	—
Remote Loopback Type	Sets the remote loopback type.	• None • Remote Loopback

Parameter	Description	Options
Execution	Turns on or off the remote loopback operation. In CTC, the reason for the failure of remote loopback is not notified. It is not notified whether Start/Stop remote loopback is functional at the remote end. This occurs when the Ethernet Link OAM or remote loopback support (at remote end) is not enabled. Whereas in Cisco IOS, the reason for the failure of remote loopback is notified appropriately.	• Start—Starts the remote loopback operation. • Stop—Stops the remote loopback operation.
Timeout	Sets a master loopback timeout setting.	The valid timeout period ranges from 1 to 10 seconds.

Understanding Ethernet OAM Messages

Ethernet OAM messages or OAM PDUs are standard length, untagged Ethernet frames within the normal frame length bounds of 64 to 1518 bytes. The maximum OAM PDU frame size exchanged between two peers is negotiated during the discovery phase.

OAM PDUs always have the destination address of slow protocols (0180.c200.0002) and an Ethertype of 8809. OAM PDUs do not go beyond a single hop and have a hard-set maximum transmission rate of 10 OAM PDUs per second. Some OAM PDU types may be transmitted multiple times to increase the likelihood that they will be successfully received on a deteriorating link.

Four types of OAM messages are supported:

- Information OAM PDU—A variable-length OAM PDU that is used for discovery. This OAM PDU includes local, remote, and organization-specific information.
- Event notification OAM PDU—A variable-length OAM PDU that is used for link monitoring. This type of OAM PDU may be transmitted multiple times to increase the chance of a successful receipt; for example, in the case of high-bit errors. Event notification OAM PDUs also may include a time stamp when generated.
- Loopback control OAM PDU—An OAM PDU fixed at 64 bytes in length that is used to enable or disable the **remote loopback** command.
- Vendor-specific OAM PDU—A variable-length OAM PDU that allows the addition of vendor-specific extensions to OAM.

Understanding Connectivity Fault Management

Ethernet Connectivity Fault Management (CFM) is an end-to-end per-service Ethernet layer operations, administration, and maintenance (OAM) protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs.

CPT supports the IEEE 802.1ag standard implementation of CFM. It supports CFM over the following:

- Point–to–multipoint bridge domain associated with Ethernet Flow Points (EFP) with P2MP-EVC.
- Xconnect
- Port Maintenance End Point (MEP)

All the CFM configurations specific to point–to–multipoint EFPs also apply to Xconnect.

Understanding IEEE CFM

IEEE CFM is an end-to-end per-service Ethernet layer OAM protocol that supports provider edge-to-provider edge (PE-to-PE) and customer edge-to-customer edge (CE-to-CE) services. A service is identified as an Ethernet virtual circuit (EVC) service.

Troubleshooting carrier networks offering Ethernet Layer 2 services is challenging. Customers contract with service providers for end-to-end Ethernet service and service providers may subcontract with operators to provide equipment and networks. Compared to enterprise networks, where Ethernet traditionally has been implemented, these constituent networks belong to distinct organizations or departments, are substantially larger and more complex, and have a wider user base. Ethernet CFM provides a competitive advantage to service providers for which the operational management of link uptime and timeliness in isolating and responding to failures is crucial to daily operations.

Benefits of IEEE CFM

- End-to-end service-level OAM technology.
- Reduced operating expense for service provider Ethernet networks.
- Competitive advantage for service providers.
- Support for both distribution and access network environments with Down (toward the wire) MEPs.

CFM Limitations and Restrictions in CPT

- CFM over the point–to–point bridge domain is not supported.
- CFM over Virtual Private LAN Service (VPLS) is not supported.
- Maximum number of Maintenance End Points (MEPs) supported on a CPT system is 16000 depending on the Continuity Check (CC) interval.
- Maximum number of Maintenance Intermediate Points (MIPs) supported on a CPT system is 16000.

- CFM alarms in CTC is not supported.
- CFM over VLAN based forwarding is not supported.
- CFM is not supported on a bridge domain that has the split horizon configured.
- CFM handles blocked ports only for tagged packets as REP operates only on tagged packets.

The following table specifies the number of supported remote and local MEPs depending on the configured CC interval.

Table 35: Supported Remote and Local MEPs

CC Interval	Number of Remote MEPS	Number of Local MEPs
100 milliseconds	100	100
1 second	1000	1000
10 seconds	8000	8000
1 minute	16000	16000
10 minutes	16000	16000

NTP-J106 Configure CFM Using Cisco IOS Commands

Purpose	This procedure configures CFM using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J305 Enable or Disable CFM on the CPT System Using Cisco IOS Commands, on page 661
- DLP-J308 Enable or Disable CFM on an Interface Using Cisco IOS Commands, on page 663
- DLP-J312 Enable Caching of CFM Data Using Cisco IOS Commands, on page 666
- DLP-J309 Create a Maintenance Domain Using Cisco IOS Commands, on page 669

- DLP-J334 Create a Maintenance Association Using Cisco IOS Commands, on page 672
- DLP-J333 Configure CFM Encapsulation Using Cisco IOS Commands, on page 674
- DLP-J310 Create a Port MEP Using Cisco IOS Commands, on page 680
- DLP-J321 Create an MEP for an EFP Using Cisco IOS Commands, on page 681
- DLP-J319 Define MEPs Statically within a Maintenance Association Using Cisco IOS Commands, on page 683
- DLP-J318 Specify the Number of MEPs in a Maintenance Association Using Cisco IOS Commands, on page 684
- DLP-J323 Configure Cross-Check for an MEP Using Cisco IOS Commands, on page 686
- DLP-J311 Create an MIP Dynamically Using Cisco IOS Commands, on page 690
- DLP-J322 Create an MIP Manually Using Cisco IOS Commands, on page 691
- DLP-J316 Enable the Transmission of Continuity Check Messages Using Cisco IOS Commands, on page 694
- DLP-J324 Send CFM Loopback and Linktrace Messages Using Cisco IOS Commands, on page 697
- DLP-J314 Enable CFM Traps Using Cisco IOS Commands, on page 700
- DLP-J315 Enable SNMP Trap Generation for CFM Continuity Check Events Using Cisco IOS Commands, on page 701

Stop. You have completed this procedure.

NTP-J105 Configure CFM Using CTC

Purpose	This procedure configures CFM using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J299 Enable or Disable CFM on the CPT System Using CTC, on page 662
- DLP-J300 Enable or Disable CFM for Each Port or Channel Group Using CTC, on page 665
- DLP-J313 Enable Caching of CFM Data Using CTC, on page 667

- DLP-J301 Create and Modify a Maintenance Domain Profile Using CTC, on page 670
- DLP-J302 Delete a Maintenance Domain Profile Using CTC, on page 671
- DLP-J303 Create and Modify a Maintenance Association Profile Using CTC, on page 675
- DLP-J304 Delete a Maintenance Association Profile Using CTC, on page 677
- DLP-J306 Create an MEP Using CTC, on page 687
- DLP-J307 Create an MIP Using CTC, on page 693

Stop. You have completed this procedure.

DLP-J305 Enable or Disable CFM on the CPT System Using Cisco IOS Commands

Purpose	This procedure enables or disables Ethernet CFM globally on the CPT system using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ethernet cfm global** **Example:** Router(config)# ethernet cfm global	Enables Ethernet CFM globally on the system. The **no** form of this command disables Ethernet CFM globally on the system.

	Command or Action	Purpose
Step 4	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 5	Return to your originating procedure (NTP).	—

Example: Enable or Disable CFM on the System

The following example shows how to enable CFM on the system using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# ethernet cfm global
```

The following example shows how to disable CFM on the system using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# no ethernet cfm global
```

DLP-J299 Enable or Disable CFM on the CPT System Using CTC

Purpose	This procedure enables or disables CFM on the CPT system using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note CFM is disabled globally on the system by default. This indicates that the CFM frames are transparently forwarded in the system.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to enable or disable CFM on the CPT system.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 In the left pane, click **CFM**.

Step 5 Click the **Global Settings** tab.

Step 6 In the Global Settings area, check the **Enable CFM** check box to enable CFM on the CPT system. Uncheck the **Enable CFM** check box to disable CFM on the CPT system.

Step 7 Check the **MIP Filter Enable** check box to configure a CFM MIP filter that drops all the CFM frames at a lower level irrespective of whether they originate from the wire or the bridge relay.

Step 8 Enter a value in the MEP Cross Check Delay field to specify the number of seconds a device waits for remote MEPs to come up before the cross-check starts. The default value is 30. The range is from 1 to 65535.

Step 9 Click **Apply**.

Step 10 Return to your originating procedure (NTP).

DLP-J308 Enable or Disable CFM on an Interface Using Cisco IOS Commands

Purpose	This procedure enables or disables CFM on an interface using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**ethernet cfm interface** **Example:** Router(config-if)# ethernet cfm interface	Enables the Ethernet CFM processing on the interface. The **no** form of this command disables Ethernet CFM processing on the interface.
Step 5	**exit** **Example:** Router(config-if)# exit	Returns to global configuration mode.
Step 6	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

Example: Enable or Disable CFM on an Interface

The following example shows how to enable CFM on an interface using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# ethernet cfm interface
```

The following example shows how to disable CFM on an interface using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# no ethernet cfm interface
```

DLP-J300 Enable or Disable CFM for Each Port or Channel Group Using CTC

Purpose	This procedure enables or disables CFM for each port or channel group using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note CFM is enabled on each port by default. If CFM is disabled on a port, the CFM packets on that port are dropped.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to enable or disable CFM for each port or channel group.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 In the left pane, click **CFM**.

Step 5 Click the **Global Settings** tab.

Step 6 In the Ethernet Interfaces area, expand the slot of the fabric card or the line card or the Fan–Out–Group (FOG) of the CPT 50 panel.

Step 7 If you want to enable CFM on a specific port, check the **Enable CFM** check box against that port. Uncheck the **Enable CFM** check box against the port to disable CFM on the port.

Step 8 In the Channel Groups area, if you want to enable CFM on a specific channel group, check the **Enable** check box against that channel group.

Step 9 Click **Apply** to enable CFM on the port or the channel group.

Step 10 Return to your originating procedure (NTP).

DLP-J312 Enable Caching of CFM Data Using Cisco IOS Commands

Purpose	This procedure enables caching of CFM data using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ethernet cfm traceroute cache** **Example:** Router(config)# ethernet cfm traceroute cache	Enables caching of CFM data learned through traceroute messages.
Step 4	**ethernet cfm traceroute cache size** *entries* **Example:** Router(config)# ethernet cfm traceroute cache size 200	Sets the size for the CFM traceroute cache table. The default value is 100 entries. The range is from 1 to 4095 entries.
Step 5	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** Router(config)# ethernet cfm traceroute cache holdtime 60	Sets the amount of time (in minutes) that CFM traceroute cache entries are retained. The default value is 100 minutes. The range is from 1 to 65535 minutes.

	Command or Action	Purpose
Step 6	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

Example: Enable Caching of CFM Data

The following example shows how to set the maximum number of entries in the CFM traceroute cache table to 2500 using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# ethernet cfm traceroute cache size 2500
```

The following example shows how to set the retention time for entries in the CFM traceroute cache table to 5 minutes using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# ethernet cfm traceroute cache hold-time 5
```

DLP-J313 Enable Caching of CFM Data Using CTC

Purpose	This procedure enables caching of CFM data using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to enable caching of CFM data.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 In the left pane, click **CFM**.

Step 5 Click the **Global Settings** tab.

Step 6 In the Cache Configuration area, check the **Enable** check box to enable caching of CFM data learned through traceroute messages.

Step 7 Enter the time in minutes in the HoldTime field to set the amount of time that CFM traceroute cache entries are retained. The default value is 100 minutes. The range is from 1 to 65535 minutes.

Step 8 Enter the cache size in the Size field to set the maximum size for the CFM traceroute cache table. The default value is 100. The range is from 1 to 4095.

Step 9 Click **Apply** to enable caching of CFM data.

Step 10 Return to your originating procedure (NTP).

Understanding Maintenance Domain

A maintenance domain is an administrative domain for managing and administering a network. The maintenance domain allows CFM to support multiple independent operators, each supporting service instances from multiple independent customers.

A unique maintenance level in the range of 0 to 7 is assigned to each maintenance domain by a network administrator. Maintenance levels and domain names are useful for defining the hierarchical relationship that exists among domains. The hierarchical relationship of domains parallels the structure of customer, service provider, and operator. The higher the domain level, the broader the scope of the domain. For example, a customer domain would be larger than an operator domain. The customer domain may have a maintenance level of 7 and the operator domain may have a maintenance level of 0. Typically, operators would have the smallest domains and customers the largest domains, with service provider domains in between these domains, varying in size. All levels of the hierarchy must operate together.

Domains must not intersect because intersecting would mean management by more than one entity, which is not allowed. Domains may nest or touch but when two domains nest, the outer domain must have a higher maintenance level than the domain nested within it. Nesting maintenance domains is useful in the business model where a service provider contracts with one or more operators to provide Ethernet service to a customer. Each operator would have its own maintenance domain and the service provider would define its domain that is a superset of the operator domains. Furthermore, the customer has its own end-to-end domain, which is in turn is a superset of the service provider domain. Maintenance levels of various nesting domains must be communicated among the administering organizations. For example, one approach would be to have the service provider assign maintenance levels to operators.

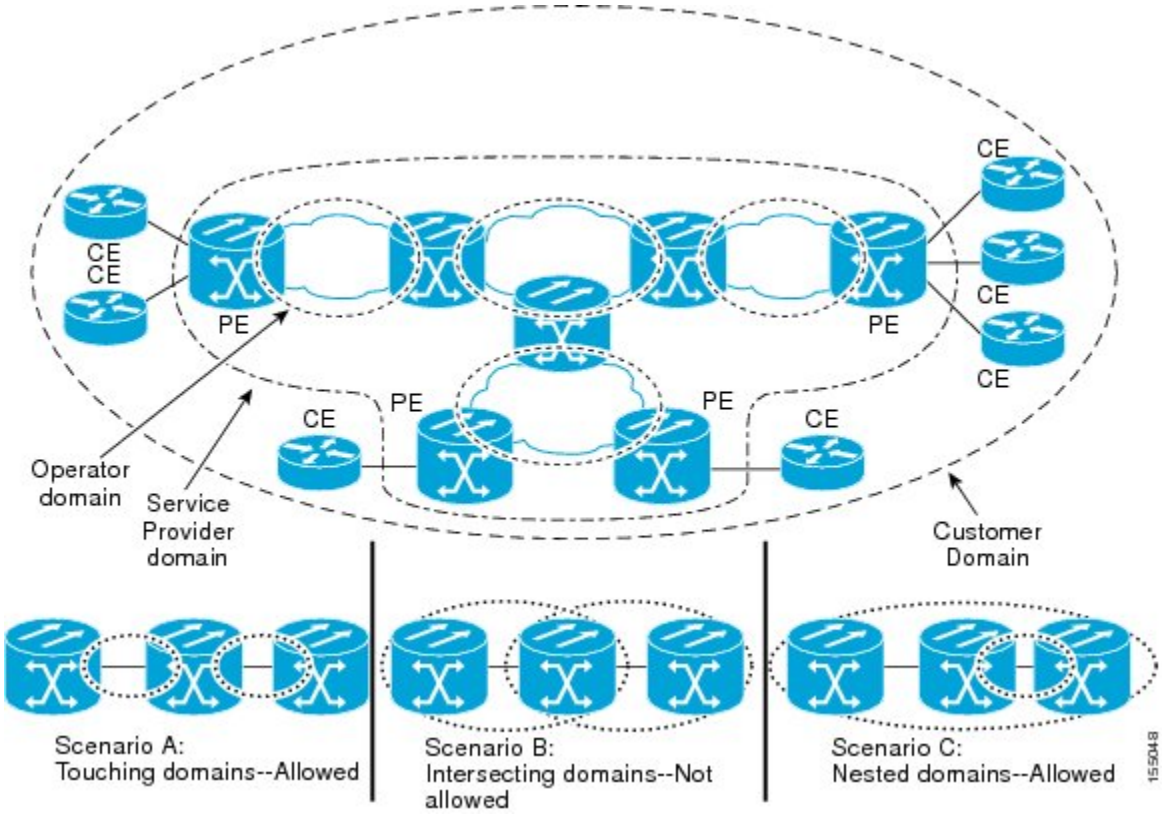
The following characteristics of maintenance domains are supported:

- Maintenance domains are identified by a unique domain name that can be up to 154 characters.

- The domain name as null is supported; the maintenance association name is used as the identifier.
- Domain configuration is not required for devices that have only Maintenance Intermediate Points (MIPs).
- Mix of Up (toward the bridge) and Down (toward the wire) Maintenance Association End Points (MEPs) is supported.

A domain can be removed when all the maintenance points within the domain have been removed and all the remote MEPs entries in the continuity check database (CCDB) for the domain have been purged.

The following figure illustrates a hierarchy of operator, service provider, and customer domains and also illustrates touching, intersecting, and nested domains.



DLP-J309 Create a Maintenance Domain Using Cisco IOS Commands

Purpose	This procedure creates a maintenance domain using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** Router(config)# ethernet cfm domain customer level 7	Creates a CFM maintenance domain at a specific maintenance level and enters Ethernet CFM configuration mode. The range of the maintenance domain level is from 0 to 7. **Note** You can create several maintenance domains at the same maintenance level. However, you cannot create a maintenance domain at several maintenance levels.
Step 4	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 5	Return to your originating procedure (NTP).	—

Example: Create a Maintenance Domain

The following example shows how to define a domain named domain1 at level 6 and enters Ethernet CFM configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# ethernet cfm domain domain1 level 6
Router(config-ecfm)#
```

DLP-J301 Create and Modify a Maintenance Domain Profile Using CTC

Purpose	This procedure creates or modifies a maintenance domain profile using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to create or modify a maintenance domain profile.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 In the left pane, click **CFM**.

Step 5 Click the **Domain Profiles** tab.

Step 6 Click **Add row(s)**.

Step 7 Enter the name of the domain in the Domain Name field.

Step 8 Enter the level of the domain profile in the Level field. The domain profile level ranges from 0 to 7.

Step 9 Check the **Sender Id** check box to include the contents of the Sender ID time-length-value (TLV) field transmitted in CFM messages for members of a maintenance domain.

Step 10 Check the **Auto Create MIP** check box to allow the automatic creation of an MIP at this maintenance domain level.

Step 11 Check the **Lower MEP** check box. When this check box and **Auto Create MIP** check box are checked, auto MIPs are created at a specified level only where an MEP is configured at the next lower level for a maintenance domain.

Step 12 Enter a value in the Archive Hold Timer field to specify the number of minutes that data from a missing MEP is kept before it is purged. The default value is 100 minutes. The range is from 1 to 65535 minutes.

Step 13 Click **Store**.

Step 14 In the CFM Profile Storing dialog box, choose the node and shelf where you want to store this domain profile and click **OK**.

Step 15 To modify a maintenance domain profile, double-click the required parameters, change the values, and click **Apply**.

Step 16 Return to your originating procedure (NTP).

DLP-J302 Delete a Maintenance Domain Profile Using CTC

Purpose	This procedure deletes a maintenance domain profile using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to delete a maintenance domain profile.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 In the left pane, click **CFM**.

Step 5 Click the **Domain Profiles** tab.

Step 6 Click **Load** to load the maintenance domain profiles from the system. The CFM Profile Loading dialog box appears.

Step 7 Choose the shelf and click **OK**. The domain profiles appear in the Domain Profiles tab.

Step 8 Choose a domain profile to delete.

Step 9 Check the **On Node** check box.

Step 10 Click **Delete Sel row(s)**. The CFM Profile Deleting dialog box appears.

Step 11 Choose the shelf to delete the domain profile from and click **OK**.

Step 12 Click **Yes** in the confirmation dialog box.

Step 13 Return to your originating procedure (NTP).

Understanding Maintenance Association

There can be any number of maintenance associations (MA) within a maintenance domain. A maintenance association identifies a service that can be uniquely identified within the maintenance domains. The CFM protocol runs within a specific maintenance association.

The MA direction is specified when the MA is configured. The MA name must be configured on a domain before MEPs can be configured. Configuring an MA is not required for devices that have only MIPs.

DLP-J334 Create a Maintenance Association Using Cisco IOS Commands

Purpose	This procedure creates a maintenance association using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** Router(config)# ethernet cfm domain Customer level 7	Creates a maintenance domain at a specified level and enters Ethernet CFM configuration mode.
Step 4	**service** {*ma-name* | **number** *ma-num*} {**evc** *evc-name* | **port** } [**direction down**] **Example:** Router(config-ecfm)# service Customer1 port	Creates a maintenance association within a maintenance domain and enters CFM service configuration mode.
Step 5	**exit** **Example:** Router(config-ecfm)# exit	Returns to global configuration mode.
Step 6	Return to your originating procedure (NTP).	—

Example: Create a Maintenance Association

The following example shows how to create a maintenance association using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# ethernet cfm domain operator level 5
Router(config-ecfm)# service operatorA port
Router(config-ecfm)# exit
```

DLP-J333 Configure CFM Encapsulation Using Cisco IOS Commands

Purpose	This procedure configures CFM encapsulation using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**service instance** *id* **ethernet** [*evc-id*] **Example:** Router(config-if)# service instance 101 ethernet	Configures an Ethernet service instance on an interface and enters service instance configuration mode.
Step 5	**encapsulation dot1q** {*any* | *vlan-id* [*vlan-id* [*-vlan-id*]]} **second-dot1q** {*any* | *vlan-id* [*vlan-id* [*-vlan-id*]]} **Example:** Router(config-if-srv)# encapsulation dot1q 100-110 second dot1q 200	Defines the matching criteria that maps the ingress dot1q, QinQ, or untagged frames on an interface to the appropriate service instance.

	Command or Action	Purpose
Step 6	**bridge-domain** *bridge-id* [**split-horizon**] **Example:** Router(config-if-srv)# bridge-domain 12	Binds the Ethernet service instance to a bridge domain instance where *bridge-id* is the identifier for the bridge domain instance.
Step 7	**cfm encapsulation** {**dot1ad** *vlan-id* | **dot1q** *vlan-id*} [**dot1q** *vlan-id* | **second-dot1q** *vlan-id*] **Example:** Router(config-if-srv)# cfm encapsulation dot1q 105 second dot1q 200	Defines the matching criteria that maps the ingress dot1q, QinQ, or untagged frames on an interface to the appropriate service instance.
Step 8	**exit** **Example:** Router(config-if-srv)# exit	Exits the service instance configuration mode.
Step 9	**exit** **Example:** Router(config-if)# exit	Returns to global configuration mode.
Step 10	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 11	Return to your originating procedure (NTP).	—

DLP-J303 Create and Modify a Maintenance Association Profile Using CTC

Purpose	This procedure creates or modifies a maintenance association profile using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to create or modify a maintenance association profile.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 In the left pane, click **CFM**.

Step 5 Click the **MA Profiles** tab.

Step 6 Click **Add row(s)**.

Step 7 Enter the name of the maintenance association profile in the Maintenance Profile Name field.

Step 8 Enter the unique ID used to represent a service in the Service ID field.
Service IDs identify customers within a domain. A service ID must be unique within a single maintenance domain.

Step 9 Check the **CC Enable** check box to globally enable transmission of Continuity Check Messages (CCMs).

Step 10 From the CC Interval drop-down list, choose the interval to transmit CCMs.
The valid values are as follows:

- 100 ms—100 milliseconds
- 1 sec—1 second
- 10 sec—10 seconds
- 1 min—1 minute
- 10 min—10 minutes

Step 11 Enter the number of CCMs that must be missed before declaring that a remote MEP is down, in the CC Threshold field.
The range is from 2 to 255. The default value is 3.

Step 12 Check the **Direction Down** check box to configure the service direction toward the LAN.

Step 13 Enter the maintenance domain name in the Domain Name field to attach this maintenance association profile to a maintenance domain profile.

Step 14 Check the **Auto Create MIP** check box to dynamically create an MIP.

Step 15 Check the **Port** check box to create a port MEP.

Step 16 Check the **Lower MEP Only** check box. When this check box and **Auto Create MIP** check box are checked, auto MIPs are created at a specified level only where an MEP is configured at the next lower level for a maintenance domain.

Step 17 Check the **CFM EFM Interaction** check box to enable the CFM and EFM protocols to interoperate.
CFM and EFM can interoperate together and can co-exist on the same port. CFM and EFM cannot interoperate together if CFM MEP is configured on the channel group. Use the **oam protocol cfm domain** *domain-name* to configure CFM and EFM to interoperate together using Cisco IOS commands.

Step 18 Enter the static MEP ID or a list of static MEP IDs in the Static MEP Id field to statically specify the MEP IDs. The range is from 1 to 8191.

Step 19 Check the **MEP Cross Check Enable** check box to enable cross-checking between the list of configured remote MEPs of a domain and MEPs learned through CCMs.

Step 20 Enter the outer dot1q encapsulation tag value in the Outer CFM Encapsulation field.

Step 21 Enter the inner dot1q encapsulation tag value in the Inner CFM Encapsulation field.

Step 22 Click **Store**.

Step 23 Choose the node and shelf where you want to store this maintenance association profile and click **OK**.

Step 24 To modify a maintenance association profile, double-click the required parameters, change the values, and click **Apply**.

Step 25 Return to your originating procedure (NTP).

DLP-J304 Delete a Maintenance Association Profile Using CTC

Purpose	This procedure deletes a maintenance association profile using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to delete a maintenance association profile.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 In the left pane, click **CFM**.

Step 5 Click the **MA Profiles** tab.

Step 6 Click **Load** to load the maintenance association profiles from the system. The CFM Profile Loading dialog box appears.

Step 7 Choose the shelf and click **OK**. The maintenance association profiles appear in the MA Profiles tab.

Step 8 Choose an association profile to delete.

Step 9 Check the **On Node** check box.

Step 10 Click **Delete Sel row(s)**. The CFM Profile Deleting dialog box appears.

Step 11 Choose the shelf to delete the association profile from and click **OK**.

Step 12 Click **Yes** in the confirmation dialog box.

Step 13 Return to your originating procedure (NTP).

Understanding Maintenance Point

Any port of a bridge is referred to as a Maintenance Point. A maintenance point is a demarcation point on an interface or port that participates in CFM within a maintenance domain. Maintenance points must be explicitly configured on Cisco devices.

There are two classes of maintenance points:

- Maintenance End Points (MEPs)
- Maintenance Intermediate Points (MIPs)

Understanding Maintenance End Points

MEPs reside at the edge of a maintenance domain and are active elements of CFM. They confine CFM messages within the domain through the maintenance domain level. MEPs periodically transmit and receive continuity check messages (CCMs) from other MEPs within the domain. MEPs also transmit linktrace and loopback messages at the request of the administrator.

MEP ID uniquely identifies each MEP along with those configured on a single MA. The MEP IDs range from 1 to 8191.

There are two types of MEPs:

- Up (inwards, toward the bridge). This is the default.

- Down (outwards, toward the wire).

MEP supports multicast loopbacks and pings. When a multicast ping is initiated for a particular domain or service, all the related remote MEPs reply to the ping.

MEP configurations can be removed after all pending loopback and linktrace replies are removed and the service on the interface is set to transparent mode. To set the service to transparent mode, MIP filtering must not be configured.

Understanding Up MEPs

An Up MEP is an MEP that resides in a bridge and transmits to and receives CFM messages from the direction of the bridge relay entity.

An Up MEP performs the following functions:

- Sends and receives CFM frames at its level through the bridge relay and not through the wire connected to the port on which the MEP is configured.
- Drops all CFM frames at its level (or lower level) that come from the direction of the wire.
- Processes all CFM frames at its level coming from the direction of the bridge.
- Drops all CFM frames at a lower level coming from the direction of the bridge.
- Forwards all CFM frames transparently at a higher level, independent of whether they came in from the bridge or wire.

Understanding Down MEPs

A Down MEP is an MEP that resides in a bridge and transmits to and receives CFM messages from the direction of the wire.

A Down MEP performs the following functions:

- Sends and receives CFM frames at its level through the wire connected to the port where the MEP is configured.
- Drops all CFM frames at its level (or at a lower level) that come from the direction of the bridge.
- Processes all CFM frames at its level coming from the direction of the wire.
- Drops all CFM frames at a lower level coming from the direction of the wire.
- Forwards all CFM frames transparently at a higher level, independent of whether they came in from the bridge or wire.

Understanding Port MEPs

CPT also supports Port MEP at the physical port. A port MEP can be created either on the physical port or on the port of a channel group. The port MEP takes higher precedence if both the port MEP and the Down MEP on untagged EFP is created on the same port.

Understanding the Cross-Check Function

The cross-check function is a timer-driven post-provisioning service verification between dynamically discovered MEPs (through CCMs) and expected MEPs (through configuration) for a service. The cross-check function verifies that all the endpoints of a multipoint or point-to-point service are operational. The function supports notifications when the service is operational; otherwise it provides alarms and notifications for unexpected or missing endpoints.

You must initiate the cross-check function each time you want a service verification. See DLP-J323 Configure Cross-Check for an MEP Using Cisco IOS Commands, on page 686.

DLP-J310 Create a Port MEP Using Cisco IOS Commands

Purpose	This procedure creates a port MEP using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**ethernet cfm mep domain** *domain-name* **mpid** *mpid* {**port**} **Example:**	Sets a port as internal to a maintenance domain and creates a port MEP. A port MEP can be created only on a physical port or on a port of a channel group.

	Command or Action	Purpose
	Router(config-if)# ethernet cfm mep domain Customer mpid 701 port	
Step 5	**exit** **Example:** Router(config-if)# exit	Returns to global configuration mode.
Step 6	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

Example: Create a Port MEP

The following example shows how to set a port as internal to a maintenance domain and creates a port MEP:

```
Router> enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# ethernet cfm mep domain CustomerB mpid 5 port
```

DLP-J321 Create an MEP for an EFP Using Cisco IOS Commands

Purpose	This procedure creates an MEP for an EFP using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**service instance** *id* **ethernet** [*evc-id*] **Example:** Router(config-if)# service instance 101 ethernet	Configures an Ethernet service instance on an interface and enters service instance configuration mode.
Step 5	**encapsulation dot1q** {*any* | *vlan-id* [*vlan-id* [*-vlan-id*]]} **second-dot1q** {*any* | *vlan-id* [*vlan-id* [*-vlan-id*]]} **Example:** Router(config-if-srv)# encapsulation dot1q 100 second dot1q 200	Defines the matching criteria that maps the ingress dot1q, QinQ, or untagged frames on an interface to the appropriate service instance.
Step 6	**bridge-domain** *bridge-id* [**split-horizon**] **Example:** Router(config-if-srv)# bridge-domain 12	Binds the Ethernet service instance to a bridge domain instance where *bridge-id* is the identifier for the bridge domain instance.
Step 7	**cfm mep domain** *domain-name* **mpid** *mpid-value* **Example:** Router(config-if-srv)# cfm mep domain Customer mpid 701	Creates an MEP under the Ethernet service instance.
Step 8	**exit** **Example:** Router(config-if-srv)# exit	Exits the service instance configuration mode.
Step 9	**exit** **Example:** Router(config-if)# exit	Returns to global configuration mode.
Step 10	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 11	Return to your originating procedure (NTP).	—

Example: Create an MEP for an EFP

The following example shows how to create an MEP for an EFP using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# service instance 101 ethernet
Router(config-if-srv)# encapsulation  dot1q 100
Router(config-if-srv)# bridge-domain 12
Router(config-if-srv)# cfm mep domain CustomerB mpid 5
Router(config-if-srv)# exit
```

DLP-J319 Define MEPs Statically within a Maintenance Association Using Cisco IOS Commands

Purpose	This procedure statically defines MEPs within a maintenance association using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ethernet cfm domain** *domain-name* **level** *level-id*	Defines a CFM domain at a specified level and enters Ethernet CFM configuration mode. The

	Command or Action	Purpose
	Example: Router(config)# ethernet cfm domain Customer level 7	range of maintenance domain level is from 0 to 7.
Step 4	**service** {*ma-name* | **number** *ma-num*} {**evc** *evc-name* | **port** } [**direction down**] **Example:** Router(config-ecfm)# service Customer1 port	Configures a maintenance association within a maintenance domain for a port MEP or MEP for an EFP and enters CFM service configuration mode.
Step 5	**mep mpid** *mpid* **Example:** Router(config-ecfm-srv)# mep mpid 702	Statically defines the MEPs within a maintenance association.
Step 6	**exit** **Example:** Router(config-ecfm-srv)# exit	Returns to Ethernet CFM configuration mode.
Step 7	**exit** **Example:** Router(config-ecfm)# exit	Returns to global configuration mode.
Step 8	Return to your originating procedure (NTP).	—

Example: Define the MEPs Statically within a Maintenance Association

The following example shows how to configure an MEP with an ID of 25 using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# ethernet cfm domain operator level 5
Router(config-ecfm)# service operatorA port
Router(config-ecfm-srv)# mep mpid 25
Router(config-ecfm-srv)# exit
Router(config-ecfm)# exit
```

DLP-J318 Specify the Number of MEPs in a Maintenance Association Using Cisco IOS Commands

Purpose	This procedure allows you to specify the number of MEPs in a maintenance association using Cisco IOS commands.
Tools/Equipment	None

Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** Router(config)# ethernet cfm domain Customer level 7	Defines a CFM domain at a specified level and enters Ethernet CFM configuration mode. The range of maintenance domain level is from 0 to 7.
Step 4	**service** {*ma-name* | **number** *ma-num*} {**evc** *evc-name* | **port**} [**direction down**] **Example:** Router(config-ecfm)# service Customer1 port	Configures a maintenance association within a maintenance domain for a port MEP or MEP for an EFP and enters CFM service configuration mode.
Step 5	**maximum meps** *max-num* **Example:** Router(config-ecfm-srv)# maximum meps 50	Specifies the maximum number of MEPs in a maintenance association. The default is 100. The range is from 1 to 65535.
Step 6	**exit** **Example:** Router(config-ecfm-srv)# exit	Returns the CLI to Ethernet CFM configuration mode.
Step 7	**exit** **Example:** Router(config-ecfm)# exit	Returns to global configuration mode.
Step 8	Return to your originating procedure (NTP).	—

Example: Specify the Number of MEPs in a Maintenance Association

The following example shows how to configure a maximum of 50 MEPs using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# ethernet cfm domain operator level 5
Router(config-ecfm)# service operatorA port
Router(config-ecfm-srv)# maximum meps 50
Router(config-ecfm-srv)# exit
Router(config-ecfm)# exit
```

DLP-J323 Configure Cross-Check for an MEP Using Cisco IOS Commands

Purpose	This procedure configures cross-checking for an MEP using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** Router(config)# ethernet cfm domain ServiceProvider level 4	Creates a maintenance domain at a specified level and enters Ethernet CFM configuration mode. The range of maintenance domain level is from 0 to 7.

	Command or Action	Purpose
Step 4	**service** {*ma-name* | **number** *ma-num*} {**evc** *evc-name* | **port** } [**direction down**] **Example:** Router(config-ecfm)# service Customer1 port	Configures a maintenance association within a maintenance domain and enters CFM service configuration mode.
Step 5	**mep mpid** *mpid* **Example:** Router(config-ecfm-srv)# mep mpid 702	Statically defines the MEPs within a maintenance association.
Step 6	**exit** **Example:** Router(config-ecfm-srv)# exit	Returns to Ethernet CFM configuration mode.
Step 7	**exit** **Example:** Router(config-ecfm)# exit	Returns to global configuration mode.
Step 8	**ethernet cfm mep crosscheck start-delay** *delay* **Example:** Router(config)# ethernet cfm mep crosscheck start-delay 60	Configures the maximum amount of time that the device waits for remote MEPs to come up before the cross-check operation is started. The default value is 30 seconds. The range is from 1 to 65535 seconds.
Step 9	**exit** **Example:** Router(config)# exit	Returns to privileged EXEC mode.
Step 10	**ethernet cfm mep crosscheck** {**enable** | **disable**} **domain** *domain-name* **port** **Example:** Router# ethernet cfm mep crosscheck enable domain cust4 port	Enables cross-checking between the list of configured remote MEPs of a domain and MEPs learned through CCMs.
Step 11	Return to your originating procedure (NTP).	—

DLP-J306 Create an MEP Using CTC

Purpose	This procedure creates a maintenance end point using CTC.

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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to create a maintenance end point.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 In the left pane, click **CFM**.

Step 5 Click the **MEP** tab.

Step 6 Click **Create**. The Create MEP dialog box appears.

Step 7 To create an MEP on an EFP:

a) Choose the **Service Id** option.
b) From the Domain drop-down list, choose a maintenance domain.
c) Enter the service id in the Service ID field.
d) Enter the maintenance point ID (MPID) in the MPID field.
The MPID ranges from 1 to 8191. The MPID must not be the same between the maintenance end points.
e) Enter the class-of-service (CoS) for CFM packets in the COS field.
The range of CoS is from 0 to 7.

Step 8 To create an MEP on a port:

Note A port MEP can be created only on a physical port or on a port of a channel group.

a) Choose the **Port** option.
b) From the Slot drop-down list, choose a fabric card or a line card slot.
c) From the Port drop-down list, choose a port.
d) From the Domain drop-down list, choose a maintenance domain.
e) Enter the maintenance point ID (MPID) in the MPID field.
The MPID ranges from 1 to 8191. The MPID must not be the same between the maintenance end points.
f) Enter the class-of-service (CoS) for CFM packets in the COS field.
The range of CoS is from 0 to 7.

Step 9 To create an MEP on a channel group:

a) Check the **MEP on Ch.Grp** check box.
b) From the Domain drop-down list, choose a maintenance domain.
c) Enter the service id in the Service ID field.
d) Enter the maintenance point ID (MPID) in the MPID field.

The MPID ranges from 1 to 8191. The MPID must not be the same between the maintenance end points.

e) Enter the class-of-service (CoS) for CFM packets in the COS field.
The range of CoS is from 0 to 7.

f) From the Ch Grp drop-down list, choose a channel group.

Step 10 Click **OK** in the Create MEP dialog box to create an MEP.

Step 11 To delete an MEP:

a) Choose an MEP to delete in the MEP tab.
b) Click **Delete**.
c) Click **Yes** in the Delete MEP dialog box.

Step 12 Return to your originating procedure (NTP).

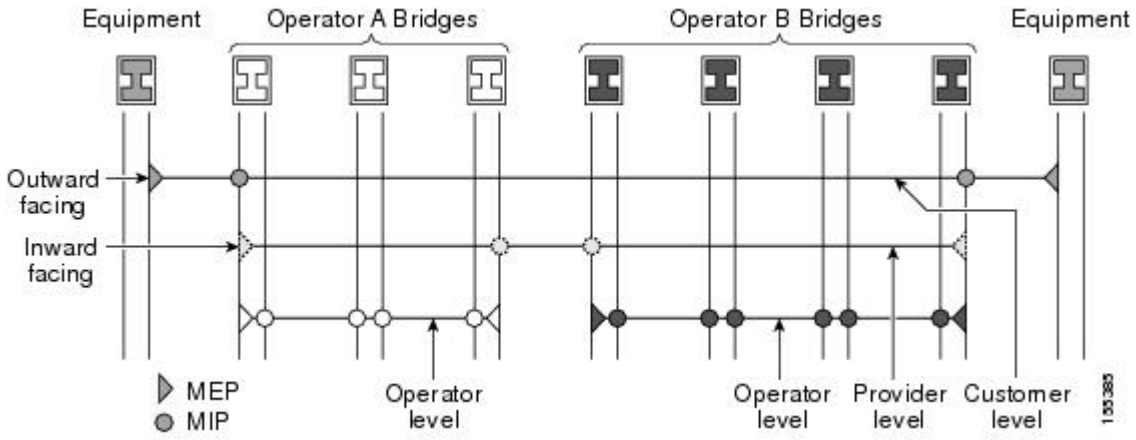
Understanding Maintenance Intermediate Points

Maintenance intermediate points (MIPs) are internal to the maintenance domain and are passive elements of CFM. They store information received from MEPs and other MIPs and respond only to CFM linktrace and loopback messages. An MIP has only one level associated with it. MIPs forward CFM messages within a maintenance domain.

MIPs are defined as two MIP half functions (MHFs)—An Up MHF that resides above the port filtering entities and a Down MHF that resides below the port filtering entities. The same configuration parameters and characteristics apply to both MHFs of an MIP:

- Can be created manually or dynamically (auto MIPs).
- Dynamically created depending on configured policies at managed objects (MA, maintenance domain, or the default domain level).
- Manual MIPs can be created under an interface and under a service instance within an interface.
- Auto MIP commands can be issued globally or under a domain or service.
- Can be created per MA, which means that an MIP in the MA can be lower level than an MEP in another MA.
- CFM frames received from MEPs and other MIPs are cataloged and forwarded, using both the wire and the bridge relay.
- When MIP filtering is enabled, all CFM frames at a lower level are stopped and dropped, independent of whether they originate from the wire or the bridge relay.
- All CFM frames at a higher level are forwarded, independent of whether they arrive from the wire or from the bridge relay.
- Passive points respond only when triggered by CFM linktrace and loopback messages.

The following figure illustrates MEPs and MIPs at the operator, service provider, and customer levels.



DLP-J311 Create an MIP Dynamically Using Cisco IOS Commands

Purpose	This procedure creates an MIP dynamically using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note **ethernet cfm mip auto-create** command has lower precedence than the **ethernet cfm mip level** manual MIP command. For example, if you manually configure an MIP for a particular maintenance association, that configuration overrides the MIP created by the global **ethernet cfm mip auto-create** command for that maintenance association.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ethernet cfm mip {auto-create level** *level-id* [**lower-mep-only**] [**sender-id chassis**] | **filter**} **Example:** Router(config)# ethernet cfm mip auto-create level 1	Dynamically creates an MIP and provisions it globally at a specified maintenance level and enables level filtering.
Step 4	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 5	Return to your originating procedure (NTP).	—

Example: Create an MIP Dynamically

The following example shows how to dynamically create an MIP at maintenance level 6 using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# ethernet cfm mip auto-create level 6
```

DLP-J322 Create an MIP Manually Using Cisco IOS Commands

Purpose	This procedure creates an MIP manually using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You cannot configure an MIP at a level lower than the level of already configured maintenance endpoints (MEPs) on an interface. Configuring an MIP using this command is known as a manual MIP and has precedence over the **ethernet cfm mip auto-create** command.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**ethernet cfm mip level** *level-id* **Example:** Router(config-if)# ethernet cfm mip level 1	Creates an MIP manually at a specified maintenance level on an interface. The range of level is from 0 to 7.
Step 5	**exit** **Example:** Router(config-if)# exit	Returns to global configuration mode.
Step 6	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

Example: Create an MIP Manually

The following example shows how to provision an MIP manually at maintenance level 5 using Cisco IOS commands.

```
Router> enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# ethernet cfm mip level 5
Router(config-if)# exit
```

DLP-J307 Create an MIP Using CTC

Purpose	This procedure creates a maintenance intermediate point with a specific maintenance level using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to create a maintenance intermediate point.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 In the left pane, click **CFM**.

Step 5 Click the **MIP** tab.

Step 6 Click **Create**. The Create MIP dialog box appears.

Step 7 To create an MIP on an EFP:

a) Choose the **service Id** option.
b) From the Slot drop-down list, choose a fabric card or a line card slot.
c) From the Port drop-down list, choose a port.
d) From the Level drop-down list, choose a maintenance level. The maintenance level ranges from 0 to 7.
e) Enter the service id in the ServiceId field.

Step 8 To create an MIP on a channel group:

a) Check the **MIP on Ch.Grp** check box.
b) From the Level drop-down list, choose a maintenance level. The maintenance level ranges from 0 to 7.
c) Enter the service id in the ServiceId field.
d) From the Ch Grp drop-down list, choose a channel group.

Step 9 Click **OK** in the Create MIP dialog box to create an MIP.

Step 10 To delete an MIP:

a) Choose an MIP to delete in the MIP tab.
b) Click **Delete**.
c) Click **Yes** in the Delete MIP dialog box.

Step 11 Return to your originating procedure (NTP).

Understanding CFM Messages

CFM uses standard Ethernet frames that can be distinguished by their EtherType and for multicast messages by their MAC address. CFM frames are sourced, terminated, processed, and relayed by bridges.

Bridges that cannot interpret CFM messages forward them as normal data frames. All CFM messages are confined to a maintenance domain and to a maintenance association. Three types of messages are supported:

- Continuity Check
- Linktrace
- Loopback

Understanding Continuity Check Messages

CFM continuity check messages (CCMs) are multicast heartbeat messages exchanged periodically among MEPs. They allow MEPs to discover other MEPs within a domain and allow MIPs to discover MEPs. CCMs are confined to a domain.

CFM CCMs have the following characteristics:

- Transmitted at a periodic interval by MEPs. The interval can be one of the following configurable values. The default is 10 seconds.
  - 100 milliseconds
  - 1 second
  - 10 seconds
  - 1 minute
  - 10 minutes
- Cataloged by MIPs at the same maintenance level.
- Terminated by remote MEPs at the same maintenance level.
- Unidirectional and do not solicit a response.
- Indicate the status of the bridge port on which the MEP is configured.

DLP-J316 Enable the Transmission of Continuity Check Messages Using Cisco IOS Commands

Purpose	This procedure enables the transmission of continuity check messages (CCM) using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** Router(config)# ethernet cfm domain Customer level 7	Creates a CFM maintenance domain at a specified maintenance level and enters Ethernet CFM configuration mode. The range of maintenance domain level is from 0 to 7.
Step 4	**service** {*ma-name* | **number** *ma-num*} {**evc** *evc-name* | **port** } [**direction down**] **Example:** Router(config-ecfm)# service Customer1 port	Configures a maintenance association within a maintenance domain for a port MEP or MEP for an EFP and enters CFM service configuration mode.
Step 5	**continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**] **Example:** Router(config-ecfm-srv)# continuity-check	Enables the transmission of CCMs.
Step 6	**continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**] **Example:** Router(config-ecfm-srv)# continuity-check interval 10s	Configures the time period between CCM transmissions.
Step 7	**continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**] **Example:** Router(config-ecfm-srv)# continuity-check lossthreshold 10	Sets the number of CCMs that must be missed before declaring that a remote MEP is down.

	Command or Action	Purpose
Step 8	**exit** **Example:** Router(config-ecfm-srv)# exit	Returns to Ethernet CFM configuration mode.
Step 9	**mep archive-hold-time** *minutes* **Example:** Router(config-ecfm)# mep archive-hold-time 60	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged. The default value is 100 minutes. The range is from 1 to 65535 minutes.
Step 10	**exit** **Example:** Router(config-ecfm)# exit	Returns to global configuration mode.
Step 11	Return to your originating procedure (NTP).	—

Example: Enable the Transmission of Continuity Check Messages

The following example shows how to configure a loss threshold of 50 CCMs using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# ethernet cfm domain operator level 5
Router(config-ecfm)# service operatorA port
Router(config-ecfm-srv)# continuity-check loss-threshold 50
Router(config-ecfm-srv)# exit
Router(config-ecfm)# exit
```

Understanding Loopback Messages

CFM loopback messages (LBMs) are unicast frames that an MEP transmits, at the request of an administrator, to verify connectivity to a specific maintenance point. A loopback message reply (LBR) indicates whether a destination is reachable but does not allow hop-by-hop discovery of the path. A loopback message is similar in concept to an Internet Control Message Protocol (ICMP) Echo (ping) message.

Since LBMs are unicast messages, they are forwarded like normal data frames except with the maintenance level restriction. If the outgoing port is known in the forwarding database of the bridge and allows CFM frames at the maintenance level of the image to pass through, the frame is sent out on that port. If the outgoing port is unknown, the message is broadcast on all the ports in that domain.

A CFM LBM can be generated on demand using the CLI. The source of a loopback message must be an MEP; the destination may be an MEP or MIP. Both CFM LBMs and LBRs are unicast. CFM LBMs specify the destination MAC address or MPID, VLAN, and maintenance domain.

Understanding Linktrace Messages

CFM linktrace messages (LTMs) are multicast frames that an MEP transmits, at the request of an administrator, to track the path (hop-by-hop) to a destination MEP. They are similar to Layer 3 traceroute messages. LTMs allow the transmitting node to discover vital connectivity data about the path and allow the discovery of all MIPs along the path that belong to the same maintenance domain. LTMs are intercepted by maintenance points along the path and processed, transmitted, or dropped. At each hop where there is a maintenance point at the same level, a linktrace message reply (LTR) is transmitted back to the originating MEP. For each visible MIP, linktrace messages indicate ingress action, relay action, and egress action. LTMs are multicast and LTRs are unicast.

DLP-J324 Send CFM Loopback and Linktrace Messages Using Cisco IOS Commands

Purpose	This procedure allows you to send CFM loopback and traceroute messages to a destination MAC address using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**ping ethernet** {**mpid** *mpid* | *mac-address*} {**domain** *domain-name*} {**port** | **evc** *evc-name*} [**source** *source-mpid*] [**cos** *cos-value*] **Example:** Router(config)# ping ethernet 1010.pcef.1010 level 2 evc evc5	Sends CFM loopback messages to the destination MEP through MAC address or MPID.

	Command or Action	Purpose
Step 3	**traceroute ethernet** {**mpid** *mpid* | *mac-address*} {**domain** *domain-name*} {**port** | **evc** *evc-name*} [**cos** *cos-value*] [**fdb-only**] **Example:** Router(config)# traceroute ethernet aabb.cc00.1010 level 4 evc evc_100	Sends CFM traceroute messages to the destination MEP through MAC address or MPID.
Step 4	Return to your originating procedure (NTP).	—

Example: Send CFM Loopback and Traceroute Messages

The following example shows how to send an Ethernet CFM loopback message to MAC address 1010.pcef.1010 on evc5:

```
Router> enable
Router# ping ethernet 1010.pcef.1010 domain domain1 evc evc5
```

The following example shows how to send an Ethernet CFM traceroute message to MAC address aabb.cc00.1010 at maintenance level 4 on evc_100

```
Router> enable
Router# traceroute ethernet aabb.cc00.1010 domain domain1 evc evc_100
```

NTP-J107 Perform ping and traceroute Operations on Services Using CTC

Purpose	This procedure performs ping and traceroute operations on services using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to perform ping and traceroute operations.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Maintenance** tab.

Step 4 In the left pane, click **OAM**.

Step 5 From the Service drop-down list, choose **TP Tunnel**, **TE Tunnel**, **Pseudowire**.

Step 6 From the Command drop-down list, choose **Ping** or **Traceroute**.

Step 7 If you choose TP Tunnel as the service, complete the following:

a) Enter the tunnel ID in the Tunnel No field.

b) From the LSP drop-down list, choose **Active**, **Working**, or **Protect**.

Step 8 If you choose TE Tunnel as the service, complete the following:

a) Enter the tunnel ID in the Tunnel No field.

Step 9 If you choose Pseudowire as the service, complete the following:

a) Enter the IP address in the IP field.

b) Enter the virtual circuit ID in the VC ID field.

Step 10 Click **Execute** to run the OAM operation for the specified service.
Stop. You have completed this procedure.

Understanding Continuity Check Traps and Cross-Check Traps

MEPs generate two types of Simple Network Management Protocol (SNMP) traps. They are Continuity Check (CC) traps and Cross-Check traps.

Continuity Check Traps

- MEP up—Sent when a new MEP is discovered, the status of a remote port changes, or connectivity from a previously discovered MEP is restored after interruption.
- MEP down—Sent when a timeout or last gasp event occurs.
- Cross-connect—Sent when a service ID does not match the VLAN.
- Loop—Sent when an MEP receives its own CCMs.
- Configuration error—Sent when an MEP receives a continuity check with an overlapping MPID.

Cross-Check Traps

- Service up—Sent when all the expected remote MEPs are up in time.
- MEP missing—Sent when an expected MEP is down.

• Unknown MEP—Sent when a CCM is received from an unexpected MEP.

DLP-J314 Enable CFM Traps Using Cisco IOS Commands

Purpose	This procedure enables CFM traps using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**snmp-server enable traps ethernet cfm alarm** **Example:** Router(config)# snmp-server enable traps ethernet cfm alarm	Enables CFM fault alarms (traps).
Step 4	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 5	Return to your originating procedure (NTP).	—

Example: Enable CFM Traps

The following example shows how to enable CFM traps using Cisco IOS commands:

```
Router> enable
```

```
Router# configure terminal
Router(config)# snmp-server enable traps ethernet cfm alarm
Router(config)# end
```

DLP-J315 Enable SNMP Trap Generation for CFM Continuity Check Events Using Cisco IOS Commands

Purpose	This procedure enables SNMP trap generation for CFM Continuity Check events using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**snmp-server enable traps ethernet cfm cc [mep-up][mepdown][config] [loop] [cross-connect]** **Example:** Router(config)# snmp-server enable traps ethernet cfm cc mep-up mep-down config loop cross-connect	Enables SNMP trap generation for CFM mep-up, mep-down, config, loop, and cross-connect continuity check events.
Step 4	**snmp-server enable traps ethernet cfm crosscheck [mepunknown|mep-missing| service-up]** **Example:** Router(config)# snmp-server enable traps ethernet cfm crosscheck mep-unknown	Enables SNMP trap generation for CFM mepunknown, mep-missing, and service-up continuity check events in relation to the cross-check operation between statically configured MEPs and those learned through CCMs.

	Command or Action	Purpose
Step 5	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

Example: Enable SNMP Trap Generation for CFM Continuity Check Events

The following example shows how to enable SNMP trap generation for CFM continuity checks when a new remote MEP is discovered and learned by the device:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps ethernet cfm cc mep-up
```

The following example shows how to enable SNMP trap generation for CFM continuity check events when an unconfigured MEP comes up:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps ethernet cfm crosscheck mep-unknown
```

Understanding Y.1731

Y.1731 Fault Management and Performance Monitoring

Y.1731 is an extension of the Connectivity Fault Management (CFM). The ITU-T Y.1731 feature provides operations, administration, and maintenance (OAM) functions for fault management and performance monitoring to serve the needs of service providers in a large network.

CPT supports Ethernet Alarm Indication Signal (ETH-AIS), Ethernet Remote Defect Indication (ETH-RDI), and Ethernet Locked Signal (ETH-LCK) functionality for fault detection and isolation.

Y.1731 Performance Monitoring (PM) provides a standard Ethernet PM function that includes measurement of Ethernet frame delay, frame delay variation, frame loss, and frame throughput measurements specified by the ITU-T Y-1731 standard. To measure Service Level Agreement (SLA) parameters such as frame delay or frame delay variation, a small number of synthetic frames are transmitted along with the service to the maintenance end point (MEP).

CPT supports only two–way Ethernet frame Delay Measurement (ETH-DM) in Y.1731 performance monitoring. The CPT system sends, receives, and processes PM frames in intervals of 100 ms (10 frames per second) and 1 second.

Note CFM must be enabled in the network for Y.1731 to become operational.

Y.1731 Limitations and Restrictions in CPT

- CPT supports only Ethernet Alarm Indication Signal (ETH-AIS), Ethernet Remote Defect Indication (ETH-RDI), and Ethernet Locked Signal (ETH-LCK) functionality for fault detection, verification, and isolation.
- ETH-LCK is supported on a channel group only at the MEP level and not at the interface level.
- CPT supports only two–way Ethernet frame Delay Measurement (ETH-DM) in Y.1731 performance monitoring.
- CPT does not support retransmission intervals of less than 100ms for delay measurement.
- Port MEP is not supported for both fault management and delay measurement.
- Y.1731 delay measurement is supported on UP MEP on xconnect configuration, and DOWN MEP on both xconnect and EVC configurations.
- All the members of the channel group must be present on the same card to support delay measurement. After the delay measurement session is configured on the channel group, the members cannot be moved to a different card. The delay measurement session on the channel group must be unconfigured before moving the members to a different card.
- Y.1731 is not supported for EVC encapsulation default and encapsulation untagged.

Understanding Y.1731 Fault Management

CPT supports Ethernet Alarm Indication Signal (ETH-AIS), Ethernet Remote Defect Indication (ETH-RDI), and Ethernet Locked Signal (ETH-LCK) functionality for fault detection and isolation.

ETH-AIS

The Ethernet Alarm Indication Signal function (ETH-AIS) is used to suppress alarms after defects are detected at an MEP. An MEP that receives a frame with ETH-AIS information suppresses alarms for all the peer MEPs, whether or not they are connected.

When an MEP detects a connectivity fault at a specific maintenance association level, it multicasts AIS frames in the direction away from the detected failure at the client maintenance association level. The frequency of AIS frame transmission is based on the AIS transmission period. The first AIS frame is always sent immediately following the detection of the defect condition.

When an MEP receives an AIS frame, it examines the AIS frame to ensure that the Maintenance Entity Group (MEG) level matches its own MEG and then detects the AIS default condition. After this detection, if AIS frames are not received for an interval of 3.5 times the AIS transmission period, the MEP clears the AIS defect condition. For example, if the AIS timer is set for 60 seconds, the AIS timer period expires after 3.5 times 60, or 210 seconds.

The AIS condition is terminated when a valid Continuity Check Message (CCM) is received with all the error conditions cleared or when the AIS period timer expires (the default time is 60 seconds).

ETH-RDI

When a downstream MEP detects a defect condition, such as receive signal failure or AIS , it sends Ethernet Remote Defect Indication (ETH–RDI) in the opposite upstream direction to its peer MEPs. RDI serves in informing the upstream MEPs that there has been a downstream failure and can be used as input to far-end performance monitoring.

When Ethernet OAM continuity check (ETH-CC) transmission is enabled, the Ethernet Remote Defect Indication (ETH-RDI) function uses a bit in the CFM CC message to communicate defect conditions to the MEP peers. For ETH-RDI functionality, you must configure the MEP MEG level, the ETH-CC transmission period, and the ETH-CC frame priority.

When an MEP receives frames with ETH-RDI information, it determines that its peer MEP has encountered a defect condition and sets the RDI files in the CCM frames for the duration of the defect condition. When the defect condition clears, the MEP clears the RDI field.

When an MEP receives a CCM frame, it examines the CCM frame to ensure that its MEG level is the same and if the RDI field is set, it detects an RDI condition. For point-to-point Ethernet connections, an MEP can clear the RDI condition when it receives the first frame from its peer MEP with the RDI field cleared. However, for multipoint Ethernet connectivity, the MEP cannot determine the associated subset of peer MEPs with which the sending MEP has seen the defect condition. It can clear the RDI condition after it receives CCM frames with the RDI field cleared from its entire list of peer MEPs.

ETH-LCK

The Ethernet Locked Signal (ETH-LCK) function communicates the administrative locking of an MEP and interruption of data traffic being forwarded to the MEP expecting the traffic. An MEP that receives frames with ETH-LCK information can differentiate between a defect condition and an administrative locking. ETH-LCK relies on loopback information (local, remote, port, and terminal loopback). The default timer for ETH-LCK is 60 seconds and the default level is the MIP level.

When an MEP is administratively locked, it sends LCK frames in a direction opposite to its peer MEPs, based on the LCK transmission period. The LCK transmission period is the same as the AIS transmission period. The first LCK frame is sent immediately following the administrative lock.

An MEP receiving a LCK frame verifies that the maintenance level matches its configured maintenance level and detects a LCK condition. When LCK frames are not received for an interval of 3.5 times the LCK transmission period, the MEP clears the LCK condition.

NTP-J116 Configure Y.1731 Fault Management Parameters

Purpose	This procedure configures Y.1731 fault management parameters.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J349 Configure ETH-AIS Parameters Using Cisco IOS Commands, on page 705

- DLP-J350 Clear AIS Alarms Using CTC, on page 707
- DLP-J351 Configure ETH-LCK Parameters Using Cisco IOS Commands, on page 708
- DLP-J352 Lock an MEP or an Interface Using CTC, on page 711
- DLP-J353 Enable Y.1731 Fault Management Parameters Using CTC, on page 713

Stop. You have completed this procedure.

DLP-J349 Configure ETH-AIS Parameters Using Cisco IOS Commands

Purpose	This procedure configures ETH-AIS using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	NTP-J106 Configure CFM Using Cisco IOS Commands, on page 659
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ethernet cfm ais link-status global** **Example:** Router(config)# ethernet cfm ais link-status global	Configures AIS specific commands for source MEP and enters config-ais-link-cfm mode.
Step 4	**level** *level-id* **Example:** Router(config-ais-link-cfm)# level 3	Configures the maintenance level to send AIS frames transmitted by the source MEP. The range is from 0 to 7.

	Command or Action	Purpose
Step 5	**period** *value* **Example:** Router(config-ais-link-cfm)# period 1	Configures the AIS transmission period interval for the source MEP. The allowable values are 1 second or 60 seconds.
Step 6	**exit** **Example:** Router(config-ais-link-cfm)# exit	Returns to global configuration mode.
Step 7	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** Router(config)# ethernet cfm domain customer level 7	Creates a CFM maintenance domain at a specific maintenance level and enters Ethernet CFM configuration mode. The range of the maintenance domain level is from 0 to 7.
Step 8	**service** {*ma-name* | **number** *ma-num*} {**evc** *evc-name* [**direction down**]} **Example:** Router(config-ecfm)# service Customer1 port	Creates a maintenance association within a maintenance domain and enters CFM service configuration mode.
Step 9	**ais period** *value* **Example:** Router(config-ecfm-srv)# ais period 1	Configures the specific AIS transmission period interval for the source MEP. The allowable values are 1 second or 60 seconds.
Step 10	**ais level** *level-id* **Example:** Router(config-ecfm-srv)# ais level 4	Configures the maintenance level to send AIS frames transmitted by the MEP. The range is from 0 to 7.
Step 11	**ais expiry-threshold** *value* **Example:** Router(config-ecfm-srv)# ais expiry-threshold 20	Sets the expiry threshold for the maintenance association. The range is from 2 to 255. The default value is 3.5.
Step 12	**ais suppress-alarms** **Example:** Router(config-ecfm-srv)# ais suppress-alarms	Suppresses the AIS alarm on the MEP.
Step 13	**exit** **Example:** Router(config-ecfm-srv)# exit	Returns to global configuration mode.

	Command or Action	Purpose
Step 14	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure and enters interface configuration mode.
Step 15	**ethernet cfm ais link-status** **Example:** Router(config-if)# ethernet cfm ais link-status	Enables or disables sending AIS frames from the source MEP on the interface.
Step 16	**ethernet cfm ais link-status period** *value* **Example:** Router(config-if)# ethernet cfm ais link-status period 60	Configures the ETH-AIS transmission period generated by the source MEP on the interface. The allowable values are 1 second or 60 seconds.
Step 17	**ethernet cfm ais link-status level** *level-id* **Example:** Router(config-if)# ethernet cfm ais link-status level 5	Configures the maintenance level for sending AIS frames transmitted by the source MEP on the interface. The range is from 0 to 7.
Step 18	**end** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 19	**show ethernet cfm smep** [**interface** *type number*] **Example:** Router# show ethernet cfm smep interface TenGigabitEthernet 4/1	Displays CFM information for the source MEP.
Step 20	**show ethernet cfm errors** **Example:** Router(config)# show ethernet cfm errors	Displays ETH-AIS frames that are received and other errors.
Step 21	Return to your originating procedure (NTP).	—

DLP-J350 Clear AIS Alarms Using CTC

Purpose	This procedure enables you to clear the AIS alarm on an MEP or an interface using CTC.

Tools/Equipment	None
Prerequisite Procedures	DLP-J353 Enable Y.1731 Fault Management Parameters Using CTC, on page 713
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to clear the AIS alarm on an MEP or an interface.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 In the left pane, click **Y1731**.

Step 5 Click the **Configuration > Execute Commands > Command Execution AIS** tab.

Step 6 Complete the following steps to clear the AIS alarm on an MEP.

a) Click the **MEP** option.
b) Enter the MEP ID in the MEP ID field.
c) Enter the maintenance domain name in the Domain Name field.
d) Enter the service ID in the Service ID field.
e) Click **Clear** to clear the AIS alarm on an MEP.

Step 7 Complete the following steps to clear the AIS alarm on an interface.

a) Click the **Interface** option.
b) From the Slot drop-down list, choose a slot.
c) From the Port drop-down list, choose a port to specify the interface on which to clear the AIS alarm.
d) Click **Clear** to clear the AIS alarm on an interface.

Step 8 Return to your originating procedure (NTP).

What to Do Next

- DLP-J352 Lock an MEP or an Interface Using CTC, on page 711

DLP-J351 Configure ETH-LCK Parameters Using Cisco IOS Commands

Purpose	This procedure configures ETH-LCK using Cisco IOS commands.
Tools/Equipment	None

Prerequisite Procedures	NTP-J106 Configure CFM Using Cisco IOS Commands, on page 659
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ethernet cfm lck link-status global** **Example:** Router(config)# ethernet cfm lck link-status global	Configures LCK specific commands for source MEP and enters config-lck-link-cfm mode.
Step 4	**level** *level-id* **Example:** Router(config-lck-link-cfm)# level 3	Configures the maintenance level to send ETH-LCK frames transmitted by the source MEP. The range is from 0 to 7.
Step 5	**period** *value* **Example:** Router(config-lck-link-cfm)# period 1	Configures the ETH-LCK transmission period interval for the source MEP. The allowable values are 1 second or 60 seconds.
Step 6	**exit** **Example:** Router(config-lck-link-cfm)# exit	Returns to global configuration mode.
Step 7	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** Router(config)# ethernet cfm domain customer level 7	Creates a CFM maintenance domain at a specific maintenance level and enters Ethernet CFM configuration mode. The range of the maintenance domain level is from 0 to 7.

	Command or Action	Purpose
Step 8	**service** {*ma-name* | **number** *ma-num*} {**evc** *evc-name* [**direction down**]} **Example:** Router(config-ecfm)# service Customer1 port	Creates a maintenance association within a maintenance domain and enters CFM service configuration mode.
Step 9	**lck level** *level-id* **Example:** Router(config-ecfm-srv)# lck level 3	Configures the maintenance level for sending ETH-LCK frames transmitted by the MEP. The range is from 0 to 7.
Step 10	**lck period** *value* **Example:** Router(config-ecfm-srv)# lck period 60	Configure the MEP ETH-LCK frame transmission period interval. The allowable values are 1 second or 60 seconds.
Step 11	**lck expiry-threshold** *value* **Example:** Router(config-ecfm-srv)# expiry-threshold 20	Sets the expiry threshold for the maintenance association. The range is from 2 to 255. The default value is 3.5.
Step 12	**exit** **Example:** Router(config-ecfm-srv)# exit	Returns to global configuration mode.
Step 13	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure and enters interface configuration mode.
Step 14	**ethernet cfm lck link-status** **Example:** Router(config-if)# ethernet cfm lck link-status	Enables or disables sending ETH-LCK frames from the source MEP on the interface.
Step 15	**ethernet cfm lck link-status period** *value* **Example:** Router(config-if)# ethernet cfm lck link-status period 60	Configures the ETH-LCK transmission period generated by the source MEP on the interface. The allowable values are 1 second or 60 seconds.
Step 16	**ethernet cfm lck link-status level** *level-id* **Example:** Router(config-if)# ethernet cfm lck link-status level 5	Configures the maintenance level for sending ETH-LCK frames transmitted by the source MEP on the interface. The range is from 0 to 7.

	Command or Action	Purpose
Step 17	**end** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 18	**ethernet cfm lck start mpid** *local-mpid* **domain** *domain-name* **evc** *evc name* [**drop l2-bpdu**] **Example:** Router# ethernet cfm lck start mpid test domain customer evc evc1	Places an MEP in ETH-LCK condition. To put a MEP out of ETH-LCK condition, enter the **ethernet cfm lck stop mpid** *local-mpid* **domain** *domain-name* **evc** *evc name* privileged EXEC command.
Step 19	**ethernet cfm lck start interface** *type number* **direction** {**up** | **down**} [**drop l2-bpdu**] **Example:** Router# ethernet cfm lck start interface TenGigabitEthernet 4/1 direction down	Places an interface in ETH-LCK condition. To put an interface out of ETH-LCK condition, enter the **ethernet cfm lck stop interface** *type number* **direction** {**up** | **down**} privileged EXEC command.
Step 20	**show ethernet cfm smep** [**interface** *type number*] **Example:** Router# show ethernet cfm smep interface TenGigabitEthernet 4/1	Displays CFM information for the source MEP.
Step 21	**show ethernet cfm errors** **Example:** Router(config)# show ethernet cfm errors	Displays ETH-LCK frames that are received.
Step 22	Return to your originating procedure (NTP).	—

DLP-J352 Lock an MEP or an Interface Using CTC

Purpose	This procedure enables you to start the ETH-LCK fault management function on an MEP or an interface using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J353 Enable Y.1731 Fault Management Parameters Using CTC, on page 713
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to start the ETH-LCK fault management function on an MEP or an interface.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 In the left pane, click **Y1731**.

Step 5 Click the **Configuration > Execute Commands > Command Execution LCK** tab.

Step 6 Complete the following steps to place an MEP in ETH-LCK condition.

a) Click the **MEP** option.
b) Enter the MEP ID in the MEP ID field.
c) Enter the maintenance domain name in the Domain Name field.
d) Enter the service ID in the Service ID field.
e) Check the **Drop L2 Bpdu** check box to specify that all the data frames, Layer 3 control traffic, and Layer 2 bridge protocol data units (BPDUs) be dropped except the CFM frames for that MEP.
f) Click **Start** to lock an MEP.
Click **Stop** to unlock an MEP.

Step 7 Complete the following steps to place an interface in ETH-LCK condition.

a) Click the **Interface** option.
b) From the Slot drop-down list, choose a slot.
c) From the Port drop-down list, choose a port to specify the interface to be put in ETH-LCK condition.
d) From the Direction drop-down list, choose **Down** or **Up** to specify the direction of the ETH-LCK operation.
e) Check the **Drop L2 Bpdu** check box to specify that all the data frames, Layer 3 control traffic, and Layer 2 BPDUs be dropped except the CFM frames for that interface.
f) Click **Start** to lock an interface.
Click **Stop** to unlock an interface.

Step 8 Return to your originating procedure (NTP).

What to Do Next

- DLP-J350 Clear AIS Alarms Using CTC, on page 707

DLP-J353 Enable Y.1731 Fault Management Parameters Using CTC

Purpose	Y.1731 fault management in CPT consists of ETH-LCK and ETH-AIS. This procedure enables ETH-LCK and ETH-AIS fault management functions using CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-J105 Configure CFM Using CTC, on page 660
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note ETH-AIS and ETH-LCK are enabled by default when CFM is enabled.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to enable ETH-LCK and ETH-AIS fault management functions.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 In the left pane, click **Y1731**.

Step 5 Click the **Configuration** tab.

Step 6 Complete the following steps to enable ETH-LCK and ETH-AIS configurations globally.

a) Click the **Global Configuration** tab.
b) In the LCK area, check the **LCK Config Enable** check box to enable ETH-LCK configuration globally.
c) Enter the maintenance level for sending ETH-LCK frames transmitted by the source MEP in the LCK Level field. The range is from 0 to 7.
d) From the LCK Period drop-down list, choose **One Second** or **One Minute** to configure the ETH-LCK frame transmission period generated by the source MEP.
e) Check the **Disable LCK Transmission** check box to disable generation of ETH-LCK frames.
f) In the AIS area, check the **AIS Config Enable** check box to enable ETH-AIS configuration globally.
g) Enter the maintenance level for sending ETH-AIS frames transmitted by the source MEP in the AIS Level field. The range is from 0 to 7.
h) From the AIS Period drop-down list, choose **One Second** or **One Minute** to configure the ETH-AIS transmission period generated by the source MEP.
i) Check the **Disable AIS Transmission** check box to disable generation of ETH-AIS frames.
j) Click **Apply**.

Step 7 Complete the following steps to enable ETH-LCK and ETH-AIS configurations on an interface.

a) Click the **Interface Configuration** tab.
b) In the Ethernet Interfaces area, expand the slot or Fan-Out-Group (FOG) to view the interfaces.
c) Check the **LCK LS Enable** check box to enable sending ETH-LCK frames from the source MEP on the interface.
d) Enter the maintenance level for sending ETH-LCK frames transmitted by the source MEP on the interface in the LCK LS Level field. The range is from 0 to 7.
e) From the LCK LS Period drop-down list, choose **One Second** or **One Minute** to configure the ETH-LCK transmission period generated by the source MEP on the interface.
f) Check the **AIS LS Enable** check box to enable sending ETH-AIS frames from the source MEP on the interface.
g) Enter the maintenance level for sending ETH-AIS frames transmitted by the source MEP on the interface in the AIS LS Level field.
h) From the AIS LS Period drop-down list, choose **One Second** or **One Minute** to configure the ETH-AIS transmission period generated by the source MEP on the interface.
i) Click **Apply**.

Step 8 Complete the following steps to enable ETH-LCK and ETH-AIS configurations at the MEP level.

a) Click the **MEP Configuration** tab.
The list of maintenance association profiles created in CFM appear in this tab.
b) Enter the LCK expiry threshold parameter value for the maintenance association in the LCK Ex Threshold field. The range is from 2 to 255. The default value is 3.5.
c) Enter the maintenance level for sending ETH-LCK frames transmitted by the local MEP in the LCK Level field. The range is from 0 to 7.
d) From the LCK Period drop-down list, choose **One Second** or **One Minute** to configure the ETH-LCK transmission period generated by the local MEP.
e) Enter the AIS expiry threshold parameter value for the maintenance association in the AIS Ex Threshold field. The range is from 2 to 255. The default value is 3.5.
f) Enter the maintenance level for sending ETH-AIS frames transmitted by the local MEP in the AIS Level field. The range is from 0 to 7.
g) From the AIS Period drop-down list, choose **One Second** or **One Minute** to configure the ETH-AIS transmission period generated by the local MEP.
h) Check the **AIS Suppress Alarms** check box to suppress the AIS alarm on the MEP.
i) Click **Apply**.

Step 9 Return to your originating procedure (NTP).

What to Do Next

- DLP-J352 Lock an MEP or an Interface Using CTC, on page 711
- DLP-J350 Clear AIS Alarms Using CTC, on page 707

Understanding Y.1731 Performance Monitoring

When service providers sell connectivity services to a subscriber, a Service Level Agreement (SLA) is reached between the buyer and seller of the service. The SLA defines the attributes offered by a provider and serves as a legal obligation on the service provider. As the level of performance required by subscribers increases,

service providers need to monitor the performance parameters being offered. To capture the needs of service providers, organizations have defined various standards such as IEEE 802.1ag and ITU-T Y.1731 that define the methods and frame formats used to measure performance parameters.

Y.1731 Performance Monitoring (PM) provides a standard ethernet PM function that includes measurement of ethernet frame delay, frame delay variation, frame loss, and frame throughput measurements specified by the ITU-T Y-1731 standard. To measure SLA parameters such as frame delay or frame delay variation, a small number of synthetic frames are transmitted along with the service to the MEP.

Note CPT supports only two–way Ethernet frame Delay Measurement (ETH-DM) in Y.1731 performance monitoring. The CPT system sends, receives, and processes PM frames in intervals of 100ms (10 frames per second) and 1 second.

The SLA delay measurement sessions are removed after the Stateful Switchover (SSO) of the fabric card. These sessions must be manually restarted after SSO.

Frame Delay and Frame Delay Variation

Ethernet frame Delay Measurement (ETH-DM) is used for on-demand Ethernet OAM to measure frame delay and frame delay variation. Ethernet frame delay and frame delay variation are measured by:

- Sending periodic frames with Ethernet Delay Measurement Message (ETH-DMM) information to the peer MEP.
- Receiving frames with Ethernet Delay Measurement Reply (ETH-DMR) information from the peer MEP.

During the interval, one or both MEPs in a maintenance association measures the frame delay and frame delay variation. Ethernet frame delay measurement also collects useful information, such as minimum and maximum delay over a fixed time, average delay, and average delay variation. Ethernet frame delay measurement supports hardware-based time stamping in the ingress direction. It provides a runtime display of delay statistics during a two-way delay measurement.

In two–way delay measurement, MEP transmits frames with ETH-DM request information to its peer MEP and receives frames with ETH-DM reply information from its peer MEP. Two–way frame delay and frame delay variation is measured using ETH-DMM and ETH-DMR frame combination.

NTP-J117 Configure and Schedule Two-Way Delay Measurement

Purpose	This procedure configures and schedules two-way delay measurement.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J354 Configure and Schedule Two-Way Delay Measurement Using Cisco IOS Commands, on page 716
- DLP-J355 Configure and Schedule Two-Way Delay Measurement Using CTC, on page 719
- DLP-J356 Display IP SLA Configuration and Statistics Using CTC, on page 721
- Troubleshooting an IP SLA Session, on page 722

Stop. You have completed this procedure.

DLP-J354 Configure and Schedule Two-Way Delay Measurement Using Cisco IOS Commands

Purpose	This procedure configures and schedules two-way delay measurement using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ip sla** *n* **Example:** Router(config)# ip sla 1	Enables the IP SLA configuration.

	Command or Action	Purpose
Step 4	**ethernet y1731 delay dmm domain** *domain-name* {**evc** *evc-name*} {**mpid** | **mac-address** *target-address*} **cos** *cos-value* {**source mpid** | **mac-address** *source-address*} **Example:** Router(config-ip-sla)# ethernet y1731 delay dmm domain r3 evc e3 mpid 500 cos 3 source mpid 400	Configures a two-way delay measurement on the sender. • **evc –** Specifies the Ethernet Virtual Circuit (EVC) identifier. • **cos –** Specifies the Class of Service (CoS). The values range from 0 to 7. • **mpid –** Specifies the destination MP ID. The values range from 1 to 8191. • **mac-address –** Specifies the destination MAC address. • **source –** Specifies the source MP ID or MAC address.
Step 5	**frame** {**interval** | **offset** | **size**} *bytes* **Example:** Router(config-sla-y1731-delay)# frame interval 100	Configures the following Y.1731 frame parameters: • **interval –** Specifies the retransmission period for DMM. The allowable values are 100 milliseconds or 1 second. • **offset –** Specifies the frame offset to be used for calculations. The values range from 1 to 10. • **size –** Specifies the frame size. The values range from 64 to 384.
Step 6	**history** {**interval**} *intervals-stored* **Example:** Router(config-sla-y1731-delay)# history interval 5	Configures the following Y.1731 history parameters: • **interval –** Specifies the number of historical aggregated interval statistics to be retained. The number of intervals range from 1 to 10.
Step 7	**aggregate** {**interval**} *seconds* **Example:** Router(config-sla-y1731-delay)# aggregate interval 5	Configures the following Y.1731 aggregation parameters: • **interval –** Specifies the duration for which individual delay measurements are aggregated into cumulative statistics. The aggregation period ranges from 1 to 65535 seconds.
Step 8	**distribution** {**delay** | **delay-variation**} **two-way** *number_of_bins comma_separated_values* **Example:** Router(config-sla-y1731-delay)# distribution delay 5 10,30,500,700,1000	Configures the following Y.1731 distribution parameters: • **delay –** Specifies the delay distribution parameters. • **delay-variation –** Specifies the delay variation distribution parameters.

	Command or Action	Purpose
Step 9	**max-delay** *milliseconds* **Example:** Router(config-sla-y1731-delay)# max-delay 1000	Configures maximum delay which is allowed as a valid delay measurement. The values range from 1 to 65535 milliseconds.
Step 10	**owner** *owner-id* **Example:** Router(config-sla-y1731-delay)#owner john	Specifies the operation owner.
Step 11	**exit** **Example:** Router(config-sla-y1731-delay)# exit	Exits the Y.1731 submode and enters the global configuration mode.
Step 12	**ip sla schedule** *n* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*month day* | *day month*] | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**] **Example:** Router(config)# ip sla schedule 10 start-time now life forever	Schedules the two-way delay measurement on the sender. • **life forever –** Schedules the operation to run indefinitely. • **start-time –** Specifies the time to start the entry. • **now –** Specifies that the operation must start immediately. • **after –** Specifies that the operation must start *hh* hours, *mm* minutes, and *ss* seconds after this command was entered. • **ageout –** Specifies the period to retain an inactive SLA instance. The range is from 0 to 2073600 seconds. • **recurring –** Specifies that the operation will start automatically at the specified time and for the specified duration every day. See the Troubleshooting an IP SLA Session, on page 722 section if the IP SLA delay measurement session does not start.
Step 13	**exit** **Example:** Router(config)# exit	Exits the global configuration mode.
Step 14	**show ip sla configuration** **Example:**	Displays the IP SLA configuration details.

	Command or Action	Purpose
	Router# show ip sla configuration	
Step 15	**show ip sla statistics** [**details**] **Example:** Router# show ip sla statistics	Displays the IP SLA statistics.
Step 16	Return to your originating procedure (NTP).	—

Example: Configure Two-Way Delay Measurement

The following example configures a two-way delay measurement using Cisco IOS commands:

```
Router# enable
Router# configure terminal
Router(config)# ip sla 1
Router(config-ip-sla)# ethernet y1731 delay DMM domain ifm_400 evc e1 mpid 401 cos 4 source
 mpid 1
Router(config-sla-y1731-delay)# frame interval 100
Router(config-sla-y1731-delay)# history interval 5
Router(config-sla-y1731-delay)# aggregate interval 60
Router(config-sla-y1731-delay)# exit
Router(config)# ip sla schedule 1 start-time now life forever
Router(config)# exit
```

DLP-J355 Configure and Schedule Two-Way Delay Measurement Using CTC

Purpose	This procedure configures and schedules two-way delay measurement using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to configure and schedule two-way delay measurement.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

Step 4 In the left pane, click **Y1731**.

Step 5 Click the **Delay Measurement > Configuration** tab.

Step 6 Click **Create**.

Step 7 In the Basic area of the Create DM Config dialog box, specify the following mandatory parameters:

a) Enter the SLA instance ID in the IP SLA ID field.
b) From the Domain drop-down list, choose a maintenance domain.
c) Enter the service ID in the Service ID field.
d) Enter the Class of Service (CoS) value in the CoS field. The values range from 0 to 7.
The user must reconfigure the IP SLA session if the QoS configurations relating to the CoS value change.
e) Specify the source MP ID or source MAC address in the Source MPID or Source MAC ID field. The values of source MP ID range from 1 to 8191.
f) Specify the destination MP ID or destination MAC address in the Destination MPID or Destination MAC ID field. The values of destination MP ID range from 1 to 8191.

Step 8 In the Advanced area of the Create DM Config dialog box, specify the following optional delay measurement parameters:

a) Enter the frame size in the Frame Size field. The values range from 64 to 384.
b) From the Frame Interval drop-down list, choose **100 msec** or **1 sec** for the retransmission period for DMM.
c) Enter the duration for which individual delay measurements are aggregated into cumulative statistics in the Aggregation Interval field. The values range from 1 to 65535 seconds.
d) Enter the number of historical aggregated interval statistics to be retained in the History Interval field. The values range from 1 to 10.
e) Enter the maximum delay in the Maximum Delay field. The values range from 1 to 65535 milliseconds.
f) Enter the delay distribution parameters in the Delay Distribution field.
g) Enter the delay variation distribution parameters in the Delay Variation List field.
h) Enter the IP SLA operation owner name in the Owner Name field.
i) From the Reaction Type drop-down list, choose **Immediate**.
When the measured delay exceeds or meets the threshold, an alarm is raised or cleared.
j) Enter the low threshold value in the Falling Threshold field.
The falling threshold is the value below which the alarm is cleared.
k) Enter the high threshold value in the Rising Threshold field.
The rising threshold is the value above which the alarm is raised.

Step 9 Click **OK** in the Create DM Config dialog box to configure a two-way delay measurement.

Step 10 Complete the following steps to schedule a two-way delay measurement.

a) Click the **Schedule** tab.
b) Enter the SLA instance ID in the IP SLA ID field.

c) Enter the period to retain an inactive SLA instance in the Age-out field.
d) Click the **Forever** option to schedule the operation to run indefinitely or enter the time interval for the operation to run in the Secs field.
e) Check the **Recurring** check box to specify that the operation will start automatically at the specified time and for the specified duration every day.
f) From the Start time drop-down list, choose **After** or **Now** to specify the time to start the IP SLA operation.

- **After—**Specifies that the operation must start hh hours, mm minutes, and ss seconds after this command was entered.
- **Now—**Specifies that the operation must start immediately.

g) From the Time drop-down list, choose hour, minute, and second.
h) Click **Schedule** to schedule a two-way delay measurement.

See the Troubleshooting an IP SLA Session, on page 722 section if the IP SLA delay measurement session does not start.

Step 11 Complete the following steps to start the IP SLA operation immediately.
a) Enter the SLA instance ID in the IP SLA ID field.
b) Click **Start now** to start the IP SLA operation immediately.

Step 12 (Optional) Complete the following steps to delete the IP SLA instance(s).
a) Enter the SLA instance ID in the IP SLA ID field and click **Delete** to delete the specific IP SLA instance.
b) Click **Delete All** to delete all the current IP SLA statistics and configuration information from the router and to reset the IP SLA engine.

Step 13 (Optional) Check the **Enable IP SLA Trap** check box to enable IP SLA traps.
The traps need to be enabled only if SLA alarm needs to be configured.

Step 14 Click **Apply**.

Step 15 Return to your originating procedure (NTP).

DLP-J356 Display IP SLA Configuration and Statistics Using CTC

Purpose	This procedure enables you to display configuration values and statistics of IP SLA operations using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J355 Configure and Schedule Two-Way Delay Measurement Using CTC, on page 719
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to display configuration values and statistics of IP SLA operations.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Maintenance** tab.

Step 4 In the left pane, click **OAM**.

Step 5 From the Command drop-down list, choose **Show IP-SLA**.

Step 6 Enter the IP SLA instance in the IP SLA ID field. The range is from 1 to 2147483647.

Step 7 Complete the following steps to display the statistics of IP SLA operations.

a) Click the **Statistics** option.

b) Check the **Aggregated** check box to display the aggregated statistical errors and distribution information for IP SLA operations.

c) Check the **Details** check box to display the current operational status and statistics of all IP SLAs operations.

Step 8 Click the **Configuration** option to display the configuration values including all defaults for the IP SLA operations.

Step 9 Click the **Interval Statistics** option to display the interval statistics of IP SLA operations.

Step 10 Click **Execute**.

Step 11 Return to your originating procedure (NTP).

Troubleshooting an IP SLA Session

The IP SLA sessions must have a delayed start of at least 10 minutes to allow adequate time for sessions to restart on node power cycle.

To start IP SLA automatically, check the following:

- IP SLA aggregate interval should be above 300 seconds.
- IP SLA start time should be equal to the time taken by all the cards of the node, to come up after node reload.

If an IP SLA delay measurement session does not start, check the following:

- There are no CFM errors such as AIS and RDI on the source MEP or local MEP.
- The remote MEP is visible locally.
- If the local MEP is on a channel group, all its members are present on the same card.
- MEPs between which the SLA session is configured do not have another SLA session for the same pair of MEP.

The following table describes the commands that can used to troubleshoot issues for an IP SLA delay measurement session.

Command	Purpose
show ethernet cfm pm	Displays mapping of SLA ID to delay measurement session ID. If there is no output from this command, it indicates that the session was not created or the ETH-DMR was not received.
show ethernet cfm pm session *dm_session_id*	Displays the database of delay measurement.
clear ethernet cfm pm session *dm_session_id*	Clears the database of delay measurement.
• **debug ethernet cfm pm diagnostics** • **debug ethernet cfm pm events** • **debug ethernet cfm pm errors** • **debug ethernet cfm pm packets** • **debug ethernet cfm pm monitor**	Enables delay measurement engine logs. The **debug ethernet cfm pm monitor** command is applicable only on the fabric card.

Show Commands

This section describes several show commands that can be used with IP SLA.

Display IP SLA Configuration

This command displays the configuration values including all defaults for all IP SLA operations or a specified operation.

```
Router# show ip sla configuration [operation-number]
```

```
IP SLAs Infrastructure Engine-III
Entry number: 1
Owner:
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: DMM
Domain: Level1
Evc: PWEVC
Target Mpid: 10
Source Mpid: 11
CoS: 7
   Max Delay: 5000
   Request size (Padding portion): 64
   Frame Interval: 1000
   Clock: Not In Sync
Threshold (milliseconds): 5000
Schedule:
   Operation frequency (seconds): 900  (not considered if randomly
```

```
scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Statistics Parameters
  Aggregation Period: 900
  Frame offset: 1
  Distribution Delay Two-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1

  Distribution Delay-Variation Two-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
History
  Number of intervals: 2
```

Display IP SLA Statistics

This command displays the current operational status and statistics of all IP SLAs operations or a specified operation.

```
Router# show ip sla statistics [operation-number] [details]
```

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
Delay Statistics for Y1731 Operation 1
Type of operation: Y1731 Delay Measurement
Latest operation start time: 05:50:54.467 PDT Sat Jul 8 2000
Latest operation return code: OK
Distribution Statistics:

Interval
 Start time:  05:50:54.467 PDT Sat Jul 8 2000
 Elapsed time: 610 seconds
 Number of measurements initiated: 608
 Number of measurements completed: 608
 Flag: OK
```

Display IP SLA Aggregated Statistics

This command displays the aggregated statistical errors and distribution information for all IP SLAs operations or a specified operation.

```
Router# show ip sla statistics aggregated [operation-number] [details]
```

```
IPSLAs aggregated statistics

IPSLA operation id: 1
Delay Statistics for Y1731 Operation 1
Type of operation: Y1731 Delay Measurement
```

```
Latest operation start time: 05:50:54.467 PDT Sat Jul 8 2000
Latest operation return code: OK
Distribution Statistics:


Interval
 Start time:  05:50:54.467 PDT Sat Jul 8 2000
 Elapsed time: 787 seconds
 Number of measurements initiated: 777
 Number of measurements completed: 777
 Flag: OK

Delay:
  Number of TwoWay observations: 773
    Min/Avg/Max TwoWay: 58/66/98 (microsec)
  Time of occurrence TwoWay:
    Min - 06:03:39.978 PDT Sat Jul 8 2000
    Max - 06:02:54.975 PDT Sat Jul 8 2000

Delay Variance:
  Number of TwoWay positive observations: 367
    Min/Avg/Max TwoWay positive: 0/3/38 (microsec)
  Time of occurrence TwoWay positive:
    Min - 06:02:04.967 PDT Sat Jul 8 2000
    Max - 06:02:54.975 PDT Sat Jul 8 2000
  Number of TwoWay negative observations: 405
    Min/Avg/Max TwoWay negative: 0/3/34 (microsec)
  Time of occurrence TwoWay negative:
    Min - 05:59:19.937 PDT Sat Jul 8 2000
    Max - 05:53:49.821 PDT Sat Jul 8 2000
```

Display IP SLA Global Information

This command displays global information about IP SLAs.

```
Router# show ip sla application
```

```
IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, 802.1agEcho VLAN, EVC, Port
        802.1agJitter VLAN, EVC, Port, y1731Delay, y1731Loss, udpApp
        wspApp

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 260261241
Estimated system max number of entries: 190621

Estimated number of configurable operations: 190620
Number of Entries configured  : 1
Number of active Entries      : 1
Number of pending Entries     : 0
```

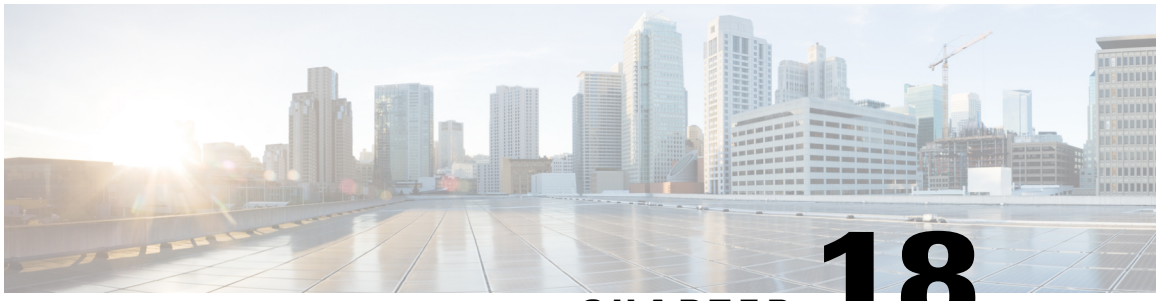
```
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: 09:23:56.488 PDT Sun Jul 2 2000
```

Display IP SLA Threshold Settings

This command displays the configured proactive threshold monitoring settings for all IP SLA operations or a specified operation.

```
Router# show ip sla reaction-configuration [operation-number]
```

```
Entry number: 1
Index: 1
Reaction: rtt
Threshold Type: Immediate
Rising (milliseconds): 10
Falling (milliseconds): 10
Action Type: None
```



CHAPTER 18

Configuring Synchronous Ethernet

This chapter describes the Synchronous Ethernet features, standards, and limitations in CPT. This chapter also describes procedures to configure Synchronous Ethernet.

This chapter includes the following topics:

Synchronous Ethernet Overview

A separate external time-division multiplexing (TDM) circuit is required to provide synchronized timing to multiple remote network elements (NEs) for packet transport networks like Cisco Carrier Packet Transport

system. The Synchronous Ethernet (SycnE) feature addresses this requirement by providing effective timing to the remote NEs through a packet network without using an external circuit for timing.

With Ethernet equipment gradually replacing existing Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) equipment in service-provider networks, frequency synchronization is required to provide high-quality clock synchronization over Ethernet ports. The SyncE feature provides the required synchronization at the physical level. Operation messages maintain SyncE links and ensure that a node always derives timing from the most reliable source. SyncE uses the Ethernet Synchronization Message Channel (ESMC) to enable traceability of the best clock source to correctly define the timing source and prevent a timing loop.

Understanding SyncE

SyncE provides the Ethernet physical layer network (ETY) level frequency distribution of known common precision frequency references. Clocks for use in SyncE are compatible with the clocks used in the SONET/SDH synchronization network. To achieve network synchronization, synchronization information is transmitted through the network via synchronous network connections with performance of egress clock. In SONET/SDH the communication channel for conveying clock information is SSM, and in SyncE it is the ESMC.

SyncE is a standard for distribution of frequency over Ethernet links. Other standards (IEEE Std. 1588 Precision Time Protocol [PTP], IETF Network Time Protocol [NTP], etc.) have been and are being developed or enhanced for high-quality time distribution and Adaptive Clock Recovery (ACR) requirements.

To maintain the timing chain in SONET/SDH, operators often use SSM. Information provided by SSM Quality Levels (SSM-QL) helps a node derive timing from the most reliable source and prevent timing loops. The SONET/SDH header has a QL information present in the S1 bytes of its header. Hence, the SONET/SDH does not require any specific channel for QL information exchange. As the Ethernet does not have the QL information in its header, it requires ESMC for QL information. Because Ethernet networks are not required to be synchronous on all links or in all locations, a specific channel, the ESMC channel defined in G.8264, provides this service. ESMC is composed of the standard Ethernet header for an organization-specific slow protocol, the ITU-T OUI; a specific ITU-T subtype; an ESMC-specific header; a flag field; and a type, length, value (TLV) structure: the use of flags and TLVs aimed at improving the management of Synchronous Ethernet links and the associated timing change.

SyncE Standards

- ITU-T G.8261: Timing and synchronization aspects in packet network
- ITU-T G.8262: Timing characteristics of Synchronous Ethernet equipment slave clock
- ITU-T G.8264: Distribution of timing through packet networks
- ITU-T G.781: Synchronization layer functions

These standards specify the jitter and wander tolerances, supported frequencies, clock specifications (Synchronous Ethernet Equipment Clocks [EECs] are defined to ensure compatibility with SONET/SDH clocks detailed in ITU-T G.813 and G.812 or Telcordia GR-1244-CORE), clock selection logic, possible clock quality levels, error responses, noise tolerances, noise generation and transfer limits, holdover performance, deployment scenarios, interworking requirements, clock selection process, SSM support, and a new ESMC (which allows interworking with existing SONET/SDH infrastructure by allowing the SyncE links to convey the SSM quality level as defined in ITU-T G.707, G.781, Telcordia GR-253-CORE, and ANSI T1.101).

SyncE Support in CPT

The clock selection algorithm of SyncE runs on the controller card of the Cisco CPT. The controller card has a Digital Phase Lock Loop (DPLL) that validates the clock for OOB (Out of Bound) frequency and then based on the clock stability and Quality Level (QL) selects the appropriate clock. All the clocks selected as reference are sent to the controller card for validation and selection. However, if an appropriate clock is not found, the controller card that has an ST3 internal clock is used as a FreeRunning clock to drive the system.

CPT supports a maximum of three clock references (per node) to be configured including BITS, 10G ports on the fabric or line card, and 1G CPT-50 ports. The clock source can be configured on any of the10G ports of the fabric, line card, and 1G ports in CPT-50. The fabric XFP port in OTN mode can also be configured as the clock source and does not require Ethernet Synchronization Message Channel (ESMC) because it derives the QL information from the OTN OTU2E RES header. The XFP ports in OTN mode transmits the SSM-QL information in OTN OTU2E RES header.

ESMC can be enabled on any port. Administrative configuration of QL is used to support non-ESMC legacy clock sources (ITUT G.8264 /10.2) or to override a QL. CPT needs a clock to be stable for 140 seconds to use it as HoldOver.

SyncE can be used with TNC, TSC, TNC-E, and TSC-E as a controller card in CPT.

SyncE Limitations in CPT

- SyncE is supported for all pluggables except copper GE SFPs.
- Clock source per slot supported is only one.
- Clock that is persistent for less than 140 seconds then the clock cannot go to the holdover state.
- Controller card handles up to three clock sources and selects the best of the three clock sources.
- Clock sources that are configured and the ports configured with "ESMC Enabled" must be disabled when changing the clock mode.
- SyncE phase transients fail mask during hardware reset of the TNC-E card.
- Generation 1 to Generation 2 or SDH mode to SONET mode (or vice-versa) migration requires all the clock sources and ESMC enabled ports to be deselected and the generation/clock mode, changed.

Synchronization Status Message in Ethernet

Network clocking uses the Synchronization Status Messages (SSM) mechanism to exchange the Quality Level (QL) of the clock between the network elements. In Ethernet, Ethernet Synchronization Message Channel (ESMC) is used for SSM exchange.

Synchronization Status Message

Network elements use SSM to inform the neighboring elements about the QL of the clock. The non-ethernet interfaces, such as optical interfaces and T1 or E1 SPA frames, use SSM. The key benefits of the SSMs are:

- Prevents timing loops.

- Provides fast recovery when a part of the network fails.
- Ensures that a node get timing from the most reliable clock source.

SSM is either Generation 1 or Generation 2. Generation 1 is the first and most widely deployed SSM message set. Generation 2 is a newer version.

The following table shows the SDH message set.

Table 36: SDH SSM Message Set

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

The following table shows the Generation 1 message sets for SONET.

Table 37: SONET SSM Generation 1 Message Set

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

The following table shows the Generation 2 message sets for SONET.

Table 38: SONET SSM Generation 2 Message Set

Message	Quality	Description
PRS	1	Primary reference source-Stratum 1
STU	2	Sync traceability unknown

Message	Quality	Description
ST2	3	Stratum 2
TNC	4	Transit node clock
ST3E	5	Stratum 3E
ST3	6	Stratum 3
SMC	7	SONET minimum clock
ST4	8	Stratum 4
DUS	9	Do not use for timing synchronization
RES	—	Reserved; quality level set by user

Ethernet Synchronization Messaging Channel

In order to maintain a logical communication channel in synchronous network connections, Ethernet relies on a channel called the Ethernet Synchronization Messaging Channel (ESMC), which is based on the IEEE 802.3 Organization-Specific Slow Protocol (OSSP) standards. ESMC relays the SSM code that represents the quality level of the Ethernet Equipment Clock (EEC) in a physical layer.

ESMC carries a QL identifier that identifies the timing quality of the synchronization trail. QL values in QL-TLV are the same as QL values defined for SONET and SDH SSM. Information provided by SSM QLs during the network transmission helps a node derive timing from the most reliable source and prevents timing loops. ESMC is used with the synchronization selection algorithms. Because Ethernet networks are not required to be synchronous on all links or in all locations, the ESMC channel provides this service. ESMC is comprises of the standard Ethernet header for an organization-specific slow protocol; the ITU-T OUI, a specific ITU-T subtype; an ESMC-specific header; a flag field; and a type, length, value (TLV) structure. The use of flags and TLVs improves the management of SyncE links and the associated timing change.

The ESMC packets are received only for the ports configured as clock sources, and transmitted on all the SyncE interfaces in the system. These packets are then processed by the clock selection algorithm on route processors (RP) and are used to select the best clock. The Tx frame is generated based on the QL value of the selected clock source, and sent to all the enabled SyncE ports.

DLP-J326 Set Up Timing Parameters Using CTC

Purpose	This procedure sets up timing parameters using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to set up timing parameters.

Step 2 Go to the Node View.

Step 3 Click the **Provisioning** > **Timing** > **General** tabs.

Step 4 In Timing Standard area, Click **Change** button to change the Current Timing Standard.
The "Change Timing Standard" dialog box appears.

Step 5 Select the **SONET** or **SDH** radio button as required. Click **OK**.

Step 6 In the General Timing section, complete the following information:

- Timing Mode—Choose External if the CPT derives its timing from a BITS source; choose Line if timing is derived from the line card that is connected to the timing node. A third option, Mixed, allows you to set both external and line timing references.

  Note Because Mixed timing might cause timing loops, we do not recommend its use. Use this mode with care.

- SSM Message Set—Choose either Generation 1 or Generation 2 synchronization status messaging (SSM) option if the Timing Standard selected is SONET.
- Quality of RES—Sets the timing quality for the user-defined, reserved (RES) QL value if your timing sources supports RES. Most timing sources do not use RES. If it does not support RES, choose RES=DUS (do not use for timing reference). Qualities are displayed in the descending quality order as ranges. For example, in Generation 1 SSM, ST3<RES<ST2 means that the timing reference RES is higher than a Stratum 3 (ST3) and lower than a Stratum 2 (ST2). If the Timing Standard selected is SDH, RES is not supported.
- Revertive—Check this check box if you want the CPT to revert to a primary reference source after the conditions that caused it to switch to a secondary timing reference are corrected.
- Reversion Time—Check this check box and choose the amount of time that the CPT system should wait before reverting to its primary timing source. The default value is 5 minutes.

Step 7 Click **Apply**.

Step 8 Click the **BITS Facilities** tab.

Note The BITS Facilities section sets the parameters for your BITS-1 and BITS-2 timing references. Many of these settings are determined by the timing source manufacturer. If equipment is timed through BITS Out, you can set timing parameters to meet the requirements of the equipment.

Step 9 In the BITS In area, complete the following information:

- Facility Type—(TNC/TSC/TNC-E/TSC-E only) Choose the BITS signal type supported by your BITS clock, either DS1 or 64Khz+8Khz.
- BITS In State—Set the BITS In state for BITS-1, BITS-2, or both, to IS (in service) if Timing Mode is set to External or Mixed, depending on whether one or both BITS input pin pairs are connected to the external timing source. If Timing Mode is set to Line, set the BITS In state to OOS (out of service).

Step 10 If the BITS In state is set to OOS, continue with Step 12. If the BITS In state is set to IS, complete the following information:

- Coding—Choose the coding used by your BITS reference, either B8ZS (binary 8-zero substitution) or AMI (alternate mark inversion).
- Framing—Choose the framing used by your BITS reference, either ESF (Extended Super Frame) or SF (D4) (Super Frame).
- Sync Messaging—Check this check box to enable SSM. SSM is not available if framing is set to Super Frame.
- Admin SSM—Choose the SSM Generation 2 type fromt the drop-down list if the SyncE Messaging check box is unchecked. Available options are PRS (Primary reference source; Stratum 1), ST2 (Stratum 2), TNC (Transit Node Clock), ST3E (Stratum 3E), ST3 (Stratum 3), SMC (SONET minimum clock), and ST4 (Stratum 4).

Step 11 In the BITS Out area, complete the following information, as needed:

- Facility Type—(TNC/TSC only) Choose the BITS Out signal type, either DS1 or 64Khz+8Khz.
- BITS Out state—Set the BITS Out state for BITS-1, BITS-2, or both to IS ((depending on which BITS Out pins are used for the external equipment): if the equipment is connected to the BITS output pins of the node on the backplane (ANSI) or MIC-C/T/P FMEC (ETSI); and to time the equipment from a node reference. If equipment is not attached to the BITS output pins, set the BITS Out state to OOS.

Step 12 If the BITS Out state is set to OOS, continue with Step 12. If the BITS Out state is set to IS, complete the following information:

- Coding—Choose the coding used by your BITS reference, either B8ZS or AMI.
- Framing—Choose the framing used by your BITS reference, either ESF or SF (D4).
- AIS Threshold—Choose the quality level where a node sends an alarm indication signal (AIS) from the BITS 1 Out and BITS 2 Out backplane pins (ANSI) or MIC-C/T/P FMEC (ETSI), if SSM is disabled or Super Frame is used. An AIS alarm is raised when the optical source for the BITS reference falls to or below the SSM quality level defined in this field.
- LBO—Set the line build-out (LBO) distance between the ONS 15454 and an external device, if an external device is connected to the BITS Out pins. If an external device is connected to BITS Out, choose the distance between the device and the CPT system. Options are: 0-133 ft (default), 134-266 ft, 267-399 ft, 400-533 ft, and 534-655 ft. LBO relates to the BITS cable length. If an external device is not connected to BITS Out, leave this field set to the default.

Step 13 Click **Apply**.

Step 14 Return to your originating procedure (NTP).

DLP-J330 Enable or Disable ESMC Using CTC

Purpose	This procedure enables or disables ESMC using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to enable or disable ESMC.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**.

Step 3 The Packet Transport System View window appears. Click the **Provisioning** > **Timing** tabs.
In the Timing Configurations area, expand the appropriate slot and check the **ESMC Enable** check box on the port where you want to enable SyncE.

Note For Ring port, SyncE is enabled by default.

You can select the clock source among the ESMC enabled ports. To select the clock source among the OTN ports, do not check the **ESMC Enable** check box.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-J328 Configure SyncE Port Using CTC

Purpose	This procedure configures SyncE port using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to configure the SyncE port.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**.

Step 3 The Packet Transport System View window appears. Choose the SyncE port parameters as shown in the following table.

Table 39: SyncE Port Configuration Parameters

Parameter	Description	Options
Port	(Display only) Displays the port number (n-n) and rate.	—
ProvidesSync	(Display only) Selects port automatically after the port is used as a clock source.	—
SyncMsgIn	Sets the EnableSync card parameter. Enables synchronization status messages, which allow the node to choose the best timing source.	Checked or unchecked
Admin SSM In	Overrides the synchronization status message (SSM) and the synchronization traceability unknown (STU) value. If the node does not receive an SSM signal, it defaults to STU.	• PRS-Primary Reference Source (Stratum 1) • ST2-Stratum 2 • TNC-Transit node clock • ST3E-Stratum 3E • ST3-Stratum 3 • SMC-SONET minimum clock • ST4-Stratum 4 • DUS-Do not use for timing synchronization • RES-Reserved; quality level set by user
Send DoNotUse	Sends a DUS message as the QL value, when checked.	Checked or unchecked

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

Clock Selection Algorithm

The clock selection algorithm selects the best available synchronization source from the nominated sources. This algorithm exhibits nonrevertive behavior among the clock sources with the same QL value, and always

selects the signal with the best QL value. For clock option SDH, the default is revertive, and for clock option SONET, the default is nonrevertive.

Clock Source Selection

The CPT supports the following clock source references:

Internal Clock Source

The controller card has it own internal clock ST3 in SONET mode, and SEC in SDH mode. This clock is used during the freerunning mode. By default, the internal clock is selected as the clock reference.

External Clock Source

BITS-IN1 and BITS-IN2 can be configured as the external clock reference and the QL can be configured as the BITS-IN clock.

Line Card Clock Source

One SyncE clock source per line card is supported. In Cisco CPT-600, a maximum of six clock sources are available for selection excluding the BITS; In Cisco CPT-200, a maximum of two clock sources are available for selection excluding BITS.

Note The CPT supports a maximum of three clock references.

For example, more than one clock source per line card (inclusive of all the Cisco CPT-50 fanout ports) cannot be selected. If a Cisco CPT-50 1G port is selected as a clock source, no other clock source from any other Cisco CPT-50 fanout from that slot (where the former CPT-50 was fanned out) nor can any port from the line card can be selected.

Clock Source Protection in Cisco CPT-50

The Cisco CPT-50 can have one of the 44 GE ports to act as a clock source. When 1G port is selected as a clock source, the clock is preserved when bundled interlinks are added. The clock protection is also maintained on the bundled interlinks. When one of the interlinks fail, the clock momentarily moves to holdover or freerunning state, but will restore using the other interlinks.

Clock Mode

- Holdover Mode—In this mode, all external or line timing references are lost and the clock uses timing data referenced while in normal operating mode to control its output signal. However, holdover frequency drifts over time until a timing reference becomes available. If the previous timing reference was available for less than 140 seconds before it was lost, TCC enters the Free-running mode when the timing reference is lost. This mode is better than the Free-running mode because it uses the average of 140 seconds of data from the last qualified timing reference to augment its internal clock. TCC remains in this mode until a reference becomes available to switch, or the drift is out of bounds. Traffic is guaranteed to be uninterrupted by a transition to the Holdover mode for the first 24 hours.

- Free-running Mode—This mode mode only references the internal clock on the TCC card. It is also the default mode when other references are lost, even when it is not specifically provisioned as a reference. Ensure that your network does not operate with the internal clock of the TCC card as the only or primary timing source.

Timing Modes

- External—Only external clock can be used as a source. The external clock source can be configured as Internal, BITS-IN1, and BITS-IN2.
- Line—Internal controller card clock (ST3 in SONET, and SEC in SDH) or line card ports (10G ports in fabric or line card and 1G ports in CPT-50) can be selected as clock source.
- Mixed—Both External and Line clock sources can be configured.

DLP-J327 Select Timing Reference Using CTC

Purpose	This procedure selects the timing reference using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to select the timing reference.

Step 2 Go to the Node View.

Step 3 Click the **Provisioning** > **Timing** > **General** tabs.

Step 4 In the Reference Lists area, complete the following information:

- NE Reference—Defines three timing references (Ref 1, Ref 2, Ref 3). The node uses Reference 1 unless a failure occurs to that reference, in which case the node uses Reference 2. If Reference 2 fails, the node uses Reference 3, which is typically set to Internal Clock. Internal Clock is the Stratum 3 clock provided on the TNC/TSC/TNC-E/TSC-E card.
  - If the Timing Mode is set to External, the options are BITS-1, BITS-2, and Internal Clock.
  - If the Timing Mode is set to Line, the options are the 10G PTM, 10G PTF, and 1G, or both Cisco CPT-50 ports that are ESMC enabled. In addition, the internal clock can also be selected.

- If the Timing Mode is set to Mixed, both BITS references and the 10G PTM, 10G PTF, or 1G, Cisco CPT-50 ports are available, allowing to set a mixture of external BITS clocks and 10G PTM, 10G PTF, and 1G, or both Cisco CPT-50 ports as timing references.

- BITS-1 Out/BITS-2 Out—Sets the timing references for equipment wired to the BITS Out. BITS-1 Out and BITS-2 Out are enabled when BITS-1 Out and BITS-2 Out facilities are put in service. If Timing Mode is set to external, choose the 10G PTM, 10G PTF, and 1G, or both Cisco CPT-50 ports used to set the timing. If Timing Mode is set to Line, choose an 10G PTM, 10G PTF, or 1G Cisco CPT-50 ports or choose NE Reference to have the BITS-1 Out, BITS-2 Out, or both, follow the same timing references as the network element (NE).

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

Revertive and Non-revertive Clock Switching

The switching of timing references can be made revertive or non-revertive. In non-revertive switching, a switch to an alternate reference is maintained even after the original reference has recovered from the failure that caused the switch. However, that the node should switch back to the original reference (rather than enter the Holdover) if the original reference has recovered from its failure and the alternate reference subsequently fails. The clock enters Holdover only when all references fail, regardless of the revertive setting. In revertive switching, the clock switches back to the original reference after that reference recovers from the failure, independent of the condition of the alternate reference. In CPT, support for revertive and non-revertive clock source is on a slot basis as CPT does not support more than one clock source per line card slot.

If the primary external source fails, the clock card enters holdover mode. After a few seconds, it switches over to the secondary external source. The clock card switches back to the primary external source only when it becomes available.

DLP-J329 View Timing Status Report Using CTC

Purpose	This procedure views the timing status report using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

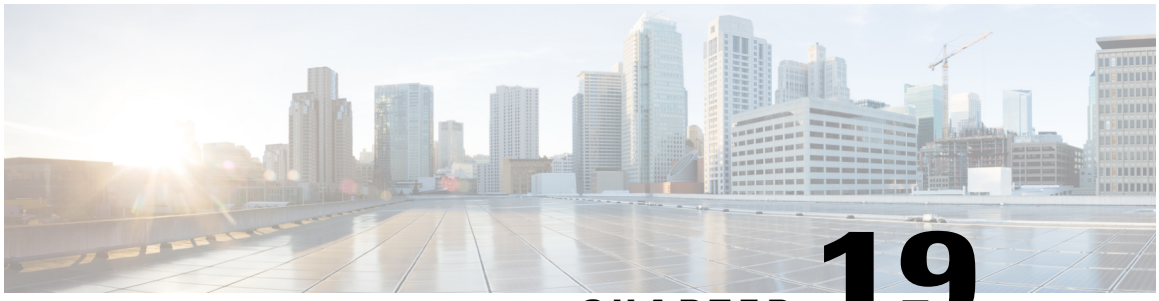
Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to view the timing status report.

Step 2 Go to the Node View.

Step 3 Click the **Maintenance** > **Timing** > **Report** tabs.
The report shows current timing information of the CPT system, including the timing mode, clock state and status, switch type, and reference data.

Step 4 Return to your originating procedure (NTP).



CHAPTER 19

Configuring Performance Monitoring, RMON, OTN, and Port Provisioning

This chapter describes performance monitoring, RMON, and OTN, port provisioning and the configuration procedures.

Understanding Performance Monitoring

Performance monitoring (PM) parameters are used by service providers to gather, store, set thresholds, and report performance data for early detection of problems. In this chapter, PM parameters and concepts are defined for the fabric card, line card, and CPT 50 panel.

Note For additional information regarding PM parameters, see the ITU G.826, ITU-T G.8021, ITU G.709, Telcordia documents GR-1230-CORE, GR-820-CORE, GR-499-CORE, and GR-253-CORE, and the ANSI T1.231 document entitled *Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*.

Note In CPT IOS, performance monitoring statistics are provided only for 15 minute and 1 day intervals. Historical counts are not maintained in CPT IOS.

Understanding Threshold Performance Monitoring

Thresholds are used to set error levels for each PM parameter. You can set individual PM threshold values from the card view in the Provisioning tab in CTC.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 15-minute interval, a threshold crossing alert (TCA) is raised. The number represents the counter value for each specific PM parameter.

TCAs provide early detection of performance degradation. When a threshold is crossed, the node continues to count the errors during a given accumulation period. If zero is entered as the threshold value, generation of TCAs is disabled but performance monitoring continues.

Change the threshold value if the default value does not meet your error monitoring needs. For example, customers with a critical OC192/STM64 transponder installed for 911 calls must guarantee the best quality of service on the line; therefore, they lower all thresholds on the client side so that the slightest error raises a TCA.

Performance Monitoring, RMON, OTN, and Port Provisioning Procedures

The following procedures can be performed using Cisco IOS commands to configure performance monitoring, RMON, OTN, and port provisioning:

- DLP-J72 Display Performance Monitoring Parameters Using Cisco IOS Commands, on page 752
- DLP-J74 Configure RMON Settings Using Cisco IOS Commands, on page 759
- Display RMON Status Using Cisco IOS Commands, on page 761

The following procedures can be performed using CTC to configure performance monitoring, RMON, OTN, and port provisioning:

- NTP-J23 Change the PM Display Using CTC, on page 743
- NTP-J24 Monitor Performance Using CTC, on page 751
- DLP-J73 Change the RMON Thresholds Using CTC, on page 761
- DLP-J75 Change the Optical Transport Network Settings Using CTC, on page 765
- DLP-J77 Provision Alarm and TCA Thresholds Using CTC, on page 773
- DLP-J78 Change the Port and Ethernet Settings Using CTC, on page 774

NTP-J23 Change the PM Display Using CTC

Purpose	This procedure enables you to change the appearance of PM counts using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to change the appearance of PM counts.

Step 2 As needed, use the following procedures to change the display of PM counts:

- DLP-J61 Refresh PM Counts at 15–Minute Intervals Using CTC, on page 743
- DLP-J62 Refresh PM Counts at One–Day Intervals Using CTC, on page 744
- DLP-J63 View Near–End PM Counts Using CTC, on page 745
- DLP-J64 View Far-End PM Counts Using CTC, on page 746
- DLP-J65 Reset Current PM Counts Using CTC, on page 747
- DLP-J66 Clear Selected PM Counts Using CTC, on page 748
- DLP-J67 Clear All PM Thresholds Using CTC, on page 750
- DLP-J68 Set the Auto–Refresh Interval for Displayed PM Counts Using CTC, on page 750

Stop. You have completed this procedure.

DLP-J61 Refresh PM Counts at 15–Minute Intervals Using CTC

Purpose	This procedure changes the window view to display PM counts in 15–minute intervals using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to change the window view to display PM counts in 15–minute intervals.

Step 2 In node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card, line card, or CPT50 panel.

Step 4 Click the **Performance** tab.

Step 5 To change the PM interval to 15 minutes for a subtab, click the relevant subtabs.

Note Performance subtabs vary depending on the card.

Step 6 To change the PM interval to 15 minutes for a specific port, select the port from the Ports drop-down list (when available).

Step 7 Click the **15 min** radio button.

Step 8 Click **Refresh**. PM parameters appear in 15-minute intervals synchronized with the time of day.

Step 9 View the Curr column to find PM counts for the current 15-minute interval.
Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 15-minute interval, a TCA is raised. The number represents the counter value for each specific PM parameter.

Step 10 View the Prev-n columns to find PM counts for the previous 15-minute intervals.

Note If a complete 15-minute interval count is not possible, the value appears with a yellow background. An incomplete or incorrect count can be caused by monitoring for less than 15 minutes after the counter started, changing the node timing settings, changing the time zone settings, replacing a card, resetting a card, or changing port service states. When the problem is corrected, the subsequent 15-minute interval appears with a white background.

Step 11 Return to your originating procedure (NTP).

DLP-J62 Refresh PM Counts at One–Day Intervals Using CTC

Purpose	This procedure changes the window view to display PM counts in one day intervals using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to change the PM count display interval.

Step 2 In node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card, line card, or CPT50 panel.

Step 4 Click the **Performance** tab.

Step 5 To change the PM interval to one day for a subtab, click the relevant subtabs.

Note Performance subtabs vary depending on the card.

Step 6 To change the PM interval to one day for a specific port, select the port from the Ports drop-down list (when available).

Step 7 Click the **1 day** radio button.

Step 8 Click **Refresh**. PM parameters appear in one day intervals synchronized with the time of day.

Step 9 View the Curr column to find PM counts for the current one day interval.
Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular one day interval, a TCA is raised. The number represents the counter value for each specific PM parameter.

Step 10 View the Prev-n columns to find PM counts for the previous one day intervals.

Note If a complete count over a one day interval is not possible, the value appears with a yellow background. An incomplete or incorrect count can be caused by monitoring for less than 24 hours after the counter started, changing the node timing settings, changing the time zone settings, replacing a card, resetting a card, or changing port service states. When the problem is corrected, the subsequent one day interval appears with a white background.

Step 11 Return to your originating procedure (NTP).

DLP-J63 View Near–End PM Counts Using CTC

Purpose	This procedure displays the near–end PM counts for the selected card and port using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

Note Near-end PM parameters are available only for OTN.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to view the near-end PM counts.

Step 2 In node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card, line card, or CPT50 panel.

Step 4 Click the **Performance** tab.

Step 5 To view the near-end PM counts for a subtab, click the relevant subtabs.

Note Performance subtabs vary depending on the card.

Step 6 To view near-end PM counts for a specific port, select the port from the Ports drop-down list (when available).

Step 7 Click the **Near End** radio button (when available). Viewing near-end PM counts is not available on some tabs.

Step 8 Click **Refresh**. All the current PM parameters for the selected card on the incoming signal appear.

Step 9 View the Curr column to find PM counts for the current time interval.

Step 10 View the Prev-n columns to find PM counts for the previous time intervals.

Step 11 Return to your originating procedure (NTP).

DLP-J64 View Far-End PM Counts Using CTC

Purpose	This procedure displays the far-end PM parameters for the selected card and port using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Far-end PM parameters are available only for OTN.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to view the far-end PM counts.

Step 2 In node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card, line card, or CPT50 panel.

Step 4 Click the **Performance** tab.

Step 5 To view the far-end PM counts for a subtab, click the relevant subtabs.

Note Performance subtabs vary depending on the card.

Step 6 To view the far-end PM counts for a specific port, select the port from the Ports drop-down list (when available).

Step 7 Click the **Far End** radio button (when available). Viewing far-end PM counts is not available on some tabs.

Step 8 Click **Refresh**. All the PM parameters recorded by the far-end node for the selected card on the outgoing signal appear.

Step 9 View the Curr column to find PM counts for the current time interval.

Step 10 View the Prev-n columns to find PM counts for the previous time intervals.

Step 11 Return to your originating procedure (NTP).

DLP-J65 Reset Current PM Counts Using CTC

Purpose	This procedure resets the current PM counts using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to reset the current PM counts.

Step 2 In node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card, line card, or CPT50 panel.

Step 4 Click the **Performance** tab.

Step 5 To reset the PM counts for a subtab, click the relevant subtabs.

Note Performance subtabs vary depending on the card.

Step 6 To reset the PM counts for a specific port, select the port from the Ports drop-down list (when available).

Step 7 Click **Baseline**.

Note The Baseline button clears the PM counts that appear in the current time interval but does not clear the PM counts on the card. When the current time interval expires or the window view changes, the total number of PM counts on the card and in the window appears in the appropriate column. The baseline values are discarded if you change views to a different window and then return to the Performance window.

Step 8 In the Baseline Statistics dialog box, click one of the following radio buttons:

- **All statistics for port x—**Resets all the PM counts associated with all the combinations of the statistics on the selected port from the card and the window. This means that all time intervals, directions, and signal type counts are reset from the card and the window.
- **All statistics for card—**Resets all the PM counts for all the ports from the card and the window.

Step 9 In the Baseline Statistics dialog box, click **Set Baseline** to reset the selected statistics.

Step 10 View the current statistics columns to observe changes to PM counts for the current time interval.

Step 11 Return to your originating procedure (NTP).

DLP-J66 Clear Selected PM Counts Using CTC

Purpose	This procedure clears the selected PM counts using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Clicking the Clear button can mask problems if used incorrectly. This button is commonly used for testing purposes. After clicking this button, the current count is marked invalid. Also note that the unavailable seconds (UAS) count is not cleared if you were counting UAS; therefore, this count could be unreliable when you click Clear.

Note The CTC and IOS interface counters are mutually exclusive. When you clear the counters through CTC (Card view -> Performance or Card view -> Performance -> Payload PM), the IOS counters are not cleared. When you clear the counters through IOS using the **clear count** command, the CTC counters are not cleared. The baseline is maintained separately for both the CTC and IOS counters. The user must not view the IOS counters if the configuration mode is in CTC mode and vice versa.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to clear the selected PM counts.

Step 2 In node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card, line card, or CPT50 panel.

Step 4 Click the **Performance** tab.

Step 5 To clear the selected PM counts for a subtab, click the relevant subtabs and click **Clear**.

Note Performance subtabs vary depending on the card.

Step 6 To clear the selected PM counts for a specific port, select the OTN subtab or port from the Ports drop-down list (when available).

Step 7 Click **Clear**.

Step 8 In the Clear Statistics dialog box, click one of the following radio buttons:

- **All statistics for port x—**Clears all the statistics for port x by erasing all the PM counts associated with all the combinations of the statistics on the selected port from the card and the window. This means that all time intervals, directions, and signal type counts are erased from the card and the window.
- **All statistics for card—**Clears all the statistics for the card by erasing all the PM counts for all the ports from the card and the window.

Step 9 In the Clear Statistics dialog box, click **OK** to clear the selected statistics. Click **Yes** to confirm the change.

Step 10 Verify that the selected PM counts have been cleared.

Step 11 Return to your originating procedure (NTP).

DLP-J67 Clear All PM Thresholds Using CTC

Purpose	This procedure clears all the PM thresholds using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Clicking the Reset button can mask problems if used incorrectly. This button is commonly used for testing purposes.

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to clear all the PM thresholds.

Step 2 In node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card, line card, or CPT50 panel.

Step 4 Click the **Provisioning** tab.

Step 5 Click the **Thresholds** subtabs. The subtab names vary depending on the selected card.

Step 6 Click **Reset to Default**.

Step 7 Click **Yes** in the Reset to Default dialog box.

Step 8 Verify that the PM thresholds have been reset.

Step 9 Return to your originating procedure (NTP).

DLP-J68 Set the Auto–Refresh Interval for Displayed PM Counts Using CTC

Purpose	This procedure sets the auto–refresh interval for displayed PM counts using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to set the auto-refresh interval for displayed PM counts.

Step 2 In node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card, line card, or CPT50 panel.

Step 4 Click the **Performance** tab.

Step 5 To set the PM auto-refresh interval for a subtab, click the relevant subtabs.

Note Performance subtabs vary depending on the card.

Step 6 To set the PM auto-refresh interval for a specific port, select the port from the Ports drop-down list (when available).

Step 7 From the Auto-refresh drop-down list, choose one of the following options:

- **None**: Disables the auto-refresh feature.
- **15 Seconds—**This option sets the window auto-refresh at 15-seconds time interval.
- **30 Seconds—**Sets the window auto-refresh at 30-seconds time interval.
- **1 Minute—**Sets the window auto-refresh at one minute time interval.
- **3 Minutes—**Sets the window auto-refresh at three minutes time interval.
- **5 Minutes—**Sets the window auto-refresh at five minutes time interval.

Note System refreshes the PM statistics with minimum time interval of 60 seconds. It is recommended to set the auto-refresh time interval minimum to 60 seconds.

Step 8 Click **Refresh**. The PM counts for the newly selected auto-refresh time interval appear.
Depending on the selected auto-refresh interval, the displayed PM counts automatically update when each refresh interval completes. If the auto-refresh interval is set to None, the PM counts that appear are not updated unless you click Refresh.

Step 9 Return to your originating procedure (NTP).

NTP-J24 Monitor Performance Using CTC

Purpose	This procedure monitors the near-end or far-end performance of the node for selected time intervals on the fabric and line cards.

Tools/Equipment	None
Prerequisite Procedures	Ensure you have created the appropriate circuits and provisioned the card according to your specifications.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at the node that you want to monitor the performance.

Step 2 Complete the following procedures as needed to view the PM parameters for the fabric, line card, or CPT 50 shelf:

- DLP-J69 Provision PPM and Port Using CTC, on page 753
- DLP-J70 View Optics PM Parameters Using CTC, on page 755
- DLP-J71 View Payload PM Parameters Using CTC, on page 756
- DLP-J72 Display Performance Monitoring Parameters Using Cisco IOS Commands, on page 752

Note To refresh, reset, or clear PM counts, see the NTP-J23 Change the PM Display Using CTC, on page 743 procedure.

Stop. You have completed this procedure.

DLP-J72 Display Performance Monitoring Parameters Using Cisco IOS Commands

Purpose	This procedure displays the performance monitoring parameters using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note In CPT IOS, performance monitoring statistics are provided only for 15 minute and 1 day intervals. Historical counts are not maintained in CPT IOS. FEC, optical transport network (OTN), alarm, and TCA thresholds are not provided through CPT IOS.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router# enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**show controllers dwdm** *slot/port* **pm interval** {**15-min** | **24-hour**} **Example:** Router# show controllers dwdm 4/3 pm interval 15-min	**Need confirmation on whether this command is supported.** Displays the performance parameters for 15 minute or 1 day intervals.
Step 4	Return to your originating procedure (NTP).	—

DLP-J69 Provision PPM and Port Using CTC

Purpose	This procedure provisions a PPM and port in a fabric card, line card, or CPT50 panel using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to provision a PPM and port.

Step 2 In the node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 In the Packet Transport System View dialog box, double-click a fabric card, line card, or CPT50 panel.

Step 4 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 5 In the Pluggable Port Modules area, click **Create**. The Create PPM dialog box appears.

Step 6 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.

Step 7 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 the PPM.

Step 8 In the Pluggable Ports area, click **Create**. The Create Port dialog box appears.

Step 9 In the Create Port dialog box, complete the following:

- Port—Choose the port you want to configure from the Port drop-down list.
- Port Type—(for fabric and line cards) Choose the port type, such as TEN-GE from the Port Type drop-down list.
- Port Type—(for CPT 50 panel) Choose the port type, such as ONE-GE, FE, or TEN-GE from the Port Type drop-down list.

Note CPT 50 panel supports ONE-GE and FE for ports 1 to 44. CPT 50 panel supports TEN-GE for ports 45 to 48.

Step 10 Click **OK**. The newly created port appears in the Pluggable Ports area. The port type you provisioned is listed in the Rate column.
In case of PROV-MISMATCH alarm, user needs to provide acceptable reach value for the PPM. Change the value to **.This can be done without making shut.

In case of WVL-MISMATCH alarm , user needs to change the wavelength of PPM based on it's type. This can be made only when port is admin down. Changing wavelength without making port as admin down will be available in later release.

Step 11 Repeat Steps DLP-J69 Provision PPM and Port Using CTC, on page 753 through DLP-J69 Provision PPM and Port Using CTC, on page 753 to provision another PPM and port.

Step 12 Return to your originating procedure (NTP).

DLP-J70 View Optics PM Parameters Using CTC

Purpose	This procedure displays the optics PM parameters using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to view the optics PM parameters.

Step 2 In node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card, line card, or CPT50 panel.

Step 4 Click the **Performance > Optics PM > Current Values** tabs.

Step 5 View the current PM parameter names that appear in the Param column.

Step 6 Click the **Historical PM** tab.

Step 7 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-n (previous) columns.
Table 40: Optics PM Parameters, on page 755 describes the settings for the optics PM parameters.

Table 40: Optics PM Parameters

Optics PM Parameters	Definition
Laser Bias (Min,%)	Minimum laser bias current (Laser Bias Min) is the minimum percentage of laser bias current during the PM time interval.
Laser Bias (Avg,%)	Average laser bias current (Laser Bias Avg) is the average percentage of laser bias current during the PM time interval.
Laser Bias (Max,%)	Maximum laser bias current (Laser Bias Max) is the maximum percentage of laser bias current during the PM time interval.
Rx Optical Pwr (Min,dBm)	Minimum receive optical power (Rx Optical Pwr Min, dBm) is the minimum optical power received during the PM time interval.
Rx Optical Pwr (Avg,dBm)	Average receive optical power (Rx Optical Pwr Avg, dBm) is the average optical power received during the PM time interval.

Optics PM Parameters	Definition
Rx Optical Pwr (Max,dBm)	Maximum receive optical power (Rx Optical Pwr Max, dBm) is the maximum optical power received during the PM time interval.
Tx Optical Pwr (Min,dBm)	Minimum transmit optical power (Tx Optical Pwr Min, dBm) is the minimum optical power transmitted during the PM time interval.
Tx Optical Pwr (Avg,dBm)	Average transmit optical power (Tx Optical Pwr Avg, dBm) is the average optical power transmitted during the PM time interval.
Tx Optical Pwr (Max,dBm)	Maximum transmit optical power (Tx Optical Pwr Max, dBm) is the maximum optical power transmitted during the PM time interval.

Step 8 Return to your originating procedure (NTP).

DLP-J71 View Payload PM Parameters Using CTC

Purpose	This procedure displays the payload PM parameters using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J69 Provision PPM and Port Using CTC, on page 753
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to view the payload PM parameters.

Step 2 In node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card, line card, or CPT50 panel.

Step 4 Click the **Performance > Payload PM > Statistics** tabs.

Step 5 Click **Refresh**. PM statistics appear for each port on the card.

Note System refreshes the PM statistics with minimum time interval of 60 seconds so if user presses the Refresh button with less than 60 seconds interval, it will not display the updated statistics. It is also applicable for PM statistics retrieved using SNMP.

Step 6 View the PM parameter names that appear in the Param column. The current PM parameter values appear in the Port # columns.
Payload PM parameters are as follows:

- IfInOctets
- rxTotalPkts
- ifInUcastPkts
- ifInMulticastPkts
- ifInDiscards
- ifInErrors
- ifOutOctets
- txTotalPkts
- ifOutUcastPkts
- ifOutMulticastPkts
- ifOutDiscards
- ifOutErrors

Step 7 Click the **Performance > Payload PM > Utilization** tabs.

Step 8 Click **Refresh**. PM utilization values appear for each port on the card.

Step 9 View the appropriate row for the port you want to monitor. The transmit (Tx) and receive (Rx) bandwidth utilization values for the previous time intervals appear in the Prev-n columns.

Step 10 Click the **Performance > Payload PM > History** tabs.

Step 11 From the Port drop-down list, choose the desired port.

Step 12 Click **Refresh**. PM statistics appear for the selected port.

Step 13 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Prev-n columns.

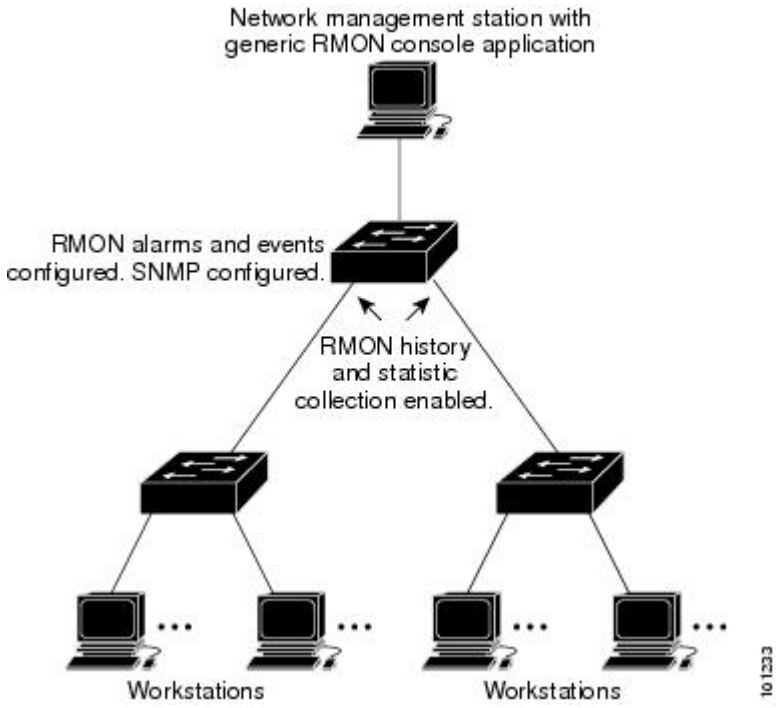
Step 14 Return to your originating procedure (NTP).

Understanding RMON

Remote Network Monitoring (RMON) is a standard monitoring feature that allows various network agents and console systems to exchange network monitoring data. RMON provides you with comprehensive network-fault diagnosis, planning, and performance-tuning information. You can use the RMON feature with the Simple Network Management Protocol (SNMP) agent in the switch to monitor all the traffic flowing

among switches on all connected LAN segments as shown in Figure 77: Remote Monitoring Example, on page 758.

Figure 77: Remote Monitoring Example



Default RMON Configuration

RMON is disabled by default; no alarms or events are configured.

NTP-J25 Configure RMON Settings

Purpose	This procedure configures RMON settings.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

• DLP-J74 Configure RMON Settings Using Cisco IOS Commands, on page 759
• DLP-J73 Change the RMON Thresholds Using CTC, on page 761

Stop. You have completed this procedure.

DLP-J74 Configure RMON Settings Using Cisco IOS Commands

Purpose	This procedure configures the RMON settings using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router# enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface type slot/port** **Example:** Router(config)# interface TenGigabitEthernet4/1	Specifies the interface and enters interface configuration mode.
Step 4	**rmon** {**native** | **promiscuous**} **Example:** Router(config-if)# rmon native	Enables RMON on an Ethernet interface. native—Enables the router to process only packets destined for this interface. promiscuous—Enables the router to examine every packet. This example enables RMON in native mode.

	Command or Action	Purpose
Step 5	**rmon collection history controlEntry** *integer* [**buckets** *bucket-number*] [**interval** *seconds*] [**owner** *ownername*] **Example:** Router(config-if)# rmon collection history controlEntry 5 buckets 5 interval 10 owner user1	Enables RMON history collection for the specified number of buckets and time period. This example enables RMON history collection with an ID number of 5 and an owner of *user1*.
Step 6	**rmon collection host controlEntry** *integer* [**owner** *ownername*] **Example:** Router(config-if)# rmon collection host controlEntry 10 owner user1	Enables RMON statistic collection on the interface.
Step 7	**rmon alarm** *number variable interval* {**delta** | **absolute**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *string*] **Example:** Router(config-if)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-threshold 0 owner user1	Sets a RMON alarm on a MIB object. This example configures RMON alarm number 10. The alarm monitors the MIB variable *ifEntry.20.1* once every 20 seconds until the alarm is disabled, and checks the change in the rise or fall of the variable. If the *ifEntry.20.1* value shows a MIB counter increase of 15 or more, such as from 100000 to 100015, the alarm is triggered. The alarm in turn triggers event number 1, which is configured with the **rmon event** command. The possible events include a log entry or an SNMP trap. If the *ifEntry.20.1* value changes by 0, the alarm is reset and can be triggered again.
Step 8	**rmon event** *number* [**log**] [**trap** *community*] [**description** *string*] [**owner** *string*] **Example:** Router(config-if)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner user	Adds or removes an event in the RMON event table that is associated with an RMON event number. This example creates RMON event number 1, which is defined as *High ifOutErrors*, and generates a log entry when the event is triggered by an alarm. The user *user* owns the row that is created in the event table by this command. This example also generates a Simple Network Management Protocol (SNMP) trap when the event is triggered.
Step 9	exit **Example:** Router(config-if)# exit	Exits interface configuration mode.
Step 10	Return to your originating procedure (NTP).	—

Display RMON Status Using Cisco IOS Commands

To display the current RMON agent status on the router, use one or more of the privileged EXEC commands described in Table 41: Commands for Displaying RMON Status, on page 761.

Table 41: Commands for Displaying RMON Status

Command	Purpose
show rmon or **show rmon task**	Displays general RMON statistics.
show rmon alarms	Displays the RMON alarm table.
show rmon capture	Displays the RMON buffer capture table and current configuration.
show rmon events	Displays the RMON event table.
show rmon filter	Displays the RMON filter table.
show rmon history	Displays the RMON history table.
show rmon hosts	Displays the RMON hosts table.
show rmon matrix	Displays the RMON matrix table and values associated with RMON variables.
show rmon statistics	Displays the RMON statistics table.
show rmon topn	Displays the RMON top-n hosts table.

For examples on **show rmon** command, see the *Cisco CPT Command Reference Guide*.

DLP-J73 Change the RMON Thresholds Using CTC

Purpose	This procedure changes the RMON threshold settings using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J69 Provision PPM and Port Using CTC, on page 753
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to change the RMON thresholds.

Step 2 In node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card, line card, or CPT50 panel.

Step 4 Click the **Provisioning > RMON Thresholds** tabs.

Step 5 Click **Create**. The Create Threshold dialog box appears.

Step 6 From the Port drop-down list, choose an individual port, or choose **All** to provision RMON thresholds for all the ports.

Step 7 From the Variable drop-down list, choose an appropriate Ethernet variable. Table 42: RMON Variables , on page 762 lists the available Ethernet RMON variables.

Table 42: RMON Variables

Variable	Description
ifInOctets	Total number of octets received on the interface, including framing characters.
rxTotalPkts	Total number of received packets.
ifInUcastPkts	The number of packets, delivered by this sub-layer to a higher sub-layer, which were not addressed to a multicast or broadcast address at this sub-layer.
ifInMulticastPkts	The number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both group and functional addresses.
ifInDiscards	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent them from being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
IfInErrors	Number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol.
ifOutOctets	Total number of octets transmitted out of the interface, including framing characters.
txTotalPkts	Total number of transmitted packets.
ifOutUcastPkts	The number of packets transmitted by a port that are addressed to a unicast address.
ifOutMulticastPkts	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both group and functional addresses.

Variable	Description
ifOutDiscards	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent them from being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
IfOutErrors	Number of outbound packets or transmission units that could not be transmitted because of errors.

Step 8 From the Alarm Type drop-down list, indicate whether the event will be triggered by the rising threshold, the falling threshold, or both the rising and falling thresholds.

Step 9 From the Sample Type drop-down list, choose either **Relative** or **Absolute**. Relative restricts the threshold to use the number of occurrences in the user-set sample period. Absolute sets the threshold to use the total number of occurrences, regardless of time period.

Step 10 Enter the appropriate number of seconds for the sample period in the Sample Period field.

Step 11 Enter the appropriate number of occurrences for the rising threshold in the Rising Threshold field.
For a rising type of alarm, the measured value must move from below the falling threshold to above the rising threshold. For example, if a network is running below a rising threshold of 1000 collisions every 15 seconds and a problem causes 1001 collisions in 15 seconds, the excess occurrences trigger an alarm.

Step 12 Enter the appropriate number of occurrences in the Falling Threshold field. In most cases a falling threshold is set lower than the rising threshold.
A falling threshold is the counterpart to a rising threshold. When the number of occurrences is above the rising threshold and then drops below a falling threshold, it resets the rising threshold. For example, when the network problem that caused 1001 collisions in 15 seconds subsides and creates only 799 collisions in 15 seconds, occurrences fall below a falling threshold of 800 collisions. This resets the rising threshold so that if the network collisions again spike over a 1000 per 15-second period, an event triggers when the rising threshold is crossed. An event is triggered only for the first time when a rising threshold is exceeded (otherwise, a single network problem might cause a rising threshold to be exceeded multiple times and cause a flood of events).

Step 13 Click **OK**.

Step 14 To view all the RMON thresholds, click **Show All RMON thresholds**.

Step 15 Return to your originating procedure (NTP).

Understanding OTN

The Optical Transport Network (OTN) protocol is specified in ITU-T G.709. This standard combines the benefits of SONET/SDH technology with the multiwavelength networks of DWDM. It also provides forward error correction (FEC) that reduces network costs by reducing the number of regenerators used.

To enable multiservice transport, OTN uses the concept of a wrapped overhead (OH). To illustrate this structure:

- Optical channel payload unit (OPU) OH information is added to the information payload to form the OPU. The OPU OH includes information to support the adaptation of client signals.
- Optical channel data unit (ODU) OH is added to the OPU to create the ODU. The ODU OH includes information for maintenance and operational functions to support optical channels.

- Optical channel transport unit (OTU) OH together with the FEC is added to form the OTU. The OTU OH includes information for operational functions to support the transport by way of one or more optical channel connections.
- Optical channel (OCH) OH is added to form the OCH. The OCH provides the OTN management functionality and contains four subparts: the OPU, ODU, OTU, and frame alignment signal (FAS). See Figure 78: OTN Optical Channel Structure, on page 764.

Figure 78: OTN Optical Channel Structure

OTN has the following advantages:

- Stronger forward error correction
- More levels of Tandem Connection Monitoring (TCM)
- Transparent transport of signals
- Switching scalability

Note The OTN parameters can be changed only through CTC.

NTP-J26 Configure OTN Settings

Purpose	This procedure configures OTN settings.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J75 Change the Optical Transport Network Settings Using CTC, on page 765
- DLP-J76 View OTN PM Parameters Using CTC, on page 770

Stop. You have completed this procedure.

DLP-J75 Change the Optical Transport Network Settings Using CTC

Purpose	This procedure changes the OTN settings for the fabric, line card, or CPT 50 shelf using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

This procedure applies only to the XFP ports of the fabric card (port 3 and port 4).

Procedure

Step 1 Complete the NTP-J22 Log into CTC, on page 15 procedure at a node where you want to change the OTN settings.

Step 2 In node view, right-click the fabric card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card.

Step 4 Click the **Provisioning > OTN** tabs.

Step 5 Choose one of the following subtabs**— OTN Lines, ITU-T G.709 Thresholds, FEC Thresholds, Trail Trace Identifier**.

Step 6 Modify any of the settings described in Table 43: OTN Line Settings, on page 765 to Table 46: Trail Trace Identifier Settings, on page 769.

Note You must modify Near End and Far End; 15 Min and 1 Day; and SM and PM independently. To do so, choose the appropriate radio button and click **Refresh**.

Table 43: OTN Line Settings, on page 765 describes the values on the Provisioning > OTN > OTN Lines tab.

Table 43: OTN Line Settings

Parameter	Description	Options
Port	(Display only) Displays the port number and description.	3 (Trunk) and 4 (Trunk)
ITU-T G.709 OTN	Sets the OTN lines according to ITU-T G.709.	• Enable • Disable

Parameter	Description	Options
FEC	Sets the OTN lines to FEC. Enhanced FEC mode can be enabled to provide greater range and lower bit error rate.	• Disable • Standard • Enhanced1.4 • Enhanced1.7
SF BER	(Display only) Displays the signal fail bit error rate.	• 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9

Table 44: ITU-T G.709 Threshold Settings, on page 766 describes the values on the Provisioning > OTN > ITU-T G.709 Thresholds tab.

Table 44: ITU-T G.709 Threshold Settings

Parameter	Description	Options
Port	(Display only) Displays the port number and optional name.	3 (Trunk) and 4 (Trunk)

Parameter	Description	Options
ES	Errored seconds.	Numeric. Threshold display options include: • Direction—Near End or Far End • Interval—15 Min (minutes) or 1 day • Types—SM (OTUk) or PM (ODUk) Choose an option in each category and click **Refresh**. **Note** SM (OTUk) is the ITU-T G.709 optical channel transport unit order of k overhead frame used for management and performance monitoring. PM (ODUk) is the ITU-T G.709 optical channel data unit order of k overhead frame unit used for path performance monitoring.
SES	Severely errored seconds	Numeric. Threshold display options include: • Direction—Near End or Far End • Interval—15 Min (minutes) or 1 day • Types—SM (OTUk) or PM (ODUk) Choose an option in each category and click **Refresh**.

Parameter	Description	Options
UAS	Unavailable seconds	Numeric. Threshold display options include: • Direction—Near End or Far End • Interval—15 Min (minutes) or 1 day • Types—SM (OTUk) or PM (ODUk) Choose an option in each category and click **Refresh**.
BBE	Background block errors	Numeric. Threshold display options include: • Direction—Near End or Far End • Interval—15 Min (minutes) or 1 day • Types—SM (OTUk) or PM (ODUk) Choose an option in each category and click **Refresh**.
FC	Failure counter	Numeric. Threshold display options include: • Direction—Near End or Far End • Interval—15 Min (minutes) or 1 day • Types—SM (OTUk) or PM (ODUk) Choose an option in each category and click **Refresh**.

Table 45: FEC Threshold Settings, on page 769 describes the values on the Provisioning > OTN > FEC Thresholds tab.

Table 45: FEC Threshold Settings

Parameter	Description	Options
Port	(Display only) Displays the port number and optional name.	3 (Trunk) and 4 (Trunk)
Bit Errors Corrected	(Display only) Displays the number of bit errors corrected during the selected time period.	Numeric display. Can be set for 15-minute or one-day intervals.
Uncorrectable Words	(Display only) Displays the number of uncorrectable words in the selected time period.	Numeric display. Can be set for 15-minute or one-day intervals.

Table 46: Trail Trace Identifier Settings, on page 769 describes the values on the Provisioning > OTN > Trail Trace Identifier tab.

Table 46: Trail Trace Identifier Settings

Parameter	Description	Options
Port	(Display only) Displays the port number.	3 (Trunk) and 4 (Trunk)
Level	Sets the level of monitoring.	• Section • Path
Received Trace Mode	Sets the trace mode.	• Off/None • Manual
Transmit	Displays and sets a transmit string. You can click the button on the right to change the display. Its title changes, based on the current display mode. Click **Hex** to change the display to hexadecimal (button changes to ASCII); click **ASCII** to change the display to ASCII (button changes to Hex).	String of trace string size
Disable FDI on TTIM	If a Trace Identifier Mismatch (TTIM) on Section overhead alarm arises because of a overhead string mismatch, no Forward Defect Indication (FDI) signal is sent to the downstream nodes if this box is checked.	• Checked (FDI on TTIM is disabled) • Unchecked (FDI on TTIM is enabled)
Expected	Displays and sets a expected string. You can click the button on the right to change the display. Its title changes, based on the current display mode. Click **Hex** to change the display to hexadecimal (button changes to ASCII); click **ASCII** to change the display to ASCII (button changes to Hex).	String of trace string size

Parameter	Description	Options
Received	(Display only) Displays the current received string. You can click Refresh to manually refresh this display, or check the Auto-refresh every 5 sec check box to keep this panel updated.	String of trace string size
Auto-refresh	If checked, automatically refreshes the display every 5 minutes.	• Checked • Unchecked (default)

Step 7 Return to your originating procedure (NTP).

DLP-J76 View OTN PM Parameters Using CTC

Purpose	This procedure displays the OTN PM parameters using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to view the near-end or far-end OTN PM parameters for the selected time intervals.

Step 2 In node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card.

Step 4 Click the **Performance > OTN PM > ITU-T G.709 PM** tabs.

Step 5 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-n (previous) columns.
Table 47: ITU G.709 Section Monitoring and Path Monitoring PM Definitions, on page 771 describes the settings for ITU G.709 PM definitions.

Table 47: ITU G.709 Section Monitoring and Path Monitoring PM Definitions

Parameter	Definition
BBE-SM	Background Block Errors Section Monitoring (BBE-SM) shows the number of background block errors recorded in the OTN section during the PM time interval.
ES-SM	Errored Seconds Section Monitoring (ES-SM) shows the errored seconds recorded in the OTN section during the PM time interval.
SES-SM	Severely Errored Seconds Section Monitoring (SES-SM) shows the severely errored seconds recorded in the OTN section during the PM time interval.
UAS-SM	Unavailable Seconds Section Monitoring (UAS-SM) shows the unavailable seconds recorded in the OTN section during the PM time interval.
FC-SM	Failure Counts Section Monitoring (FC-SM) shows the failure counts recorded in the OTN section during the PM time interval.
ESR-SM	Errored Seconds Ratio Section Monitoring (ESR-SM) shows the severely errored seconds ratio recorded in the OTN section during the PM time interval.
SESR-SM	Severely Errored Seconds Ratio Section Monitoring (SESR-SM) shows the severely errored seconds ratio recorded in the OTN section during the PM time interval.
BBER-PM	Background Block Errors Ratio Path Monitoring (BBER-PM) shows the background block errors ratio recorded in the OTN path during the PM time interval.
BBE-PM	Background Block Errors Path Monitoring (BBE-PM) shows the number of background block errors recorded in the OTN path during the PM time interval.
ES-PM	Errored Seconds Path Monitoring (ES-PM) shows the errored seconds recorded in the OTN path during the PM time interval.
SES-PM	Severely Errored Seconds Path Monitoring (SES-PM) shows the severely errored seconds recorded in the OTN path during the PM time interval.
UAS-PM	Unavailable Seconds Path Monitoring (UAS-PM) shows the unavailable seconds recorded in the OTN path during the PM time interval.
FC-PM	Failure Counts Path Monitoring (FC-PM) shows the failure counts recorded in the OTN path during the PM time interval.
ESR-PM	Errored Seconds Ratio Path Monitoring (ESR-PM) shows the severely errored seconds ratio recorded in the OTN path during the PM time interval.

Step 6 Click the **FEC PM** tab.

Step 7 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-n (previous) columns.
Table 48: FEC PM Definitions, on page 772 describes the settings for FEC PM definitions.

Table 48: FEC PM Definitions

Parameter	Definition
Bit Errors	Bit errors are the number of bit errors corrected.
Uncorrectable words	Uncorrectable words occur when FEC detects and corrects errors to deliver a 7 to 8 dB improvement in the signal-to-noise ratio (also called margin). For ITU G.709, the FEC code used is Reed-Solomon RS (255, 239).

Step 8 Return to your originating procedure (NTP).

NTP-J27 Modify the Ethernet Settings and Alarm Thresholds

Purpose	This procedure modifies the Ethernet settings and alarm thresholds.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J77 Provision Alarm and TCA Thresholds Using CTC, on page 773
- DLP-J78 Change the Port and Ethernet Settings Using CTC, on page 774

Stop. You have completed this procedure.

DLP-J77 Provision Alarm and TCA Thresholds Using CTC

Purpose	This procedure changes the alarm and TCA thresholds for the fabric, line card, or CPT 50 panel using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to provision alarm and TCA thresholds.

Step 2 In node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card, line card, or CPT50 panel.

Step 4 Click the **Provisioning > Optics Thresholds** tabs.

Note You must modify 15 Min and 1 Day independently. To do so, choose the appropriate radio button and click **Refresh**.

Step 5 If TCA is not selected, click **TCA** and then click **Refresh**.

Note Do not modify the Laser Bias parameters.

Step 6 Verify the provisioned TCA threshold values in the Warning Thresholds table. To provision new thresholds as needed, click the threshold value you want to change, delete it, enter a new value, and press **Enter**.

Step 7 Under Types, click the **Alarm** radio button and click **Refresh**.

Note Do not modify the Laser Bias parameters.

Step 8 Verify the provisioned alarm threshold values in the Alarm Thresholds table. To provision new thresholds as needed, click the threshold value you want to change, delete it, enter a new value, and press **Enter**.

Step 9 Click **Apply**.

Step 10 Return to your originating procedure (NTP).

Carrier Delay

Carrier delay is the soak period before link failure is communicated to higher protocols.

Default Carrier Delay Duration

This table lists the default duration for carrier delay.

Table 49: Default Carrier Delay Duration

Card/Port	Default Time
Ports on the fabric card	2 seconds
Ports on the line card	200 milliseconds
Ports on the CPT 50 panel	200 milliseconds
Ports on the ring	10 milliseconds

The range of carrier delay is from 0 to 60. The higher carrier delay affects the switch times for protocols such as LAG and REP. See DLP-J78 Change the Port and Ethernet Settings Using CTC, on page 774 to change the carrier delay time.

Carrier Delay Limitations

When Ethernet services are configured, set the carrier delay time to greater than or equal to 2 seconds for fabric cards and CPT 50 panels attached to fabric cards. When MPLS services are configured, set the carrier delay time to less than 2 seconds, for fabric cards and CPT 50 panels attached to fabric cards. However, this time limit does not apply to line cards and CPT 50 panels attached to line cards. The carrier delay time of 2 seconds in fabric cards can cause traffic drops on SSO.

DLP-J78 Change the Port and Ethernet Settings Using CTC

Purpose	This procedure changes the port and Ethernet settings for the fabric, line card, or CPT 50 shelf using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to change the port and Ethernet settings.

Step 2 In node view, right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Double-click a fabric card, line card, or CPT50 panel.

Step 4 Click the **Provisioning > Ether Ports > Ethernet** tabs.

Step 5 Modify any of the settings for the Ethernet tab as described in Table 50: Ethernet Settings, on page 775.

Table 50: Ethernet Settings

Parameter	Description	Options
Port	(Display only) Displays the port number and rate.	—
MTU	The maximum size of the Ethernet frames accepted by the port. The port must be in OOS/locked state.	Numeric. Default: 9600 Range 64 to 9600
Link State	(Display only) Displays the state of the link. **Note** Link status shows up in CTC and IOS for TDM pluggables even when there is no physical connection.	• DOWN • UP
Expected Speed	The expected speed of the device that is or will be attached to the Ethernet port. The 10GE SFP+/XFP ports on the fabric or line card supports only 10000 Mbps. (For 1GE SFPs in the CPT 50 panel) If you know the speed, choose **1000 Mbps**, **100 Mbps**, or **10 Mbps** to match the attached device. If you do not know the speed, choose **Auto** to enable autonegotiation for the speed of the port. In this case, the port attempts to negotiate a mutually acceptable speed with the attached device. If the expected speed is set to **Auto**, you cannot enable Selective Auto Negotiation.	For fabric and line card: 10000 Mbps For CPT 50 panel, the options are: • 10 Mbps • 100 Mbps • 1000 Mbps • Auto

Parameter	Description	Options
Expected Duplex	The expected duplex of the device that is or will be attached to the Ethernet port. The 10GE SFP+/XFP ports on the fabric or line card supports only Full duplex. (For 1GE SFPs in the CPT 50 panel) If you know the duplex, choose **Full** or **Half** to match the attached device. If you do not know the duplex, choose **Auto** to enable autonegotiation for the duplex of the port. In this case, the port attempts to negotiate a mutually acceptable duplex with the attached device. If the expected duplex is set to Auto, you cannot enable Selective Auto Negotiation.	For fabric and line card: Full For CPT 50 panel, the options are: • Full • Half • Auto
Flow Control	Enables or disables flow control messaging with the external device. For example, consider you have a 1GE port on the CPT 50 panel. The external device is sending the traffic with higher rate. Hence, the 1GE port cannot handle all the incoming traffic. If flow control is enabled, the 1GE port will send a Pause frame to the external device and the external device will not transmit data for a specific period.	• ON • OFF
Interconnect Mode	(Display only) The SFP+ ports on the fabric or line card can serve as normal ports or InterConnect (IC) ports. When the SFP+ ports are used as normal ports, it can be used as 10000 Mbps ports. When the SFP+ ports are used as IC ports, these ports are used to connect with the SFP+ ports on the CPT 50 panel. When a Fan-Out Group is created on SFP+ ports, the SFP+ ports will be automatically converted to InterConnect ports. If checked, it indicates that the port is an InterConnect port.	—
Operating Speed	(Display only) Displays the speed at which the port is operating.	For fabric and line card: 10000 Mbps For CPT 50 panel, the options are: • 10 Mbps • 100 Mbps • 1000 Mbps • Auto

Parameter	Description	Options
Operating Duplex	(Display only) Displays the duplex at which the port is operating.	For fabric and line card: Full For CPT 50 panel, the options are: • Full • Half • Auto
Operating Flow Control	(Display only) Displays the flow control mode at which the port is operating.	• ON • OFF
Carrier Delay (ms)	Sets the soak period before the link failure is communicated to higher protocols.	• Fabric card: 2000 ms • Line card: 200 ms • CPT 50 panel: 200 ms
Fan-Out	(Display only) Displays the name of the Fan-Out group created for the port.	—
L2PT Config	Configures Layer 2 protocol tunneling actions for each Layer 2 protocol.	• Drop • Forward • Peer
Channel Group	(Display only) Displays the name of the channel group associated with this port.	—
Selective Auto Negotiation	(Only for CPT 50 panel) Check this check box to enable selective auto negotiation on the port. If checked, the port attempts to auto negotiate only to the selected expected speed and duplex. The link will come up if both the expected speed and duplex of the attached auto negotiating device matches that of the port. You cannot enable Selective Auto Negotiation if either the expected speed or expected duplex is set to **Auto**.	—
Auto Negotiation State	(Only for CPT 50 panel) Displays the auto negotiation state of the port.	—

Parameter	Description	Options
Media Type	Sets the Media Type. **Note** In IOS mode, remove all the services configured on the port before changing media type for TDM interface.	• Ethernet • DS1 over Ethernet • DS3 over Ethernet • E1 Over Ethernet • E3 Over Ethernet

Step 6 Click the **Provisioning > Ether Ports > Port** tabs.

Step 7 Modify any of the settings for the Port tab as described in Table 51: Port Settings, on page 778.

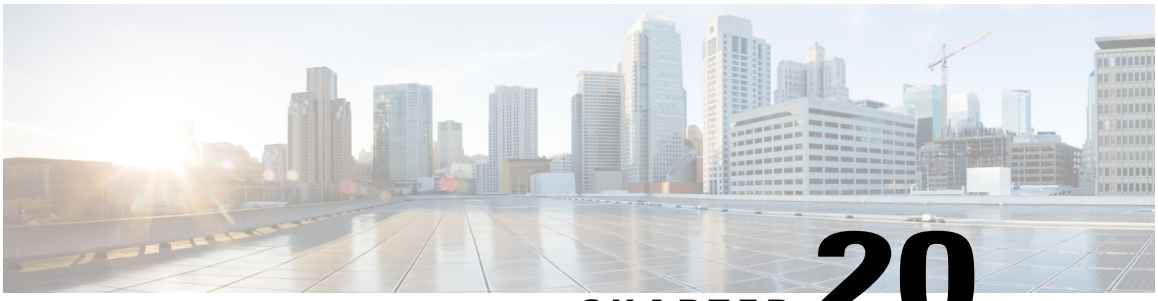
Table 51: Port Settings

Parameter	Description	Options
Port	(Display only) Displays the port number.	—
Port Name	Sets the port name for a port.	User-defined. Name can be up to 32 alphanumeric or special characters or both. Blank by default.
Admin State	Sets the port service state.	• IS • IS,AINS • OOS,DSBLD • OOS,MT
Service State	(Display only) Displays the autonomously generated state that gives the overall condition of the port. Service states appear in the format—Primary State-Primary State Qualifier, Secondary State.	• IS-NR • OOS-AU,AINS • OOS-MA,DSBLD • OOS-MA,MT
AINS Soak	Sets the automatic in-service soak period. Double-click the time and use the up and down arrows to change settings.	• Duration of valid input signal, in hh.mm format, after which the card becomes IS automatically. • 0 to 48 hours, 15-minute increments

Parameter	Description	Options
Reach	Sets the optical reach distance of the ports	The Reach options depend on the traffic type that has been selected.
Wavelength	Sets the wavelength of the ports.	• First Tunable Wavelength • Further wavelengths: 850 nm through 1610 nm, 100-GHz ITU spacing; coarse wavelength division multiplexing (CWDM) spacing.

Step 8 Click **Apply**.

Step 9 Return to your originating procedure (NTP).



CHAPTER 20

Configuring Local Authentication

This chapter describes local authentication. This chapter also describes procedures to configure local authentication and privilege levels.

This chapter includes the following topics:

Understanding Authentication

Access control enables you to restrict access to the network server and its services to a specific group of users. The authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you can set up access control on your router or access server.

Authentication is a way of identifying a user before permitting access to the network and network services. The Carrier Packet Transport (CPT) supports local authentication mechanism to administer its security functions.

NTP-J102 Configure Local Authentication Using Cisco IOS Commands

Purpose	This procedure configures local authentication using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

The only supported login authentication method in CPT is local authentication.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** Router(config)# aaa new-model	Enables authentication, authorization, and accounting (AAA) globally.
Step 4	**aaa authentication login default** *methodname* **Example:** Router(config-if)# aaa authentication login default local	Creates the default local authentication list.
Step 5	**line** [**aux** | **console** | **tty** | **vty**] **line-number** [**ending-line-number**] **Example:** Router(config)# line vty 0 4	Enters line configuration mode for the lines to which you want to apply the authentication list.
Step 6	**login authentication default** **Example:** Router(config-line)# login authentication default	Applies the authentication list to a line or set of lines.
Step 7	**end** **Example:** Router(config-line)# end	Returns to global configuration mode.

Example: Configure Local Authentication

The following example shows how to configure local authentication using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# aaa new-model
Router(config-if)# aaa authentication login default local
Router(config)# line vty 0 4
Router(config-line)# login authentication default
Router(config-line)# end
```

NTP-J103 Protect Access to Privileged EXEC Commands Using Cisco IOS Commands

Purpose	This procedure provides a way to control access to the system configuration file and privileged EXEC (enable) commands, using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the listed procedures as needed.

- DLP-J291 Set or Change a Static Enable Password Using Cisco IOS Commands, on page 783
- DLP-J292 Protect Passwords with Enable Password and Enable Secret Using Cisco IOS Commands, on page 784
- DLP-J293 Set or Change a Line Password Using Cisco IOS Commands, on page 786
- DLP-J294 Encrypt Passwords Using Cisco IOS Commands, on page 787

Stop. You have completed this procedure.

DLP-J291 Set or Change a Static Enable Password Using Cisco IOS Commands

Purpose	This procedure sets or changes a static password that controls access to privileged EXEC (enable) mode, using Cisco IOS commands.

Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**username** *user* **password** *password* **Example:** Router(config)# username user1 password pwd	Sets the user name and password.
Step 4	**enable password** *password* **Example:** Router(config)# enable password user1	Enables a new password or changes an existing password for the privileged command level.
Step 5	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J292 Protect Passwords with Enable Password and Enable Secret Using Cisco IOS Commands

Purpose	This procedure configures the router to require an enable password and an enable secret password using Cisco IOS commands.

Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

To provide an additional layer of security, particularly for passwords that cross the network or are stored on a TFTP server, you can use either the **enable password** or **enable secret** commands. Both commands accomplish the same thing; that is, they allow you to establish an encrypted password that users must enter to access enable mode (the default), or any privilege level you specify.

We recommend that you use the **enable secret** command because it uses an improved encryption algorithm.

If you configure the **enable secret** command, it takes precedence over the **enable password** command; the two commands cannot be in effect simultaneously.

Note If neither the **enable password** command nor the **enable secret** command is configured, and if there is a line password configured for the console, the console line password serves as the enable password for all VTY sessions.

Use the **enable password** or **enable secret** commands with the **level** keyword to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the **privilege level** configuration command to specify the commands accessible at various levels.

You can enable or disable password encryption with the **service password-encryption** command. If you have the **service password-encryption** command enabled, the password you enter is encrypted. When you display it with the **more system:running-config** command, it is displayed in encrypted form.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**username** *user* **password** *password* **Example:** Router(config)# username user1 password pwd	Sets the user name and password.

	Command or Action	Purpose
Step 4	**enable password** [**level** *level-number*] {*password* | *encryption-type encrypted-password*} **Example:** Router(config)# enable password level 2 pswd2	Enables a password for a privilege command mode.
Step 5	**enable secret** [**level** *level-number*] {*password* | *encryption-type encrypted-password*} **Example:** Router(config)# enable secret greentree	Specifies a secret password, saved using a non-reversible encryption method. If both **enable password** and **enable secret** commands are set, the user must enter the **enable secret** password.
Step 6	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

DLP-J293 Set or Change a Line Password Using Cisco IOS Commands

Purpose	This procedure sets or changes a password on a line, using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	Router# configure terminal	
Step 3	**password** *password_new* **Example:** Router(config)# password user1	Enables a new password or changes an existing password for the privileged command level.
Step 4	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 5	Return to your originating procedure (NTP).	—

DLP-J294 Encrypt Passwords Using Cisco IOS Commands

Purpose	This procedure encrypts passwords using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Encryption prevents the password from being readable in the configuration file.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**service password-encryption**	Encrypts a password.

	Command or Action	Purpose
	Example: Router(config)# service password-encryption	The actual encryption process occurs when the current configuration is written or when a password is configured. The password encryption is applied to all the passwords, including authentication key passwords, privileged command password, and console and virtual terminal line access passwords. The **service password-encryption** command is used to keep unauthorized individuals from viewing your password in your configuration file.
Step 4	**end** **Example:** Router(config)# end	Returns to privileged EXEC mode.
Step 5	Return to your originating procedure (NTP).	—

Understanding Multiple Privilege Levels

CPT supports multiple privilege levels, which provide access to commands. By default, there two levels of access to commands:

- User EXEC mode (level 1)
- Privileged EXEC mode (level 15)

You can configure additional levels of access to commands, called privilege levels, to meet the needs of users while protecting the system from unauthorized access. Up to 16 privilege levels can be configured from level 0, which is the most restricted level, to level 15, which is the least restricted level.

The access to each privilege level is enabled through separate passwords, which you can specify when configuring the privilege level.

For example, if you want a certain set of users to be able to configure only certain interfaces and configuration options, you could create a separate privilege level only for specific interface configuration commands and distribute the password for that level to those users.

NTP-J104 Configure Privilege Levels Using Cisco IOS Commands

Purpose	This procedure configures privilege levels using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the listed procedures as needed.

- DLP-J295 Set the Privilege Level for a Command Using Cisco IOS Commands, on page 789
- DLP-J296 Change the Default Privilege Level for Lines Using Cisco IOS Commands, on page 790
- DLP-J297 Display Current Privilege Levels Using Cisco IOS Commands, on page 791
- DLP-J298 Log In to a Privilege Level Using Cisco IOS Commands, on page 792

Stop. You have completed this procedure.

DLP-J295 Set the Privilege Level for a Command Using Cisco IOS Commands

Purpose	This procedure configures a new privilege level for users, and associate commands with that privilege level, using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**privilege** *mode* **level** *level_number command-string* **Example:** Router(config)# privilege exec level 14 configure	Configures the specified privilege level to allow access to the specified command.
Step 4	**enable secret level** *level_number* {**0** | **5**} *password-string* **Example:** Router(config)# end	Sets the password for the specified privilege level. This is the password users will enter after entering the **enable** *level* command to access the specified level. **0** indicates that an unencrypted password string follows; **5** indicates that an encrypted password string follows.
Step 5	**exit** **Example:** Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J296 Change the Default Privilege Level for Lines Using Cisco IOS Commands

Purpose	This procedure changes the default privilege level for a given line or a group of lines, using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Router> enable	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**line** [**aux** | **console** | **tty** | **vty**] **line-number** [**ending-line-number**] **Example:** Router(config)# line vty 0 4	Enters line configuration mode for the lines.
Step 4	**privilege level** *level_number* **Example:** Router(config-line)# privilege level 10	Specifies a default privilege level for a line.
Step 5	**end** **Example:** Router(config-line)# end	Returns to global configuration mode.
Step 6	Return to your originating procedure (NTP).	—

DLP-J297 Display Current Privilege Levels Using Cisco IOS Commands

Purpose	This procedure displays the current privilege levels using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

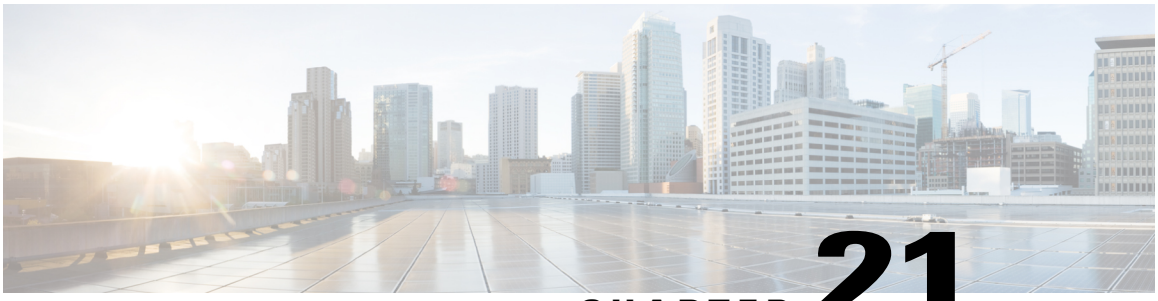
	Command or Action	Purpose
	Example: Router> enable	• Enter your password if prompted.
Step 2	**show privilege** **Example:** Router# show privilege	Displays the current privilege level you can access based on the password you used.
Step 3	Return to your originating procedure (NTP).	—

DLP-J298 Log In to a Privilege Level Using Cisco IOS Commands

Purpose	This procedure logs in to a router at a specified privilege level, using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**enable** *level* **Example:** Router# enable 12	Logs in to a specified privilege level.
Step 3	Return to your originating procedure (NTP).	—



CHAPTER 21

Configuring Cisco Discovery Protocol

This chapter describes Cisco Discovery Protocol (CDP) and the configuration examples.

Understanding CDP

Cisco Discovery Protocol (CDP) is used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to show information about the interfaces your router uses. CDP is media- and protocol-independent, and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches.

Use of SNMP with the CDP Management Information Base (MIB) allows network management applications to learn the device type and the SNMP agent address of neighboring devices, and to send SNMP queries to those devices. Cisco Discovery Protocol uses the CISCO-CDP-MIB.

CDP is enabled on the system and on the interfaces by default. If you prefer not to use the CDP device discovery capability, you can disable it with the **no cdp run** command at the system level and **no cdp enable** command at the interface level.

NTP-J66 Configure CDP

Purpose	This procedure configures CDP.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J225 Configure CDP Using Cisco IOS Commands, on page 794
- DLP-J224 Configure CDP Using CTC, on page 795

Stop. You have completed this procedure.

DLP-J225 Configure CDP Using Cisco IOS Commands

Purpose	This procedure configures CDP using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

For information on **show cdp** commands, see the *Cisco CPT Command Reference Guide*.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router# enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**[no] cdp run** **Example:** Router(config)# cdp run	Re-enables or disables CDP on the system.

	Command or Action	Purpose
Step 4	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Configures a Ten Gigabit Ethernet interface and enters interface configuration mode.
Step 5	**[no] cdp enable** **Example:** Router(config-if)# cdp enable	Re-enables or disables CDP on the interface.
Step 6	**end** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 7	Return to your originating procedure (NTP).	—

DLP-J224 Configure CDP Using CTC

Purpose	This procedure configures CDP using CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to configure CDP.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** tab.

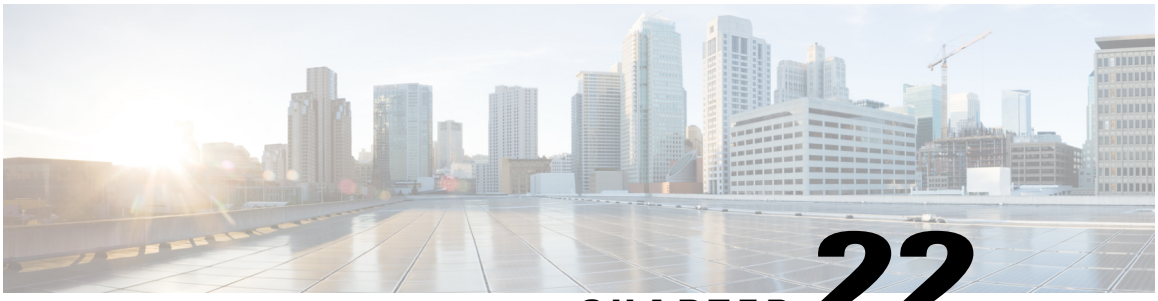
Step 4 From the left pane, click the **Port Configuration** tab.

Step 5 Check the **Enable System-Level CDP** check box to enable CDP on the CPT system.

Step 6 In the Port Configurations area, expand each slot and check the **CDP Enable** check box for each port that you want to enable CDP.

Step 7 Click **Apply** to save the configuration.

Step 8 Return to your originating procedure (NTP).



CHAPTER 22

Alarm Troubleshooting

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco CPT alarm and condition. Sections Critical (CR) Alarms, on page 799 through NR Conditions, on page 801 provide lists of CPT alarms organized by severity. Table 57: Alphabetical List of CPT Alarms and Conditions, on page 802 provides a list of alarms organized alphabetically. Table 58: Alarm Logical Object Type Definitions, on page 804 gives definitions of all CPT alarm logical objects, which are the basis of the alarm profile list in Alarm List by Logical Object Type, on page 805.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html or call at the Cisco Technical Assistance Center (1 800 553-2447).

Cisco CPT Alarms

The Cisco Carrier Packet Transport (CPT) supports the following alarms:

- Alarms specific to Cisco CPT. See Table 57: Alphabetical List of CPT Alarms and Conditions, on page 802.

Note The Switching Provider Edge (SPE) alarms are not displayed in CTC. These alarms can be viewed in an IOS console using the **show ons simple ether_alarms** command.

- Alarms that are common to Cisco CPT and Cisco ONS 15454 DWDM. See the following table. For more info, see the

  http://www.cisco.com/en/US/docs/optical/15000r10_0/dwdm/troubleshooting/guide/b_454d98_10_ts.html.

Table 52: Cisco ONS 15454 Alarms Supported by CPT

CTNEQPT-MISMATCH (NA)	MANRESET (NA)
DIAG (CR)	MEA (CR)
EQPT (CR)	MEM-GONE (MJ)
EQPT-DEGRADE (MN)	MEM-LOW (MN)
EXCCOL (MN)	OPEN-SLOT (NA)
FAILTOSW (NA)	PEER-NORESPONSE (MJ)
FAPS-CONFIG-MISMATCH (MN)	PROTNA (MN)
FORCED-REQ (NA)	PWR-FAIL-A (MN)
FP-LINK-LOSS (MN)	PWR-FAIL-B (MN)
FTA-MISMATCH (NA)	PWR-FAIL-RET-A (MN)
HI-LASERBIAS (MN)	PWR-FAIL-RET-B (MN)
HI-LASERTEMP (MN)	RS-EOC (MN)
HI-TXPOWER (MN)	RS-TIM (CR)
HITEMP (MN)	RUNCFG-SAVENEED (NA)
IMPROPRMVL (CR)	SFTWDOWN (MN)
INHSWPR (NA)	SW-MISMATCH (NA)
INHSWWKG (NA)	UNEQ-P (CR)
LO-LASERBIAS (MN)	VOA-DISABLED (CR)
LO-LASERTEMP (MN)	WKSWBK (NA)
LO-TXPOWER (MN)	WKSWPR (NA)
LOCKOUT-REQ (NA)	WORK-QUEUE-FULL (NA)
DB-LOSS (CR)	
DB-LOSS (CR)	

CPT Alarm Indexes

The following tables group alarms and conditions by their default severities in the Cisco CPT system.

Note The CTC default alarm profile contains some alarms or conditions that are not currently implemented but are reserved for future use.

Note The CTC default alarm profile in some cases contains two severities for one alarm (for example, MJ/MN). The platform default severity comes first (in this example, MJ), but the alarm can be demoted to the second severity in the presence of a higher-ranking alarm.

Critical (CR) Alarms

The following table alphabetically lists Critical (CR) alarms.

Table 53: Critical Alarms List

DB-LOSS (PTS)	SAT-FAN-FAIL (EQPT)
LIC-EXPIRED (EQPT)	SAT-FAN-MEA (EQPT)
LIC-MISSING (DWDM_TRUNK, DWDM_CLIENT)	SAT-FAN-MFGMEM (EQPT)
PROTNA (EQPT)	SAT-FAN-MISSING (EQPT)
PTS-FAIL (PTS)	SAT-HITEMP (EQPT)
RING-CFG-OUT-OF-SYNC (NE)	SAT-IHITEMP (EQPT)
SAT-COMM-FAIL (EQPT)	SAT-IMPROPER-CONFIG (EQPT)
SAT-FAN DEGRADE (EQPT)	

Major Alarms (MJ)

The following table alphabetically lists Major (MJ) alarms.

Table 54: Major Alarms List

DH-SW-VER-MISM (NE)	RESOURCE-ALLOC-FAIL (EQPT)
EFP-FAIL (PORT)	
EFP-FAIL (PORT)	
EQPT_FAIL (EQPT)	SAT-BAT-FAIL-A (EQPT)
IMPROPRMVL (EQPT)	SAT-BAT-FAIL-B (EQPT)
LIC-EXPIRING-SHORTLY (EQPT)	SINGLE-SPAN-FAIL (RING)
LIC-EXPIRING-SOON (EQPT)	TE-TUNNEL-DOWN (PTS)
LOS (TDM)	TP-TUNNEL-DOWN (PTS)
PRT-LOC-PW-NOT-FWD (PTS)	WKG-LOC-PW-NOT-FWD (PTS)
PRT-PW-LOC-AC-RX-FLT (PORT)	WKG-PW-LOC-AC-RX-FLT (PORT)
PRT-PW-LOC-AC-TX-FLT (PORT)	WKG-PW-LOC-AC-TX-FLT (PORT)
PW-DOWN (PORT)	

Minor Alarms (MN)

The following table alphabetically lists Minor (MN) alarms.

Table 55: Minor Alarms List

BFD-DOWN (PORT)	PW-WKSWPR (PORT)
CUTOVER (EQPT)	RESOURCES-GONE (EQPT)
EVAL-LIC (EQPT)	RESOURCES-LOW (EQPT)
MAC-BD-LIMT-REACHED (PTS)	SAT-ACT-LINK-FAIL (FAC)
MAC-SYS-LIMT-REACHED (PTS)	TEMP-LIC (EQPT)

PROT-CONFIG-MISMATCH (EQPT)	WKG-LSP-DOWN (PORT)
PRT-LSP-DOWN (PORT)	WKG-LSP-LKR (FAC)
PRT-LSP-LKR (FAC)	WKG-PW-CC-DOWN (PORT)
PRT-PW-CC-DOWN (PORT)	WKG-PW-CP-DOWN (PORT)
PRT-PW-CP-DOWN (PORT)	--

NA Conditions

The following table alphabetically lists Not Alarmed (NA) conditions.

Table 56: NA Conditions List

DH-OUT-OF-SYNC(NE)	RDI (TDM)
FACILITY LOOPBACK(TDM)	TERMINAL LOOPBACK (TDM)
PRT-LSP-LDI (PORT, FAC)	TP-WKSPWR (PORT)
PRT-PW-REM-AC-RX-FLT (PORT)	WKG-LSP-LDI (PORT, FAC)
PRT-PW-REM-AC-TX-FLT (PORT)	WKG-PW-REM-AC-RX-FLT (PORT)
PRT-REM-PW-NOT-FWD (PTS)	WKG-PW-REM-AC-TX-FLT (PORT)
PRT-TP-LOCKOUT (PORT)	WKG-REM-PW-NOT-FWD (PTS)
RAI (TDM)	WKG-TP-LOCKOUT (PORT)

NR Conditions

The following is the list of Not Reported (NR) conditions.

- OTUK-BIAE (DWDM_TRUNK, DWDM_CLIENT)
- AIS (TDM)

Alarms and Conditions Listed By Alphabetical Entry

The following table alphabetically lists all CPT alarms and conditions.

Table 57: Alphabetical List of CPT Alarms and Conditions

AIS (TDM)	PW-WKSWPR (PORT)
BFD-DOWN (PORT)	
CUTOVER (EQPT)	RAI (TDM)
DB-LOSS (PTS)	RDI (TDM)
DH-OUT-OF-SYNC (EQPT)	RESOURCES-GONE (EQPT)
DH-SW-VER-MISM (NE)	RESOURCES-LOW (EQPT)
EQPT-FAIL (EQPT)	RESOURCE-ALLOC-FAIL (EQPT)
EFP-FAIL (PORT)	RING-CFG-OUT-OF-SYNC (NE)
FACILITY LOOPBACK (TDM)	SAT-ACT-LINK-FAIL (FAC)
IMPROPRMVL (EQPT)	SAT-BAT-FAIL-A (EQPT)
LIC-EXPIRED (EQPT)	SAT-BAT-FAIL-B (EQPT)
LIC-EXPIRING-SHORTLY (EQPT)	SAT-COMM-FAIL (EQPT)
EVAL-LIC (EQPT)	SAT-FAN-DEGRADE (EQPT)
LIC-EXPIRING-SOON (EQPT)	SAT-FAN-FAIL (EQPT)
LIC-MISSING (DWDM-CLIENT)	SAT-FAN-MEA (EQPT)
LIC-MISSING (DWDM-TRUNK)	SAT-FAN-MFGMEM (EQPT)
LOS (TDM)	SAT-FAN-MISSING (EQPT)
MAC-BD-LIMT-REACHED (PTS)	SAT-HITEMP (EQPT)
MAC-SYS-LIMT-REACHED (PTS)	SAT-IHITEMP (EQPT)
MEA (EQPT)	SAT-IMPROPER-CONFIG (EQPT)
MULTIPLE-SPAN-FAIL (RING)	SINGLE-SPAN-FAIL (RING)
OTUK-BIAE (DWDM-CLIENT)	
OTUK-BIAE (DWDM-TRUNK)	TERMINAL LOOPBACK (TDM)
PROT-CONFIG-MISMATCH (EQPT)	TOPO-MIS-CONF (RING)

PRT-LOC-PW-NOT-FWD (PTS)	TE-TUNNEL-DOWN (PTS)
PRT-LSP-DOWN (PORT)	TEMP-LIC (EQPT)
PRT-LSP-LDI (PORT)	TP-TUNNEL-DOWN (PTS)
PRT-LSP-LDI (FAC)	TP-WKSPWR (PORT)
PRT-LSP-LKR (FAC)	WKG-LOC-PW-NOT-FWD (PTS)
PRT-PW-CC-DOWN (PORT)	WKG-LSP-DOWN (PORT)
PRT-PW-CP-DOWN (PORT)	WKG-LSP-LDI (PORT)
PRT-PW-LOC-AC-RX-FLT (PORT)	WKG-LSP-LDI (FAC)
PRT-PW-LOC-AC-TX-FLT (PORT)	WKG-LSP-LKR (FAC)
PRT-PW-REM-AC-RX-FLT (PORT)	WKG-PW-CC-DOWN (PORT)
PRT-PW-REM-AC-TX-FLT (PORT)	WKG-PW-CP-DOWN (PORT)
PRT-REM-PW-NOT-FWD (PTS)	WKG-PW-LOC-AC-RX-FLT (PORT)
PRT-TP-LOCKOUT (PORT)	WKG-PW-LOC-AC-TX-FLT (PORT)
	WKG-PW-REM-AC-RX-FLT (PORT)
PROTNA (EQPT)	WKG-PW-REM-AC-TX-FLT (PORT)
	WKG-REM-PW-NOT-FWD (PTS)
PTS-FAIL (PTS)	
PW-DOWN (PORT)	WKG-TP-LOCKOUT (PORT)

Alarm Logical Objects

The CTC alarm profile list organizes all alarms and conditions according to the logical objects they are raised against. One alarm can appear in multiple entries. It can be raised against multiple objects.

Alarm profile list objects are defined in the following table.

Note Alarm logical object names can appear as abbreviated versions of standard terms used in the system and the documentation. Logical object names or industry-standard terms are used within the entries as appropriate.

Alarm Logical Objects

The following table lists all the logical alarm objects used in this chapter.

Table 58: Alarm Logical Object Type Definitions

Logical Object	Definition
DWDM_CLIENT	The client port on the optical or DWDM card carrying the high-speed signal.
DWDM_TRUNK	The trunk port on the optical or DWDM card carrying the high-speed signal.
EQPT	A card, its physical objects, and its logical objects as they are located in any of the noncommon card slots. The EQPT object is used for alarms that refer to the card itself and all other objects on the card including ports, and lines.
FAC	Facility payload.
NE	The entire network element.
PORT	Port on the fabric card, line card, or CPT 50 panel.
PTS	Packet transport system.
RING	Ring is a topology of the CPT 50s connected in a linear or ring fashion, subtending from the CPT 600 or CPT 200 chassis.
TDM	Time-division Multiplexing.

Note The following restrictions and limitations apply to TDM alarm:

- For DS1 structured emulation signal if LOF alarm is triggered in near end, only LOF alarm will be raised in near end TDM cloud. RDI alarm will not get raised.
- For E1 structured emulation signal if LOF alarm is triggered from near end TDM cloud, LOF alarm will be raised in near end. In addition, RDI alarm will also get raised in On and Off pattern .
- For E1 structured emulation signal if LOS alarm is triggered in near end, only LOS alarm will be raised in near end TDM cloud. RDI alarm will not be raised.
- For DS1 unstructured emulation signal if LOS alarm is triggered in near end, both LOS and RDI alarms will be raised in near end TDM cloud.
- For DS3 and E3 unstructured emulation signal if AIS alarm is triggered in near end, both AIS and RDI alarms will be raised in near end TDM cloud.

Alarm List by Logical Object Type

Lists all the alarms and logical objects as they are given in the system alarm profile. The list entries are organized by logical object name and then by alarm or condition name. Where appropriate, the alarm entries also contain troubleshooting procedures.

Table 59: Alarm List by Logical Object in Alarm Profile

DWDM_CLIENT: LIC-MISSING (CR)	PORT: PRT-PW-CC-DOWN (MN)
DWDM_CLIENT: OTUK-BIAE (NR)	PORT: PRT-PW-CP-DOWN (MN)
DWDM_TRUNK: LIC-MISSING (CR)	PORT: PRT-PW-LOC-AC-RX-FLT (MJ)
DWDM_TRUNK: OTUK-BIAE (NR)	PORT: PRT-PW-LOC-AC-TX-FLT (MJ)
EQPT: CUTOVER (MN)	PORT: PRT-PW-REM-AC-RX-FLT (NA)
EQPT: DH-OUT-OF-SYNC (MJ)	PORT: PRT-TP-LOCKOUT (NA)
EQPT: EVAL-LIC (MN)	PORT: PW-DOWN (MJ)
EQPT: EQPT-FAIL (MJ)	
EQPT: IMPROPRMVL (MJ)	PORT: PW-WKSWPR (MN)
EQPT: LIC-EXPIRED (CR)	PORT: WKG-LSP-DOWN (MN)
EQPT: LIC-EXPIRING-SHORTLY (MJ)	PORT: WKG-LSP-LDI (NA)
EQPT: LIC-EXPIRING-SOON (MJ)	PORT: WKG-PW-CC-DOWN (MN)
EQPT: PROT-CONFIG-MISMATCH (MN)	PORT: WKG-PW-CP-DOWN (MN)
	PORT: WKG-PW-LOC-AC-RX-FLT (MJ)
EQPT: RESOURCES-GONE (MN)	PORT: WKG-PW-LOC-AC-TX-FLT (MJ)
EQPT: RESOURCES-LOW (MN)	PORT: WKG-PW-REM-AC-RX-FLT (NA)
EQPT: RESOURCE-ALLOC-FAIL (MJ)	PORT: WKG-PW-REM-AC-TX-FLT (NA)
EQPT: SAT-BAT-FAIL-A (MJ)	
EQPT: SAT-BAT-FAIL-B (MJ)	PORT: WKG-TP-LOCKOUT (NA)
EQPT: SAT-COMM-FAIL (CR)	PTS: PRT-LOC-PW-NOT-FWD (MJ)
EQPT: SAT-FAN-DEGRADE (CR)	PTS: PRT-REM-PW-NOT-FWD (NA)

EQPT: SAT-FAN-FAIL (CR)	PTS: WKG-LOC-PW-NOT-FWD (MJ)
EQPT: SAT-FAN-MEA (CR)	PTS: WKG-REM-PW-NOT-FWD (NA)
EQPT: SAT-FAN-MISSING (CR)	PTS: TP-TUNNEL-DOWN (MJ)
EQPT: SAT-HITEMP (CR)	PTS: TE-TUNNEL-DOWN (MJ)
EQPT: SAT-IHITEMP (CR)	PTS: MAC-BD-LIMT-REACHED (MN)
EQPT: SAT-IMPROPER-CONFIG (CR)	PTS: MAC-SYS-LIMT-REACHED (MN)
EQPT: TEMP-LIC (MN)	PTS: PTS-FAIL (CR)
FAC: PRT-LSP-LDI (NA)	
FAC: PRT-LSP-LKR (MN)	RING: MULTIPLE-SPAN-FAIL (CR)
FAC: SAT-ACT-LINK-FAIL (MN)	RING: SINGLE-SPAN-FAIL (MJ)
FAC: WKG-LSP-LDI (NA)	RING: TOPO-MIS-CONF (CR)
FAC: WKG-LSP-LKR (MN)	TDM: AIS (NR)
NE: DH-OUT-OF-SYNC (NA)	TDM: FACILITY LOOPBACK (NA)
NE: RING-CFG-OUT-OF-SYNC (CR)	TDM: LOS (MJ)
PORT: BFD-DOWN (MN)	TDM: RAI (NA)
PORT: EFP-FAIL (MJ)	TDM: RDI (NA)
PORT: PRT-LSP-DOWN (MN)	TDM: TERMINAL LOOPBACK (NA)
PORT: PRT-LSP-LDI (NA)	TDM:LOF(CR)

NTP -J125 Suppress Alarms in CTC

Purpose	This procedure suppresses alarms in CTC.
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 NTP-J22 Log into CTC, on page 15 procedure at a node where you want to suppress alarms.

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

Step 3 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 4 From the left pane, click **Alarm Profiles**. Perform the following tasks as required:

a) To suppress all the alarms at a specific node:

1. On the **Alarm Behavior** tab, choose **Default** from the Node Profile drop-down list.
2. Check the **Suppress Alarms** check box.
3. Click **Apply**.

b) To suppress all the alarms at a specific card:

1. On the **Alarm Behavior** tab, check the check box in the Suppress Alarm column next to the required card.
2. Repeat the earlier step for each card where you want to suppress the alarms.
3. Click **Apply**.

c) To suppress alarms irrespective of a node or card:

1. Click the **Alarm Profile Editor** tab.
2. Click **New**. The New Profile dialog box appears.
3. Enter a name for the alarm profile in the New Profile Name field.
4. Click **OK**. The new alarm profile appears on the **Alarm Profile Editor** tab.
5. Under the <*Alarm Profile Name*> column, choose **NA** or **NR** from the drop-down list that is displayed next to each alarm.
6. Repeat the earlier step for all the alarms that you want to suppress.
7. From the Node Names area, choose a node where you want to store the alarm profile.
8. Click **OK**.
9. Click the **Alarm Behavior** tab.
10. From the Node Profile drop-down list, choose the newly created alarm profile to suppress all the alarms that occur at the node where the alarm profile is stored.

Stop. You have completed this procedure.

Trouble Characterizations

The Cisco CPT system reports trouble by utilizing standard alarm and condition characteristics, standard severities, and graphical user interface (GUI) state indicators. These notifications are described in the following paragraphs.

The system reports trouble notifications as alarms and status or descriptive notifications (if configured to do so) as conditions in the CTC Alarms window. Alarms typically signify a problem that the user needs to remedy, such as a loss of signal. Conditions do not necessarily require troubleshooting.

Alarm Characteristics

The Cisco CPT system uses standard alarm entities to identify what is causing trouble. All alarms stem from hardware, software, environment, or operator-originated problems whether or not they affect service. Current alarms for the network, CTC session, node, or card are listed in the Alarms tab. (In addition, cleared alarms are also found in the History tab.)

Condition Characteristics

Conditions include any problem detected on an Cisco CPT shelf. They can include standing or transient notifications. A snapshot of all current raised, standing conditions on the network, node, or card can be retrieved in the CTC Conditions window. (In addition, some but not all cleared conditions are also found in the History tab.)

Severity

The Cisco CPT system uses standard severities for alarms and conditions: Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), and Not Reported (NR). These are described below:

- A Critical (CR) alarm generally indicates severe, Service-Affecting trouble that needs immediate correction.
- A Major (MJ) alarm is a serious alarm, but the trouble has less impact on the network.
- Minor (MN) alarms generally are those that do not affect service.
- Not Alarmed (NA) conditions are information indicators. They could or could not require troubleshooting, as indicated in the entries.
- Not Reported (NR) conditions occur as a secondary result of another event. These conditions do not in themselves require troubleshooting, but are to be expected in the presence of primary alarms.

Severities can be customized for an entire network or for single nodes, from the network level down to the port level by changing or downloading customized alarm profiles.

Service Effect

Service-Affecting (SA) alarms are those that interrupt servicecould be Critical (CR), Major (MJ), or Minor (MN) severity alarms. Service-Affecting (SA) alarms indicate service is affected. Non-Service-Affecting (NSA) alarms always have a Minor (MN) default severity.

State

The Alarms or History tab State (ST) column indicate the disposition of the alarm or condition as follows:

- A raised (R) event is one that is active.
- A cleared (C) event is one that is no longer active.
- A transient (T) event is one that is automatically raised and cleared in CTC during system changes such as user login, logout, loss of connection to node/shelf view, etc. Transient events do not require user action.

Trouble-Clearing Procedures

This section list alarms alphabetically and includes some conditions commonly encountered when troubleshooting alarms. The severity, description, and troubleshooting procedure accompany each alarm and condition.

Note When you check the status of alarms for cards, ensure that the alarm filter icon in the lower right corner of the GUI is not indented. If it is, click it to turn it off. When you are done checking for alarms, you can click the alarm filter icon again to turn filtering back on.

Note When checking alarms, ensure that alarm suppression is not enabled on the card or port.

AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TDM

The Alarm Indication Signal (AIS) alarm is raised when receiving of signal on an intermediate node fails.

Clear the AIS Alarm

Procedure

Clear the signal failure.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

BFD-DOWN

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: PORT

The Bidirectional Forward Detection Down (BFD-DOWN) alarm is raised when the bidirectional forward detection (BFD) is configured and label-switched path (LSP) is down.

Clear the BFD-DOWN Alarm

Procedure

Perform any of the following, as appropriate:

- Activate the LSP.
- Verify that LSP does not have any errors.
- Verify that BFD is configured at both ends of the tunnel.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

CUTOVER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Planned Switchover (CUTOVER) alarm is raised when a planned switchover of the fabric card from working card to protect card or protect card to working card occurs.

Clear the CUTOVER Alarm

Procedure

The alarm clears after the fabric card switchover is complete.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

DB-LOSS

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: PTS

The DB LOSS alarm is raised when a PTF card notifies the TNC card to clear the database.

Clear the DB-LOSS Alarm

Procedure

Reload the PTF and the TNC card.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http:/

/www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

DH-OUT-OF-SYNC

Default Severity: Not Alarmed (NA), Service-Affecting (SA)

Logical Object: PORT

The DH-OUT-OF-SYNC alarm is raised when the PRC is used to configure the services on a CPT 50 in a dual-homed ring.

Clear the DH-OUT-OF-SYNC Alarm

Procedure

N/A. This alarm will appear in the Condition tab.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

DH-SW-VER-MISM

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: NE

The DH-SW-VER-MISM alarm is raised when the WRC and the PRC are on the different software releases.

Clear the DH-SW-VER-MISM Alarm

Procedure

Load same software releases on the WRC and the PRC.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

EFP-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: PORT

The Ethernet Flow Point Failed (EFP-FAIL) alarm is raised when the Ethernet flow point (EFP) fails due to incomplete hardware provisioning or when the interface on which the EFP present is down .

Clear the EFP-FAIL Alarm

Procedure

Activate the EFP with correct hardware provisioning.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

EQPT-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: EQPT

The Equipment Failure (EQPT_FAIL) alarm is raised:

- When a CPT 50 card is provisioned with the CPT 200 or CPT 600, but physically it is not present.
- When the Hardware Table parity errors present on a particular card.
- When the card detects defects during self diagnostics (FMEA).

Clear the EQPT-FAIL Alarm

Procedure

Attach the CPT 50 card with the CPT 200 or CPT 600 or perform soft reset for the card.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

EVAL-LIC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Evaluation License (EVAL-LIC) alarm is raised to indicate that an valid evaluation license is in use.

Clear the EVAL-LIC Alarm

Procedure

Procure and install a permanent license. For more information on installing a license, see the Licensing Configuration Guide.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Facility Loopback

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TDM

The Facility Loopback alarm is raised when the software facility (line) loopback is active for a port.

Clear the Facility Loopback Alarm

Procedure

Correct the facility (line) loopback configuration for a port.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

IMPROPRMVL

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: EQPT,PPM

The Improper Removal (IMPROPRMVL) alarm is raised when all provisioned nodes are not available during multiple span failure.

Clear the IMPROPRMVL Alarm

Procedure

Make all the provisioned nodes, available.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LICENSE-EXPIRED

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT

The License Expired (LICENSE-EXPIRED) alarm is raised when an evaluation license or a temporary license expires and there is no other valid license installed on the device.

Traffic continues to flow even after this alarm is raised. However, the traffic will stop once . To prevent traffic disruption, ensure that a valid license is installed on the device.

Traffic on the base functionality is not affected when LICENSE-EXPIRED alarm is raised.

Clear the LICENSE-EXPIRED Alarm

Procedure

Procure and install a permanent license. For more information on installing a license, see the Licensing Configuration guide.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LIC-EXPIRING-SOON

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: EQPT

The License Expiring Soon (LIC-EXPIRING-SOON)alarm is raised when the cumulative validity period of the existing evaluation and temporary licenses is in the range of 1 to 14 days.

An evaluation license and multiple temporary licenses can co-exist on a device and the validity period of each license can vary.

Clear the LIC-EXPIRING-SOON Alarm

Procedure

Procure and install a permanent license. For more information on installing a license, see the Licensing Configuration guide.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LIC-EXPIRING-SHORTLY

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: EQPT

The License Expiring Shortly (LIC-EXPIRING-SHORTLY) alarm is raised when the cumulative validity period of the existing evaluation and temporary licenses is in the range of 0 to 24 hours.

An evaluation license and multiple temporary licenses can co-exist on a device and the validity period of each license can vary.

Clear the LIC-EXPIRING-SHORTLY Alarm

Procedure

Procure and install a permanent license. For more information on installing a license, see the Licensing Configuration guide.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LIC-MISSING

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: PORT

The License Missing (LIC-MISSING) alarm is raised when a valid license on the expires.

Clear the LIC-MISSING Alarm

Procedure

Procure and install a valid license for the . For more information on installing a license, see the Licensing Configuration guide.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LoS

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: TDM

The LoS alarm is raised when the signal is not received or low frequency signal is received.

Clear the LoS Alarm

Procedure

Rectify the reason of the signal failure.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

MAC-BD-LIMT-REACHED

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: PTS

The MAC Bridge Domain Limit Reached (MAC-BD-LIMT-REACHED) alarm is raised when the MAC address learnt on the bridge domain has reached a limit of 128,000.

Clear the MAC-BD-LIMT-REACHED Alarm

Procedure

Reduce the MAC address size on the bridge domain.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

MAC-SYS-LIMT-REACHED

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: PTS

The MAC System Limit Reached (MAC-SYS-LIMT-REACHED) alarm is raised when the system MAC address limit of 256,000 is reached.

Clear the MAC-SYS-LIMT-REACHED Alarm

Procedure

Reduce the system MAC address size to less than 256,000.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

MULTIPLE-SPAN-FAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: RING

The Multiple Span Failure (MULTIPLE-SPAN-FAIL) alarm is raised when multiple links of a ring are down.

Clear the MULTIPLE-SPAN-FAIL Alarm

Procedure

Activate those links of the ring that are down.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

OTUK-BIAE Alarm

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: DWDM-CLIENT, DWDM-TRUNK

The Backward Incoming Alignment Error (OTUK-BIAE) alarm is raised when the incoming OTU2 frame contain backward incoming alignment error bits.

Clear the OTUK-BIAE Alarm

Procedure

Clear the backward incoming alignment error bits from the incoming OTU2 frame.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PROT-CONFIG-MISMATCH

Default Severity: Major (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Protection Card Configuration Mismatch (PROT-CONFIG-MISMATCH) alarm occurs when the protect card configuration does not match the active card configuration.

Clear the PROT-CONFIG-MISMATCH Alarm

Procedure

Configure the protect card similar to the working card.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PROTNA

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: EQPT

The PROTNA alarm is raised when the GCC link between Working Ring Controller and Protecting Ring Controller goes down.

Clear the PROTNA Alarm

Procedure

Activate the GCC link.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PROV-FAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT

The Provisioning Failed (PROV-FAIL) alarm is raised when the Cisco IOS sends a negative acknowledgment for a received provisioning request.

Clear the PROV-FAIL Alarm

Perform any of the following, as appropriate:

- Reset the uplink card.
- Perform a switchover of the uplink card.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or log into http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html to obtain a directory of toll-free Technical Support numbers for your country in order to report a Service-affecting (SA) problem.

PRT-LOC-PW-NOT-FWD

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: PTS

The Protect Local Pseudowire Not Forwarding (PRT-LOC-PW-NOT-FWD) alarm is raised when the local protect pseudowire is not forwarding traffic.

Clear the PRT-LOC-PW-NOT-FWD Alarm

Procedure

The alarm clears when the local protect pseudowire starts forwarding traffic.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

PRT-LSP-DOWN

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: PORT

The Protect Label-Switched Path Down (PRT-LSP-DOWN) alarm is raised when the protect label-switched path (LSP) fails on the port.

Clear the PRT-LSP-DOWN Alarm

Procedure

Perform any of the following, as appropriate:

- Verify that the LSP does not have any connectivity issues.
- Administratively shutdown the tunnel. Traffic drops when the tunnel is administratively shut down.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PRT-LSP-LDI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: PORT

The Protect Label-Switched Path Link Defect Indication (PRT-LSP-LDI) alarm is raised when the protect label-switched path (LSP) receives an LSP link defect indication signal. The PRT-LSP-LDI alarm suppresses the PRT-LSP-LKR alarm, if present.

Clear the PRT-LSP-LDI Alarm

Procedure

Perform any of the following, as appropriate:

- Verify that the LSP does not have any connectivity issues.
- Administratively shutdown the tunnel. Traffic drops when the tunnel is administratively shut down.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PRT-LSP-LKR

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: FAC

The Protect Label-Switched Path Lock Report (PRT-LSP-LKR) alarm is raised when an interface is administratively locked and a lockout request (LKR) is generated on the near reachable endpoint. The PRT-LSP-LKR alarm suppresses the PRT-LSP-LDI alarm, if present.

Clear the PRT-LSP-LKR Alarm

Procedure

Perform any of the following, as appropriate:

- Clear the lock out condition on the interface and LSP.
- Verify that the LSP does not have any connectivity issues.
- Administratively shutdown the tunnel. Traffic drops when the tunnel is administratively shut down.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PRT-PW-CC-DOWN

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: PORT

The Protect Pseudowire Continuity Check Down (PRT-PW-CC-DOWN) alarm is raised when the virtual circuit connectivity verification (VCCV) BFD fails on the port or when the port-channel is configured as attachment circuit (AC) port.

Clear the PRT-PW-CC-DOWN Alarm

Procedure

Activate the protect pseudowire continuity check.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PRT-PW-CP-DOWN

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: PORT

The Protect Pseudowire Control Plane Down (PRT-PW-CP-DOWN) alarm is raised on the port when the control plane of the protect pseudowire fails.

Clear the PRT-PW-CP-DOWN Alarm

Procedure

Activate the control plane of the protect pseudowire.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PRT-PW-LOC-AC-RX-FLT

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: PORT

The Protect Pseudowire Local AC RX Port Fault (PRT-PW-LOC-AC-RX-FLT) alarm is raised when the port fault on the receive side is detected on the local attachment circuit of the protect pseudowire.

Clear the PRT-PW-LOC-AC-RX-FLT Alarm

Procedure

Remove the port fault on the receive side that is detected on the local attachment circuit of the protect pseudowire.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http:/

/www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

PRT-PW-LOC-AC-TX-FLT

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: PORT

The Protect Pseudowire Local AC TX Port Fault (PRT-PW-LOC-AC-TX-FLT) alarm is raised when the port fault on the transmit side is detected on the local attachment circuit of the protect pseudowire.

Clear the PRT-PW-LOC-AC-TX-FLT Alarm

Procedure

Remove the port fault on the transmit side that is detected on the local attachment circuit of the protect pseudowire.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

PRT-PW-REM-AC-RX-FLT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: PORT

The Protect Pseudowire Remote AC RX Port Fault (PRT-PW-REM-AC-RX-FLT) alarm is raised when the port fault on the receive side is detected on the remote attachment circuit of the protect pseudowire.

Clear the PRT-PW-REM-AC-RX-FLT Alarm

Procedure

Remove the port fault on the receive side that is detected on the remote attachment circuit of the protect pseudowire.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PRT-PW-REM-AC-TX-FLT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: PORT

The Protect Pseudowire Remote AC TX Port Fault (PRT-PW-REM-AC-TX-FLT) alarm is raised when the port fault on the transmit side is detected on the remote attachment circuit of the protect pseudowire.

Clear the PRT-PW-REM-AC-TX-FLT Alarm

Procedure

Remove the port fault on the transmit side that is detected on the remote attachment circuit of the protect pseudowire.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PRT-PW-RX-FLT

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: PORT

The Protected Pseudowire RX Fault (PRT-PW-RX-FLT) alarm is raised when the state of the MPLS-TP tunnel, on which a protected pseudowire is created, is changed to DOWN.

Clear the PRT-PW-RX_FLT Alarm

Perform any of the following, as appropriate:

- Change the state of the MPLS-TP tunnel to UP.
- Delete the pseudowire.

If the condition does not clear, 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).

PRT-REM-PW-NOT-FWD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: PTS

The Protect Remote Pseudowire Not Forwarding (PRT-REM-PW-NOT-FWD) alarm is raised when the remote protect pseudowire is not forwarding traffic.

Clear the PRT-REM-PW-NOT-FWD Alarm

Procedure

The alarm clears when the remote protect pseudowire starts forwarding traffic.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PRT-TP-LOCKOUT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: PORT

The Protect Transport Profile Lockout (PRT-TP-LOCKOUT) alarm is raised when the LOCK-OUT request is set to ON for the protect Multiprotocol Label Switching - Transport Profile (MPLS-TP).

Clear the PRT-TP-LOCKOUT Alarm

Procedure

Set the LOCK-OUT request to OFF for the protect MPLS-TP.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PTS-FAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT, SLOT

The Packet Transport Service Failed (PTS-FAIL) alarm is raised under the following conditions:

- When there is no active fabric card present.
- When the fabric card is not up and working.

Note When PTS-FAIL alarm is present on a node, ring related alarms are not valid for that node. Also Show Actual Topology will not display the correct information.

Clear the PTS-FAIL Alarm

Procedure

Reset and activate at least one fabric card.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

PW-DOWN

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: PORT

The Pseudowire Down (PW-DOWN) alarm is raised on the port when both the working and protect pseudowire has one of the following alarms:

- WKG-PW-CP-DOWN
- PRT-PW-CP-DOWN
- WKG-PW-CC-DOWN
- PRT-PW-CC-DOWN
- WKG-PW-LOC-AC-TX-FLT
- PRT-PW-LOC-AC-TX-FLT
- WKG-LOC-PW-NOT-FWD
- PRT-LOC-PW-NOT-FWD

Clear the PW-DOWN Alarm

Procedure

Clear the following alarms, as appropriate:

- Clear the WKG-PW-CP-DOWN Alarm
- Clear the PRT-PW-CP-DOWN Alarm
- Clear the WKG-PW-CC-DOWN Alarm
- Clear the PRT-PW-CC-DOWN Alarm
- Clear the WKG-PW-LOC-AC-TX-FLT Alarm
- Clear the PRT-PW-LOC-AC-TX-FLT Alarm
- Clear the WKG-LOC-PW-NOT-FWD Alarm
- Clear the PRT-LOC-PW-NOT-FWD Alarm

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

PW-DP-FLT

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: PORT

The Pseudowire Dataplane Fault (PW-DP-FLT) alarm is raised when the state of the MPLS-TP tunnel, on which a pseudowire is created, is changed to DOWN.

Clear the PW-DP-FLT Alarm

Perform any of the following, as appropriate:

- Change the state of the MPLS-TP tunnel to UP.
- Delete the pseudowire.

If the condition does not clear, 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).

PW-WKSWPR

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: PORT

The Pseudowire Traffic Switched to Protection (PW-WKSWPR) alarm is raised on the port when the pseudowire traffic is switched from the working path to the protected path.

Clear the PW-WKSWPR Alarm

Procedure

Switch the pseudowire traffic from the protected path to the working path.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

RAI

Default Severity: Not Affected(NA), Non-Service-Affecting (NSA)

Logical Object: TDM

The Remote Alarm Indication (RAI) alarm is raised when the received signal is degraded.

Clear the RAI Alarm

Procedure

The alarm gets clear when the high frequency signals are received.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

RDI

Default Severity: Not Affected (NA), Non-Service-Affecting (NSA)

Logical Object: TDM

The Remote Defect Indication (RDI) alarm is raised when the received signal is degraded.

Clear the RDI Alarm

Procedure

The alarm gets clear when the high frequency signals are received.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

RESOURCE-ALLOC-FAIL

Default Severity: Minor (MJ), Service-Affecting (SA)

Logical Object: EQPT

The Resource Allocation Failed (RESOURCE-ALLOC-FAIL) alarm is raised when Quality of Service (QoS) cannot be configured due to lack of resources.

Clear the RESOURCE-ALLOC-FAIL Alarm

Procedure

Find the resources that are using more memory and free up the memory.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

RESOURCES-GONE

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The No More Resources Available (RESOURCES-GONE) alarm is raised, if any of the following condition is there:

- If the resource memory is used completely.
- When resources cannot be configured.

- When SEU FPGA bit error detected on the PTF card. To confirm the SEU FPGA bit error, connect to the respective PTF card using IOS command and check for any alarm on LEONE FPGA using the command “fmea alarm”.

Clear the RESOURCES-GONE Alarm

Procedure

Perform any of the following, as appropriate:

- Find the resources that are using more memory and free up the memory.
- Incase of SEU FPGA bit error, reset the PTF card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

RESOURCES-LOW

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Running Low on Resources (RESOURCES-LOW) alarm is raised if the resource memory is very low or when more resources cannot be configured.

Clear the RESOURCES-LOW Alarm

Procedure

Find the resources that are using more memory and free up the memory.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

RING-CFG-OUT-OF-SYNC

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: NE

The RING-CFG-OUT-OF-SYNC alarm is raised when the configurations between the WRC and PRC are not synched.

Clear the RING-CFG-OUT-OF-SYNC Alarm

Procedure

Synched the configurations of both the WRC and the PRC.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SAT-ACT-LINK-FAIL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: FAC

The CPT 50 Panel Active Link Failure (SAT-ACT-LINK-FAIL) alarm is raised when the Satellite Discovery Protocol fails on an active link between the line card and the CPT 50 panel fails.

Clear the SAT-ACT-LINK-FAIL Alarm

Procedure

Activate the link between the line card and the CPT 50 panel.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SAT-BAT-FAIL-A

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: EQPT

The CPT 50 Panel Battery Failure A (SAT-BAT-FAIL-A) alarm is raised when the battery A fails. This could be because the battery is removed or is not operational.

Clear the SAT-BAT-FAIL-A Alarm

Procedure

Step 1 At the site, verify if the battery is present and operational.

Step 2 Remove the power cable from the faulty supply. Reverse the power cable installation procedure.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http:/

/www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SAT-BAT-FAIL-B

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: EQPT

The CPT 50 Shelf Battery Failure B alarm occurs when battery B is down or not detected. This could be because the battery is removed or is not operational.

Clear the SAT-BAT-FAIL-B Alarm

Procedure

Activate the battery B of the CPT 50 panel.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SAT-COMM-FAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT, SLOT

The CPT 50 Panel Communication Failure (SAT-COMM-FAIL) alarm is raised when the Satellite Discovery Protocol fails on all the interconnect links that constitute a fan out group (FOG) are down.

Clear the SAT-COMM-FAIL Alarm

Procedure

Activate at least one of the interconnect links that constitute a FOG.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SAT-FAN-DEGRADE

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT, SLOT

The CPT 50 Panel Partial Fan Failure (SAT-FAN-DEGRADE) alarm is raised when the fan-tray assembly partially fails or degrades.

Clear the SAT-FAN-DEGRADE Alarm

Procedure

Replace the fan-tray assembly in the CPT 50 panel.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SAT-FAN-FAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT, SLOT

The CPT 50 Panel Fan Failure (SAT-FAN-FAIL) alarm is raised when there is a faulty fan-tray assembly.

Clear the SAT-FAN-FAIL Alarm

Procedure

Repair or replace the fan-tray assembly in the CPT 50 panel.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SAT-FAN-MEA

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT, SLOT

The CPT 50 Panel Fan Mismatch of Equipment and Attributes (SAT-FAN-MEA) alarm is raised when there is a mismatch between the CPT 50 panel and the fan-tray assembly.

Clear the SAT-FAN-MEA Alarm

Procedure

Insert the correct fan-tray assembly in the CPT 50 panel.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SAT-FAN-MFGMEM

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT, SLOT

The CPT 50 Panel Fan Manufacturing Data Memory (EEPROM) Failure (SAT-FAN-MFGMEM) alarm is raised when the fan-tray assembly manufacturing data memory (or EEPROM) fails.

Clear the SAT-FAN-MFGMEM Alarm

Procedure

Recover the fan-tray assembly manufacturing data memory (or EEPROM).
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SAT-FAN-MISSING

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT, SLOT

The CPT 50 Panel Fan Unit is Missing (SAT-FAN-MISSING) alarm is raised when the fan-tray assembly is not present in the CPT 50 panel.

Clear the SAT-FAN-MISSING Alarm

Procedure

Insert the fan-tray assembly in the CPT 50 panel.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http:/

/www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SAT-HITEMP

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT, SLOT

The CPT 50 Panel Fan High Temperature (SAT-HITEMP) alarm is raised when the temperature of the CPT 50 panel is above 149 degrees Fahrenheit (65 degrees Celsius) or below –40 degrees Fahrenheit (–40 degrees Celsius).

Clear the SAT-HITEMP Alarm

Procedure

Complete the Clear the SAT-IHITEMP Alarm procedure.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SAT-IHITEMP

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT, SLOT

The CPT 50 Panel Fan Industrial High Temperature (SAT-IHITEMP) alarm is raised when the temperature of the CPT 50 panel is above 122 degrees Fahrenheit (50 degrees Celsius).

Clear the SAT-IHITEMP Alarm

Procedure

Step 1 Verify that the environmental temperature of the room is not abnormally high.

Step 2 If the room temperature is not abnormal, physically ensure that nothing prevents the fan-tray assembly from passing air through the CPT 50 panel

Step 3 If the airflow is not blocked, physically ensure that blank faceplates fill the CPT 50 panel empty slots. Blank faceplates help airflow.

Step 4 If faceplates fill the empty slots, determine whether the air filter needs replacement.

Step 5 If the fan does not run or the alarm persists, replace the fan-tray assembly.
The fan should run immediately when correctly inserted.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SAT-IMPROPER-CONFIG

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT, SLOT

The CPT 50 Panel Improper Configuration (SAT-IMPROPER-CONFIG) alarm is raised when the CPT 50 panel is configured incorrectly.

Clear the SAT-IMPROPER-CONFIG Alarm

Procedure

Verify the following:

- The CTP 50 panel has a unique FOG identifier.
- All interconnect links on the CPT 50 panel are part of a single FOG.
- Interconnect links on the CPT 50 panel is connected to only one card (fabric card or line card).

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SINGLE-SPAN-FAIL

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: RING

The Single Span Failure (SINGLE-SPAN-FAIL) alarm is raised when a single link of a ring is down.

Clear the SINGLE-SPAN-FAIL Alarm

Procedure

Activate the link of the ring that is down.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SLA-TCA

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: PTS

The Service Level Agreement-Threshold Crossover (SLA-TCA) alarm is raised when the configured rising threshold for the IP SLA Delay Management (DM) session is exceeded.

Clear the SLA-TCA Alarm

Perform any of the following, as appropriate:

- Ensure that the measured delay is less than the falling threshold.
- Restart the SLA session.
- Delete the SLA session.

Note To clear the SLA-TCA alarm from CTC, ensure that the alarm condition does not exist for any IP SLA session.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or log into http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html to obtain a directory of toll-free Technical Support numbers for your country in order to report a Service-affecting (SA) problem.

TEMP-LIC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Temporary License (TEMP-LIC) alarm is raised to indicate that a valid temporary license is in use.

Clear the TEMP-LIC Alarm

Procedure

Procure and install a permanent license. For more information on installing a license, see the Licensing Configuration guide.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Terminal Loopback

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TDM

The Terminal Loopback alarm is raised when the software terminal (inward) loopback is active for a port.

Clear the Terminal Loopback Alarm

Procedure

Correct the terminal (inward) loopback configuration for a port.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TE-TUNNEL-DOWN

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: PTS

The TE Tunnel Down (TE-TUNNEL-DOWN) alarm is raised when the working or protect Multiprotocol Label Switching - Label-Switched Path (MPLS-LSP) is inactive. Traffic will be down.

Clear the TE-TUNNEL-DOWN Alarm

Procedure

Perform any of the following, as appropriate:

- Verify that the LSP does not have any connectivity issues.
- Administratively shut down the tunnel. Traffic drops when the tunnel is administratively shut down.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

TOPO-MIS-CONF

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: RING

The Topology Misconfiguration (TOPO-MIS-CONF) alarm is raised when the topology discovery detects the topology with any of these conditions:

- Some provisioned nodes are missing from the network.
- Some un-provisioned nodes exist in the network.
- Actual configuration of the nodes is different from the provisioned configuration.

Clear the TOPO-MIS-CONF Alarm

Procedure

Either change the topology of the nodes according to the actual configuration, or re-configure the nodes according to the topology in the network.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

TP-TUNNEL-DOWN

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: PTS

The MPLS-TP Tunnel Down (TP-TUNNEL-DOWN) alarms is raised when the working or protect label-switched path (LSP) is inactive. Traffic will be down.

Clear the TP-TUNNEL-DOWN Alarm

Procedure

Perform any of the following, as appropriate:

- Verify that the LSP does not have any connectivity issues.
- Administratively shut down the tunnel. Traffic drops when the tunnel is administratively shut down.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

TP-WKSPWR

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: PORT

The Transport Profile Traffic Switched to Protection (TP-WKSPWR) alarm is raised when the MPSL-TP traffic switches from the working pseudowire to the protected pseudowire.

Clear the TP-WKSPWR Alarm

Procedure

Switch traffic from the protected pseudowire to the working pseudowire.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

WKG-LOC-PW-NOT-FWD

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: PTS

The Working Local Pseudowire Not Forwarding (WKG-LOC-PW-NOT-FWD) alarm is raised when the local working pseudowire is not forwarding traffic.

Clear the WKG-LOC-PW-NOT-FWD Alarm

Procedure

Perform any of the following, as appropriate:

- Verify that the pseudowire does not have any connectivity issues.
- Verify that the LSP does not have any connectivity issues.
- Administratively shut down the tunnel. Traffic drops when the tunnel is administratively shut down.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

WKG-LSP-DOWN

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: PORT

The Working Label-Switched Path Down (WKG-LSP-DOWN) alarm is raised on the port if the working label-switched path (LSP) is inactive.

Clear the WKG-LSP-DOWN Alarm

Procedure

Perform any of the following, as appropriate:

- Verify that the LSP does not have any connectivity issues.
- Administratively shut down the tunnel. Traffic drops when the tunnel is administratively shut down.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

WKG-LSP-LDI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: PORT

The Working Label-Switched Path Link Defect Indication (WKG-LSP-LDI) alarm is raised when the working label switched path (LSP) receives an LSP link defect indication signal. The WKG-LSP-LDI alarm suppresses the WKG-LSP-LKR alarm, if present.

Clear the WKG-LSP-LDI Alarm

Procedure

Perform any of the following, as appropriate:

- Verify that the LSP does not have any connectivity issues.
- Administratively shut down the tunnel. Traffic drops when the tunnel is administratively shut down.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

WKG-LSP-LKR

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: FAC

The Working Label-Switched Path Lock Report (WKG-LSP-LKR) alarm is raised when an interface is administratively shut down on a working path in an MPLS-TP tunnel. The WKG-LSP-LKR alarm suppresses the WKG-LSP-LDI alarm, if present.

Clear the WKG-LSP-LKR Alarm

Procedure

Perform any of the following, as appropriate:

- Verify that the LSP does not have any connectivity issues.
- Administratively shut down the tunnel. Traffic drops when the tunnel is administratively shut down.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

WKG-PW-CC-DOWN

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: PORT

The Working Pseudowire Continuity Check Down (WKG-PW-CC-DOWN) alarm is raised when the virtual circuit connectivity verification (VCCV) BFD fails on the port or when the port-channel is configured as AC port.

Clear the WKG-PW-CC-DOWN Alarm

Procedure

Activate the working pseudowire continuity check.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

WKG-PW-CP-DOWN

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: PORT

The Working Pseudowire Control Plane Down (WKG-PW-CP-DOWN) alarm is raised on the port when the control plane of the working pseudowire fails.

Clear the WKG-PW-CP-DOWN Alarm

Procedure

Activate the control plane of the working pseudowire.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

WKG-PW-LOC-AC-RX-FLT

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: PORT

The Working Pseudowire Local AC RX Port Fault (WKG-PW-LOC-AC-RX-FLT) alarm is raised when the port fault on the receive side is detected on the local attachment circuit of the working pseudowire.

Clear the WKG-PW-LOC-AC-RX-FLT Alarm

Procedure

Remove the port fault on the receive side that is detected on the local attachment circuit of the working pseudowire.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

WKG-PW-LOC-AC-TX-FLT

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: PORT

The Working Pseudowire Local AC TX Port Fault (WKG-PW-LOC-AC-TX-FLT) alarm is raised when the port fault on the transmit side is detected on the local attachment circuit of the working pseudowire.

Clear the WKG-PW-LOC-AC-TX-FLT Alarm

Procedure

Remove the port fault on the transmit side that is detected on the local attachment circuit of the working pseudowire.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

WKG-PW-REM-AC-RX-FLT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: PORT

The Working Pseudowire Remote AC RX Port Fault (WKG-PW-REM-AC-RX-FLT) alarm is raised when the port fault on the receive side is detected on the remote attachment circuit of the working pseudowire.

Clear the WKG-PW-REM-AC-RX-FLT Alarm

Procedure

Remove the port fault on the receive side that is detected on the remote attachment circuit of the working pseudowire.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

WKG-PW-REM-AC-TX-FLT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: PORT

The Working Pseudowire Remote AC TX Port Fault (WKG-PW-REM-AC-TX-FLT) alarm is raised when the port fault on the transmit side is detected on the remote attachment circuit of the working pseudowire.

Clear the WKG-PW-REM-AC-TX-FLT Alarm

Procedure

Remove the port fault on the transmit side that is detected on the remote attachment circuit of the working pseudowire.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

WKG-PW-RX-FLT

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: PORT

The Working Pseudowire RX Fault (WKG-PW-RX-FLT) alarm is raised when the state of the MPLS-TP tunnel, on which a working pseudowire is created, is changed to DOWN.

Clear the WKG-PW-RX-FLT Alarm

Perform any of the following, as appropriate:

- Change the state of the MPLS-TP tunnel to UP.
- Delete the pseudowire.

If the condition does not clear, 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).

WKG-REM-PW-NOT-FWD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: PTS

The Working Remote Pseudowire Not Forwarding (WKG-REM-PW-NOT-FWD) alarm is raised when the remote working pseudowire is not forwarding traffic.

Clear the WKG-REM-PW-NOT-FWD Alarm

Procedure

The alarm clears when the remote working pseudowire starts forwarding traffic.
If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

WKG-TP-LOCKOUT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: PORT

The Working Transport Profile Lockout (WKG-TP-LOCKOUT) alarm is raised when the LOCK-OUT request is set to ON for the working MPLS-TP.

Clear the WKG-TP-LOCKOUT Alarm

Procedure

Set the LOCK-OUT request to OFF for the working MPLS-TP.
If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

NTP-J73 Display Alarms that Affect Services Using CTC

Purpose	This procedure displays the alarms that affect the services.
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 NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to display the alarms that affect the services.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Service Level Alarm** tab.

Step 4 In the Retrieve Alarm Affecting Services area, click **PT System** or **Port** or **Channel Group**.

Step 5 (Only for Port) From the Slot drop-down list, choose a slot.

Step 6 (Only for Port) From the Port drop-down list, choose a port.

Step 7 From the Service Type drop-down list, choose an appropriate service (EVC, PW, TUNNEL–TE, or TUNNEL–TP)

Step 8 From the Service Alarm drop-down list, choose an appropriate service alarm.
The service alarms are populated based on the chosen service type.

Step 9 Click **Show**.
The alarm affecting services are displayed.

NTP-J74 Display Alarms on Service Using CTC

Purpose	This procedure displays the alarms that are on service.
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 NTP-J22 Log into CTC, on page 15 procedure at a node on the network where you want to display the alarms that are on service.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Service Level Alarm** tab.

Step 4 In the Retrieve Alarms on Service area, click **PT System** or **Port** or **Channel Group**.

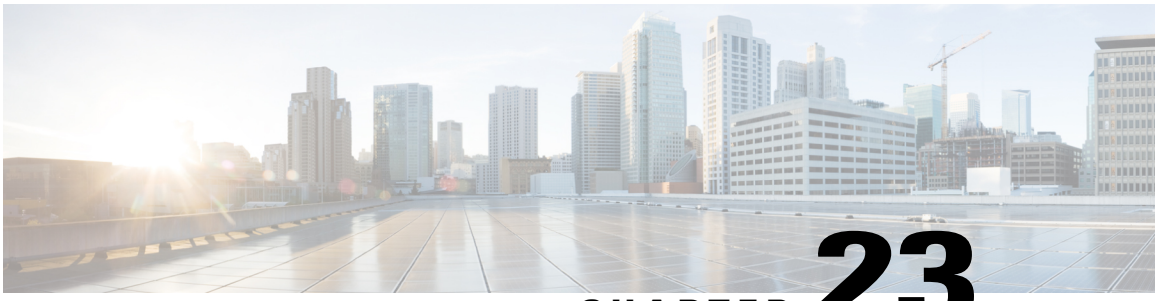
Step 5 (Only for Port) From the Slot drop-down list, choose a slot.

Step 6 (Only for Port) From the Port drop-down list, choose a port.

Step 7 From the Service Type drop-down list, choose an appropriate service (EVC, PW, TUNNEL–TE, or TUNNEL–TP)

Step 8 Enter the service ID in the Service ID field.

Step 9 Click **Show**.
The alarms that are on service are displayed.



CHAPTER 23

SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by CPT.

Understanding SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by CPT.

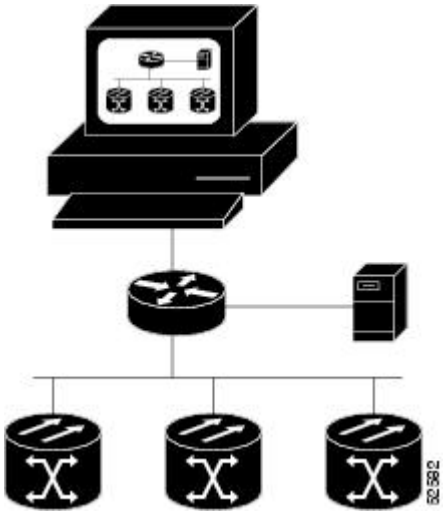
SNMP is an application–layer communication protocol that allows network devices to exchange management information among these systems and with other devices outside the network. Through SNMP, network administrators can manage network performance, find and solve network problems, and plan network growth. SNMP makes network monitoring more cost effective and allows your network to be more reliable.

CPT supports SNMP Version 1 (SNMPv1), SNMP Version 2c (SNMPv2c), and SNMP Version 3 (SNMPv3). As compared to SNMPv1, SNMPv2c includes additional protocol operations and 64–bit performance monitoring support. SNMPv3 provides authentication, encryption, and message integrity and is more secure.

Note SNMP Version 3 (SNMPv3) is not supported for PTF and line cards.

The following figure illustrates the basic layout idea of an SNMP-managed network.

Figure 79: Basic Network Managed by SNMP



The advantages of SNMP are as follows:

- SNMP is LAN based.
- SNMP is an open standard.
- SNMP can be easily extended.
- SNMP provides a common management platform for many different devices.

Understanding SNMP Components

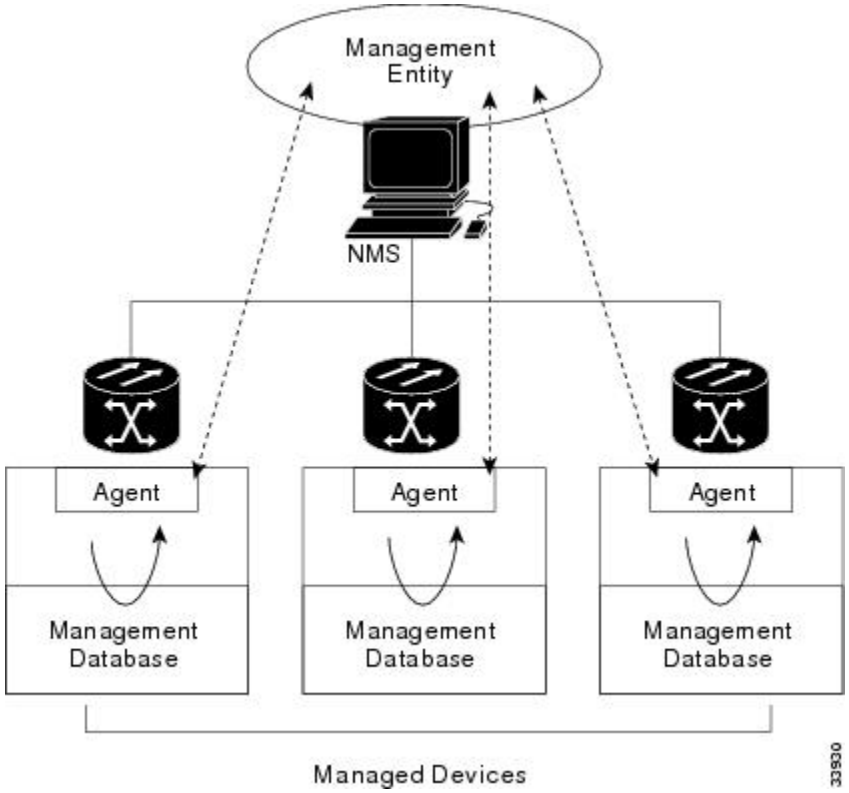
An SNMP–managed network consists of a manager, agents, and managed devices.

The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical device being managed

Management systems execute most of the management processes and provide the bulk of memory resources used for network management. A network might be managed by one or several management systems.

The following figure illustrates the relationship between the network manager, the SNMP agent, and the managed devices.

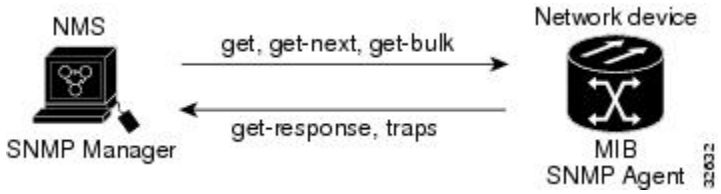
Figure 80: Example of the Primary SNMP Components



An agent residing on each managed device translates local management information data—such as performance information or event and error information—caught in software traps, into a readable form for the management system.

The following figure illustrates SNMP agent get–requests that transport data to the network management software.

Figure 81: Agent Gathering Data from a MIB and Sending Traps to the Manager



The SNMP agent captures data from MIBs, which are device parameter and network data repositories, or from error or change traps.

A managed element—such as a router, access server, switch, bridge, hub, computer host, or network element—is accessed through the SNMP agent. Managed devices collect and store management information, making it available through SNMP to other management systems having the same protocol compatibility.

Note It is recommended that the SNMP Manager timeout value be set to 60 seconds. Under certain conditions, if this value is lower than the recommended time, the TNC/TSC card can be reset. However, the response time depends on various parameters such as object being queried, complexity, number of hops in the node and so on.

Understanding MIB

The Management Information Base (MIB) is a data structure that describes SNMP network elements as a list of data objects. The SNMP manager must compile the MIB file for each equipment type in the network to monitor SNMP devices.

The manager and agent use a MIB and a relatively small set of commands to exchange information. The MIB is organized in a tree structure with individual variables being represented as leaves on the branches. A long numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and in SNMP messages. The MIB associates each OID with a readable label and various other parameters related to the object. The MIB then serves as a data dictionary or codebook that is used to assemble and interpret SNMP messages.

When the SNMP manager wants to know the value of an object, such as the state of an alarm point, the system name, or the element uptime, it will assemble a GET packet that includes the OID for each object of interest. The element receives the request and looks up each OID in its code book (MIB). If the OID is found (the object is managed by the element), a response packet is assembled and sent with the current value of the object included. If the OID is not found, a special error response is sent that identifies the unmanaged object.

MIBs Supported in CPT

The following table lists the MIBs supported in CPT.

Table 60: MIBs Supported in CPT

MIB Module
BGP4-MIB.my
BRIDGE-MIB.my
CERENT-454.mib
CERENT-ENVMON-MIB.mib
CERENT-FC-MIB.mib
CERENT-GENERIC-PM-MIB.mib
CERENT-GLOBAL-REGISTRY.mib
CERENT-HC-RMON-MIB.mib
CERENT-IF-EXT-MIB.mib
CERENT-MSDWDM-MIB.mib

MIB Module
CERENT-OPTICAL-MONITOR-MIB.mib
CERENT-TC.mib
CISCO-CDP-MIB.my
CISCO-CLASS-BASED-QOS-MIB.my
CISCO-ENTITY-ASSET-MIB.my
CISCO-ENTITY-EXT-MIB.my
CISCO-ENTITY-VENDORTYPE-OID-MI
CISCO-FRAME-RELAY-MIB.my
CISCO-FTP-CLIENT-MIB.my
CISCO-HSRP-EXT-MIB.my
CISCO-HSRP-MIB.my
CISCO-IETF-PW-MIB
CISCO-IGMP-SNOOPING-MIB.mib
CISCO-IMAGE-MIB.my
CISCO-IPMROUTE-MIB.my
CISCO-IP-STAT-MIB.my
CISCO-MEMORY-POOL-MIB.my
CISCO-OPTICAL-MONITOR-MIB.mib
CISCO-PING-MIB.my
CISCO-PORT-QOS-MIB.my
CISCO-PROCESS-MIB.my
CISCO-PRODUCTS-MIB.my
CISCO-REP-MIB.my
CISCO-SMI.mib
CISCO-SYSLOG-MIB.my
CISCO-TC.my
CISCO-TCP-MIB.my
CISCO-VLAN-IFTABLE-RELATIONSHIP
entityMIB
entityx.mib
EtherLike-MIB-rfc2665.mib

MIB Module
HCNUM-TC.mib
HC-PerfHist-TC-MIB.my
HC-RMON-rfc3273.mib
IANAifType-MIB.mib
IANA-RTPROTO-MIB.my
IEEE8023-LAG-MIB.my
IEEE-802DOT17-RPR-MIB.my
IF-MIB-rfc2233.mib
IGMP-MIB.my
INET-ADDRESS-MIB.mib
IPMROUTE-STD-MIB.my
MPLS-TE-MIB
OLD-CISCO-TCP-MIB.my
OLD-CISCO-TS-MIB.my
OSPF-MIB.my
P-BRIDGE-MIB-rfc2674.mib
PerfHist-TC-MIB-rfc2493.mib
PIM-MIB.my
Q-BRIDGE-MIB-rfc2674.mib
RFC1155-SMI.my
RFC1213-MIB.mib
RFC1253-MIB-rfc1253.mib
RFC1315-MIB.my
RIPv2-MIB-rfc1724.mib
RMON2-MIB-rfc2021.mib
RMON-MIB-rfc2819.mib
RMONTOK-rfc1513.mib
SNMP-FRAMEWORK-MIB-rfc2571.mib
SNMP-MPD-MIB.mib
SNMP-NOTIFICATION-MIB.my
SNMP-NOTIFY-MIB-rfc3413.mib

MIB Module
SNMP-PROXY-MIB-rfc3413.mib
SNMP-TARGET-MIB-rfc3413.mib
SNMP-USER-BASED-SM-MIB-rfc3414.mib
SNMPv2-MIB-rfc1907.mib
SNMPv2-SMI.my
SNMPv2-TC.my
SNMP-VIEW-BASED-ACM-MIB-rfc3415.mib
TCP-MIB.my
TOKEN-RING-RMON-MIB.my
UDP-MIB.my

Understanding SNMP Traps

CPT uses SNMP traps to generate all the alarms and events. The traps contain the following information:

- Object IDs that uniquely identify each event with information about the generating entity.
- Severity and service effect of the alarm (critical, major, minor, or event; service-affecting or non-service-affecting).
- Date and time stamp showing when the alarm occurred.

Generic IETF Traps

CPT supports the generic IETF traps listed in the following table.

Table 61: Supported Generic IETF Traps

Trap	Description
coldStart	Agent up, cold start.
warmStart	Agent up, warm start.
authenticationFailure	Community string does not match.
newRoot	Sending agent is the new root of the spanning tree.
topologyChange	A port in a bridge has changed from Learning to Forwarding or Forwarding to Blocking.
entConfigChange	The entLastChangeTime value has changed.

Trap	Description
risingAlarm	The SNMP trap that is generated when an alarm entry crosses the rising threshold and the entry generates an event that is configured for sending SNMP traps.
fallingAlarm	The SNMP trap that is generated when an alarm entry crosses the falling threshold and the entry generates an event that is configured for sending SNMP traps.

Examples of IETF Traps

coldStart

```
DISMAN-EVENT-MIB::sysUpTimeInstance = 21775
SNMPv2-MIB::snmpTrapOID.0 = SNMPv2-MIB::coldStart
CERENT-454-MIB::cerent454NodeTime.0 = 20110705135346D
CERENT-454-MIB::cerent454AlarmState.1.1 = administrative
SNMP-COMMUNITY-MIB::snmpTrapAddress.0 = 10.64.106.142"
```

warmStart

```
DISMAN-EVENT-MIB::sysUpTimeInstance = 21775
SNMPv2-MIB::snmpTrapOID.0 = SNMPv2-MIB::warmStart
CERENT-454-MIB::cerent454NodeTime.0 = 20110705135346D
CERENT-454-MIB::cerent454AlarmState.1.1 = administrative
SNMP-COMMUNITY-MIB::snmpTrapAddress.0 = 10.64.106.142"
```

authenticationFailure

```
DISMAN-EVENT-MIB::sysUpTimeInstance = 6335948
SNMPv2-MIB::snmpTrapOID.0 = SNMPv2-MIB::authenticationFailure
CERENT-454-MIB::cerent454NodeTime.0 = 20110705121300D
CERENT-454-MIB::cerent454AlarmState.1.1 = administrative
SNMP-COMMUNITY-MIB::snmpTrapAddress.0 = 10.64.106.142"
```

newRoot

```
RFC1213-MIB::sysUpTime.0 = 255172
SNMPv2-MIB::snmpTrapOID.0 = BRIDGE-MIB::newRoot
CERENT-454-MIB::cerent454NodeTime.0 = 20000125062804S
CERENT-454-MIB::cerent454AlarmState.1.1 = notAlarmedNonServiceAffecting
CERENT-454-MIB::cerent454AlarmSeverity.1.1 = notAlarmed
CERENT-454-MIB::cerent454AlarmStatus.1.1 = transient
CERENT-454-MIB::cerent454AlarmServiceAffecting.1.1 = nonServiceAffecting
SNMPv2-SMI::snmpModules.18.1.3.0 = 10.64.104.11
```

topologyChange

```
RFC1213-MIB::sysUpTime.0 = 254973
SNMPv2-MIB::snmpTrapOID.0 = BRIDGE-MIB::topologyChange
CERENT-454-MIB::cerent454NodeTime.0 = 20000125062802S
CERENT-454-MIB::cerent454AlarmState.1.1 = notAlarmedNonServiceAffecting
CERENT-454-MIB::cerent454AlarmSeverity.1.1 = notAlarmed
CERENT-454-MIB::cerent454AlarmStatus.1.1 = transient
CERENT-454-MIB::cerent454AlarmServiceAffecting.1.1 = nonServiceAffecting
SNMPv2-SMI::snmpModules.18.1.3.0 = 10.64.104.11
```

entConfigChange

```
DISMAN-EVENT-MIB::sysUpTimeInstance = 6246394
SNMPv2-MIB::snmpTrapOID.0 = ENTITY-MIB::entConfigChange
CERENT-454-MIB::cerent454NodeTime.0 = 20110705115804D
CERENT-454-MIB::cerent454AlarmState.4096.1 = administrative
SNMP-COMMUNITY-MIB::snmpTrapAddress.0 = 10.64.106.142"
```

risingAlarm

```
SNMPv2-MIB::sysUpTime.0 = 39547235
SNMPv2-MIB::snmpTrapOID.0 = RMON-MIB::risingAlarm
RMON-MIB::alarmIndex.1 = 1
RMON-MIB::alarmVariable.1 = IF-MIB::ifInOctets.16409
RMON-MIB::alarmSampleType.1 = absoluteValue
RMON-MIB::alarmValue.1 = 0
RMON-MIB::alarmRisingThreshold.1 = 100
CERENT-454-MIB::cerent454NodeTime.0 = 20090402234612D
CERENT-454-MIB::cerent454AlarmState.16409.1 = administrative
SNMP-COMMUNITY-MIB::snmpTrapAddress.0 = 10.64.105.113"
```

fallingAlarm

```
SNMPv2-MIB::sysUpTime.0 = 39463718
SNMPv2-MIB::snmpTrapOID.0 = RMON-MIB::fallingAlarm
RMON-MIB::alarmIndex.7 = 7
RMON-MIB::alarmVariable.7 = EtherLike-MIB::dot3StatsFCSErrors.16409
RMON-MIB::alarmSampleType.7 = deltaValue
RMON-MIB::alarmValue.7 = 0
RMON-MIB::alarmFallingThreshold.7 = 500
CERENT-454-MIB::cerent454NodeTime.0 = 20090402233217D
CERENT-454-MIB::cerent454AlarmState.16409.1 = administrative
SNMP-COMMUNITY-MIB::snmpTrapAddress.0 = 10.64.105.113"
```

SNMP Traps Supported in CPT

The following table lists the SNMP traps supported in CPT.

Table 62: SNMP Traps Supported in CPT

MIB Module
pseudowireDown
workingPseudowireControlPlainDown
protectPseudowireControlPlainDown
workingPseudowireConnectivityCheckDown
protectPseudowireConnectivityCheckDown
pseudowireTrafficSwitchedToProtection
workingPseudowireLocalAcTxPortFault
protectPseudowireLocalAcTxPortFault
workingPseudowireLocalAcRxPortFault
protectPseudowireLocalAcRxPortFault
workingPseudowireRemoteAcTxPortFault
protectPseudowireRemoteAcTxPortFault
workingPseudowireRemoteAcRxPortFault
protectPseudowireRemoteAcRxPortFault

MIB Module
workingRemotePseudowireNotForwarding
protectRemotePseudowireNotForwarding
tpTunnelDown
workingLabelSwitchedPathDown
protectLabelSwitchedPathDown
bidirectionalForwardDetectionDown
tpTrafficSwitchedFromWorkingToProtection
workingTpLockout
protectTpLockout
ethernetFlowPointFailed
teTunnelDown
macSystemLimitReached
macBridgeDomainLimitReached
packetTransportServiceFailed
satellitePanelDiscoveryFailure
satellitePanelActiveLinkFailure
satellitePanelCommunicationFailure
satellitePanelImproperConfiguration
satellitePanelFanMismatchOfEquipmentAndAttributes
satellitePanelFanFailure
satellitePanelPartialFanFailure
satellitePanelFANManufacturingDataMemoryEEPROMFailure
satellitePanelFANUnitIsMissing
satellitePanelIndustrialHighTemperature
satellitePanelHighTemperature
satellitePanelBatteryFailureA
protectionCardConfigurationMismatch
routerProcessorSwitchOver
runningLowOnResources
noMoreResourcesAreAvailable
licenseWillExpireWithin24Hours

MIB Module
licenseWillExpireAnytimeAfter1DayButBefore14Days
licenseIsExpired
temporaryLicenseIsInUse
evaluationLicenseIsInUse
licenseIsMissing
SMBackwardIncomingAlignmentError
resourceAllocationFailed
workingLabelSwitchedPathLinkDownIndication
protectLabelSwitchedPathLinkDownInication
workingLabelSwitchedPathLockReport
protectLabelSwitchedPathLockReport
satellitePanelBatteryFailureB
coolingProfileMismatch
trunkOduAlarmIndicationSignal
companionCardMissing
powerConsumptionLimitHasCrossed
controlPlaneUnverifiedClearedAlarmsPresent
singleSpanFail
multipleSpanFail
topoMisConfig
dbSyncFail
dbLoss
DUALHOME_STATE_CHANGE_TRAP
fastAutomaticProtectionSwitchingConfigMismatch
ftaMismatch
frontPortLinkLoss
workQueueFull
equipmentPowerFailureAtConnectorA
equipmentPowerFailureAtConnectorB
equipmentPowerFailureAtReturnConnectorA
equipmentPowerFailureAtReturnConnectorB

MIB Module
openIOSlots
voaControlLoopDisableDueToExcessiveCounterPropagationLight
eqptDegrade
plannedSwitchOver
licenseCountViolation
slaThresholdCrossAlert
primarySynchronizationReferenceFailure
secondarySynchronizationReferenceFailure
thirdSynchronizationReferenceFailure
regeneratorSectionTraceIdentifierMismatch
workQueueFull
SMBackwardIncomingAlignmentError
lossOfSynchronization
outOfSynchronization
failedToReceiveSynchronizationStatusMessage
synchronizationStatusMessagesAreDisabledOnThisInterface
stratum1PrimaryReferenceSourceTraceable
stratum2Traceable
stratum3Traceable
stratum3ETraceable
stratum4Traceable
synchronizedTraceabilityUnknown
transitNodeClockTraceable
sonetMinimumClockTraceable
doNotUseForSynchronization
reservedForNetworkSynchronizationUse
automaticSystemReset
dhSwVerMism
dhOutOfSync

Understanding SNMP Community Names

Community names are used to group SNMP trap destinations. All the trap destinations can be provisioned as part of SNMP communities in CTC. When community names are assigned to traps, the request is treated as valid if the community name matches one that is provisioned in CTC. In this case, all agent-managed MIB variables are accessible to that request. If the community name does not match the provisioned list, SNMP drops the request.

Accessing Fabric Card Through SNMP

Each fabric card runs a separate instance of SNMP. SNMP requests are relayed to the individual fabric card based on the community string. The community string uses the following format:

com_str_configured_from_CTC@fabric_card_slot_number

Understanding SNMP Messages

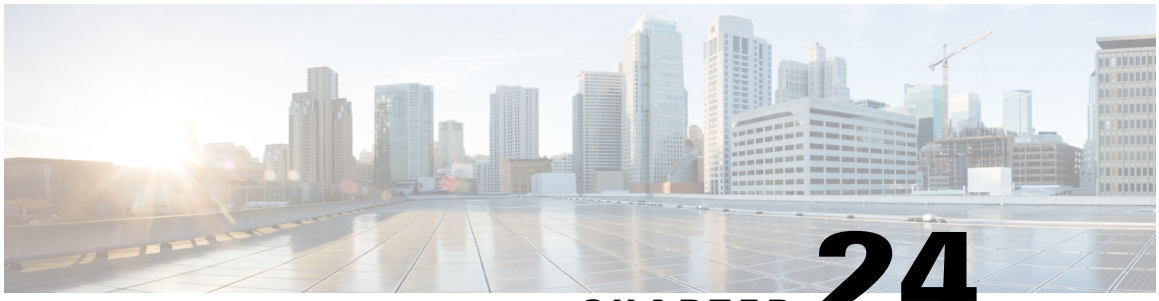
SNMP uses the following messages to communicate between the manager and the agent.

- Get
- GetNext
- GetResponse
- Set
- Trap

The Get and GetNext messages allow the manager to request information for a specific variable. The agent, upon receiving a Get or GetNext message, will issue a GetResponse message to the manager with either the information requested or an error indication as to why the request cannot be processed.

A Set message allows the manager to request a change be made to the value of a specific variable in the case of an alarm remote that will operate a relay. The agent will then respond with a GetResponse message indicating the change has been made or an error indication as to why the change cannot be made.

The Trap message allows the agent to inform the manager of an important event. An SNMP Trap is a change–of–state (COS) message—it could mean an alarm, a clear or simply a status message.



CHAPTER 24

Configuring System Log

This chapter describes the logging to syslog server , message format and its severity in CPT. This chapter also describes procedures to configure syslog.

This chapter includes the following topics:

Syslog Overview in CPT

Whenever messages need to be logged to syslog server, application module can trigger system messages. A member that generates a system message appends its hostname in the form of hostname-n, where n is a switch number from 1 to 4, and redirects the output to the logging process. The logging process controls the distribution of logging messages to the logging buffer. The process also sends messages to the console.

We can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. The switch software saves syslog messages in an internal buffer. We can also remotely monitor system messages by viewing the logs on a syslog server or by accessing the CPT through Telnet or through the console port.

System Log Message Format

System log (syslog) messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information(if configured).

Messages will appear in below format:

seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)

The part of the message preceding % depends on the setting of the **service sequence-numbers** , **service timestamps log datetime** , **service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**] , or **service timestamps log uptime** global configuration command.

The following table shows the syslog message set.

syslog message parameters:

Element	Description
seq no	Stamps log messages with a sequence number only if the **service sequence-numbers** global configuration command is configured
timestamp mm/dd hh:mm:ss or *hh:mm:ss* (short uptime) or *d h* (long uptime)	Date and time of the message or event. This information appears only if the service timestamps log [datetime | log] global configuration command is configured
facility	The facility to which the message refers (for example, SNMP, SYS, and so forth)
severity	Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, refer System Log Message Severity, on page 863
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.

Examples of syslog messages

- **interface down/up**

  Jan 20 10:20:09.920: %LINK-3-UPDOWN: Interface TenGigabitEthernet3/1, changed state to down è syslog message to indicate link down for interface 3/1 ; this is raised as error message (3)

  Jan 20 10:20:10.288: %LINK-3-UPDOWN: Interface TenGigabitEthernet3/1, changed state to up

  Jan 20 10:20:11.288: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet3/1, changed state to up è syslog message to indicate line protocol down in PI ; severity as notice message

- **New provisioning message is received from controller card (TNC)**

  Jan 20 09:34:08.641: %CARDWARE-6-PROVISIONING: new provisioning received

  Note This message will be generated whenever there is a configuration change. It is an informational message

- **Card OIR**

  Nov 22:27:05.311: %OIR-6-INSCARD: Card 6 inserted in slot 6

  Note an informational message to indicate card 6 plugin.

  Nov 3 22:24:03.949: %OIR-6-REMCARD: Card 5 removed from slot 5

Note An informational message to indicate card 5 plugout.

System Log Message Severity

- #define LOG_EMERG 0 */*system is unusable */*
- #define LOG_ALERT 1 */*action must be taken immediately */*
- #define LOG_CRIT 2 */*critical conditions */*
- #define LOG_ERR 3 */* error conditions */*
- #define LOG_WARNING 4 */*warning conditions */*
- #define LOG_NOTICE 5 */*normal but significant condition */*
- #define LOG_INFO 6 / * *informational* */*
- #define LOG_DEBUG 7 */*debug-level messages */*

DLP-J338 Configure syslog Using CTC

Purpose	This procedure configures syslog using CTC.
Tools/Equipment	none
Prerequisite Procedures	Host IP should be configured
Required/As Needed	As needed
Onsite/Remote	Onsite or Remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete theNTP-J22 Log into CTC, on page 15procedure at a node on the network where you want to configure syslog.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Maintenance** tab.

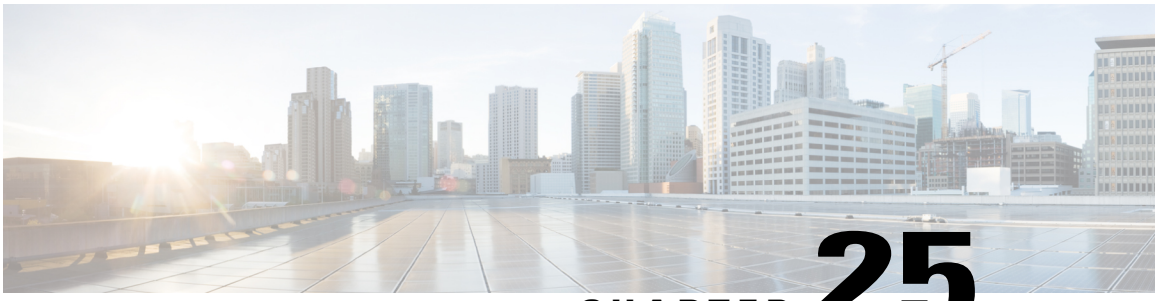
Step 4 From the left pane, click **Syslog**

Step 5 Enable below syslog settings:

- Enable Syslog
- Enable Archive Log
- Enable Mpls Tp Log
- Enable PW Log
- Enable Proxy Relay IP

Note Enable proxy relay IP is enabled when CPT600/200 is an ENE node , providing relay IP as GNE node's IP address .

Step 6 Click **Apply** to save the configuration.
Stop. You have completed this procedure.



CHAPTER 25

Security Reference

this chapter contains information related to user IDs and security levels, user privileges and policies, audit trail, and RADIUS security.

User IDs and Security Levels

The Cisco Transport Controller (CTC) ID is provided with the system, but the system does not display the user ID when you sign into CTC. This ID can be used to set up other users.

You can have up to 500 user IDs on one . Each CTC or TL1 user can be assigned one of the following security levels:

- Retrieve-Users can retrieve and view CTC information but cannot set or modify parameters.
- Maintenance-Users can access only the maintenance options.
- Provisioning-Users can access provisioning and maintenance options.
- Superusers-Users can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users.
- Security Super User-Users can set encryption and card authentication parameters. The security super user creates security users and associates each user with a WSE card. By default, at least one security super user must exist.
- Security User-Users can enable or disable card authentication and payload encryption.
- Root User-Cisco Prime user with all the security and transport privileges. The root user is not supported in CTC or TL1. The security super user can enable the root user through CTC.

See Idle User Timeout, on page 872for idle user timeout information for each security level.

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

Note You must add the same user name and password to each node the user accesses.

Note Maintenance, Provisioning, and Superusers must be properly trained on the hazards of laser safety and be aware of safety-related instructions, labels, and warnings. Refer to the Cisco Optical Products Safety and Compliance Information document for a current list of safety labels and warnings, including laser warnings. Refer to IEC 60825-2 for international laser safety standards, or to ANSI Z136.1 for U.S. laser safety standards. The explains how users can disable laser safety during maintenance or installation; when following these procedures, adhere to all posted warnings and cautions to avoid unsafe conditions or abnormal exposure to optical radiation.

User Privileges and Policies

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

User Privileges by CTC task

Below table shows the actions that each user privilege level can perform in node view. An X indicates the user is allowed to perform the action. A dash indicates that the user is not allowed to perform the action.

Table 63: Security Levels - Node View

CTC Tab	Subtab	[Subtab]: Actions	Retrieve/Security Super User/Security User	Maintenance	Provisioning	Superuser
Alarms	-	Synchronize/Filter/Delete Cleared Alarms	X	X	X	X
Conditions	-	Retrieve/Filter	X	X	X	X
History	Session	Filter	X	X	X	X
	Node	Retrieve/Filter	X	X	X	X
Circuits	Circuits	Create/Edit/Delete	-	-	X	X
		Filter/Search	X	X	X	X
	Rolls	Complete/Force Valid Signal/Finish	-	-	X	X

Provisioning	General	General: Edit	-	-	PartialA Provisioning user cannot change node name, contact, location and AIS-V insertion on STS-1 signal degrade (SD) parameters.	X
		Multishelf Config: Edit	-	-	X	-
	Network	General: Edit	-	-	X	X
		Static Routing: Create/Edit/Delete	-	-	X	X
		OSPF: Create/Edit/Delete	-	-	X	X
		RIP: Create/Edit/Delete	-	-	X	X
		Proxy: Create/Edit/Delete	-	-	X	X
		Firewall: Create/Edit/Delete	-	-	X	X
	OSI	Main Setup: Edit	-	-	X	X
		TARP: Config: Edit	-	-	X	X
		TARP: Static TDC: Add/Edit/Delete	-	-	X	X
		TARP: MAT: Add/Edit/Remove	-	-	X	X
		Routers: Setup: Edit	-	-	X	X
		Routers: Subnets: Edit/Enable/Disable	-	-	X	X
		Tunnels: Create/Edit/Delete	-	-	X	X

	Security	Users: Create/Delete/Clear Security Intrusion Alarm	-	-	-	X
		Users: Change	Same user	Same user	Same user	All users
		Active Logins: View/Logout/ Retrieve Last Activity Time	-	-	-	X
		Policy: Edit/View	-	-	-	X
		Access: Edit/View	-	-	-	X
		RADIUS Server: Create/Edit/Delete/Move Up/Move Down/View	-	-	-	X
		Legal Disclaimer: Edit	-	-	-	X
	SNMP	Create/Edit/Delete	-	-	X	X
		Browse trap destinations	X	X	X	X
	Comm Channels	SDCC: Create/Edit/Delete	-	-	X	X
		LDCC: Create/Edit/Delete	-	-	X	X
		GCC: Create/Edit/Delete	-	-	X	X
		OSC: Create/Edit/Delete	-	-	X	X
		PPC: Create/Edit/Delete	-	-	X	X
		LMP: General: Edit	X	X	X	X
		LMP: Control Channels: Create/Edit/Delete	-	-	X	X
		LMP: TE Links: Create/Edit/Delete	-	-	X	X
		LMP: Data Links: Create/Edit/Delete	-	-	X	X
	Alarm Profiles	Load/Store/DeleteThe action buttons in the subtab are active for all users, but the actions can be completely performed only by the users assigned with the required security levels.	-	-	X	X
		New/Compare/Available/Usage	X	X	X	X
	Defaults	Edit/Import	-	-	X	X
		Reset/Export	X	X	X	X
	WDMANS	Provisioning: Edit	-	-	X	X

		Provisioning: Reset	X	X	X	X
		Internal Patchcords: Create/Edit/Delete/Commit/ Default Patchcords	-	-	X	X
		Port Status: Launch ANS	-	-	X	X
		Node Setup: Setup/Edit	X	X	X	X
		Optical Side: Create/Edit/Delete	X	X	X	X
Inventory	-	Delete	-	-	X	X
		Reset	-	X	X	X

Maintenance	Database	Backup	-	X	X	X
		Restore	-	-	-	X
	Network	Routing Table: Retrieve	X	X	X	X
		RIP Routing Table: Retrieve	X	X	X	X
	OSI	IS-IS RIB: Refresh	X	X	X	X
		ES-IS RIB: Refresh	X	X	X	X
		TDC: TID to NSAP/Flush Dynamic Entries	-	X	X	X
		TDC: Refresh	X	X	X	X
	Software	Download/Cancel	-	X	X	X
		Activate/Revert	-	-	-	X
	Diagnostic	Node Diagnostic Logs	-	-	X	X
	Audit	Retrieve	-	-	-	X
		Archive	-	-	X	X
	DWDM	APC: Run/Disable/Refresh	-	X	X	X
		WDM Span Check: Retrieve Span Loss values/Edit/Reset	X	X	X	X
		ROADM Power Monitoring: Refresh	X	X	X	X
		PP-MESH Internal Patchcord: Refresh	X	X	X	X
		Install Without Metro Planner: Retrieve	X	X	X	X
		All Facilities: Mark/Refresh	X	X	X	X

Table 64: Security Levels - Network View, on page 870 shows the actions that each user privilege level can perform in network view. An X indicates the user is allowed to perform the action. A dash indicates that the user is not allowed to perform the action.

Table 64: Security Levels - Network View

CTC Tab	Subtab	[Subtab]: Actions	Retrieve/Security Super User/Security User	Maintenance	Provisioning	Superuser

Alarms	-	Synchronize/Filter/Delete	X	X	X	X
Conditions	-	Retrieve/Filter	X	X	X	X
History	-	Filter	X	X	X	X
Circuits	Circuits	Create/Edit/Delete	-	-	X	X
		Filter/Search	X	X	X	X
	Rolls	Complete/Force Valid Signal/Finish	-	-	X	X
Provisioning	Security	Users: Create/Delete/Clear Security Intrusion Alarm	-	-	-	X
		Users: Change	Same User	Same User	Same User	All Users
		Active logins: Logout/Retrieve Last Activity Time	-	-	-	X
		Policy: Change	-	-	-	X
	Alarm Profiles	New/Load/Store/DeleteThe action buttons in the subtab are active for all users, but the actions can be completely performed only by the users assigned with the required security levels	-	-	X	X
		Compare/Available/Usage	X	X	X	X
	BLSR (ANSI) MS-SPRing (ETSI)	Create/Edit/Delete/Upgrade	-	-	X	X
	Overhead Circuits	Create/Delete/Edit/Merge	-	-	X	X
		Search	X	X	X	X
	Provisionable Patchcords (PPC)	Create/Edit/Delete	-	-	X	X
	Server Trails	Create/Edit/Delete	-	-	X	X
	VLAN DB Profile	Load/Store/Merge/Circuits	X	X	X	X
		Add/Remove Rows	-	-	X	X

Maintenance	Software	Download/Cancel	-	X	X	X
	Diagnostic	OSPF Node Information: Retrieve/Clear	X	X	X	X
	APC	Run APC/Disable APC	-	-	X	X
		Refresh	X	X	X	X

Security Policies

Superusers can provision security policies on the . These security policies include idle user timeouts, password changes, password aging, and user lockout parameters.

Superuser Privileges for Provisioning Users

Superusers can grant permission to Provisioning users to perform a set of tasks. The tasks include retrieving audit logs, restoring databases, clearing PMs, and activating and reverting software loads. These privileges can be set only through CTC network element (NE) defaults, except the PM clearing privilege, which can be granted to Provisioning users using CTC Provisioning > Security > Access tabs. For more information on setting up Superuser privileges, refer to the .

Idle User Timeout

Each CTC or TL1 user can be idle during his or her login session for a specified amount of time before the CTC window is locked. The lockouts prevent unauthorized users from making changes. Higher-level users have shorter default idle periods and lower-level users have longer or unlimited default idle periods, as shown in Table 65: Default User Idle Times, on page 872.

Table 65: Default User Idle Times

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

User Password, Login, and Access Policies

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

- Password length, expiration and reuse—Superusers can configure the password length by using NE defaults. The password length, by default, is set to a minimum of six and a maximum of 20 characters.

You can configure the default values in CTC node view with the Provisioning > NE Defaults > Node > security > password Complexity tabs. The minimum length can be set to eight, ten or twelve characters, and the maximum length to 80 characters. The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters, where at least two characters are non alphabetic and at least one character is a special character. Superusers can specify when users must change their passwords and when they can reuse them.

- Locking out and disabling users—Superusers can provision the number of invalid logins that are allowed before locking out users and the length of time before inactive users are disabled. The number of allowed lockout attempts is set to the number of allowed login attempts.

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

User Accounts for Encryption and Authentication

Users' privileges are determined by these user account types:

- Security Super User- A security super user has privileges to set encryption and card authentication parameters. The security super user creates security users and associates each user with a WSE card. By default, at least one security super user must exist. Therefore, last security super user cannot be deleted and the last user's security level cannot be changed. However, the password can be reset.

The security super user can provision the encryption security feature on a pre-provisioned card. The security super user has these privileges:

- Create, delete, or edit the ‘Security User’ account
- Enable or disable card authentication
- Enable or disable payload encryption
- Reset the master key on each encrypted stream
- Provision AES secure packet

The security super user needs to authorize the security user after performing each of the following operations:

- Side switch of the controller card (resetting the active card to make the standby card as active)
- NE power cycle (power failure and recovery)
- Software upgrade
- Database restore
- Security Users—Security users are created by a security super user. The security users are associated to a WSE card through its serial number, and have these privileges:

- Enable or disable card authentication
- Enable or disable payload encryption
- Reset the master key on each encrypted stream

- Provision AES secure packet

Note The security user cannot configure encryption on a pre-provisioned card.

- Root User—The root user is Cisco Prime user with all the security and transport privileges mentioned in Table 63: Security Levels - Node View, on page 866 Table 64: Security Levels - Network View, on page 870. The root user is not supported in CTC or TL1. The security super user can enable the root user through CTC.

The following shows the actions that each user privilege level can perform. An X indicates the user is allowed to perform the action. A dash indicates that the user is not allowed to perform the action.

Table 66: Security Super User and Security User Privileges

Actions	Security Super User	Security User
Create Security Users	X	--
Assign security users to individual cards	X	--
Authenticate and authorize cards	X	X
Enable payload encryption and payload authentication	X	X
Configure Encryption on a pre-provisioned card	X	--
Reset session key and change the session key interval	X	X
Filter circuits	X	X
OTN overhead byte selection	X	--
Provision ICV mismatch threshold	X	--
Provision AES secure packet	X	X

Audit Trail

The Cisco maintains a Telcordia GR-839-CORE-compliant audit trail log that resides on the control cards. Audit trails are useful for maintaining security, recovering lost transactions and enforcing accountability. Accountability refers to tracing user activities; that is, associating a process or action with a specific user. This record shows who has accessed the system and what operations were performed during a given period

of time. The log includes authorized Cisco logins and logouts using the operating system command line interface, CTC, and TL1; the log also includes FTP actions, circuit creation/deletion, and user/system generated actions.

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

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

Audit Trail Log Entries

Table 67: Audit Trail Window Columns, on page 875 contains the columns listed in Audit Trail window.

Table 67: Audit Trail Window Columns

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

Audit trail records capture the following activities:

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

Audit Trail Capacities

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

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

RADIUS Security

Superusers can configure nodes to use Remote Authentication Dial In User Service (RADIUS) authentication. RADIUS uses a strategy known as authentication, authorization, and accounting (AAA) for verifying the identity of, granting access to, and tracking the actions of remote users. To configure RADIUS authentication, refer to the .

RADIUS server supports IPv6 addresses and can process authentication requests from a GNE or an ENE that uses IPv6 addresses.

RADIUS Authentication

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

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

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

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

Note In RADIUS authentication, the user can enter up to 39 characters for user name in CTC from R10.5. It includes alphanumeric (a-z, A-Z, 0-9) characters and the allowed special characters are @, " - " (hyphen), and " . " (dot).

Shared Secrets

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

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

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

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

When creating and using a shared secret:

- Use the same case-sensitive shared secret on both RADIUS devices.
- Use a different shared secret for each RADIUS server-RADIUS client pair.
- To ensure a random shared secret, generate a random sequence at least 22 characters long.
- You can use any standard alphanumeric and special characters.
- You can use a shared secret of up to 128 characters in length. To protect your server and your RADIUS clients from brute force attacks, use long shared secrets (more than 22 characters).
- Make the shared secret a random sequence of letters, numbers, and punctuation and change it often to protect your server and your RADIUS clients from dictionary attacks. Shared secrets should contain characters from each of the three groups listed in Table 68: Shared Secret Character Groups, on page 877.

Table 68: Shared Secret Character Groups

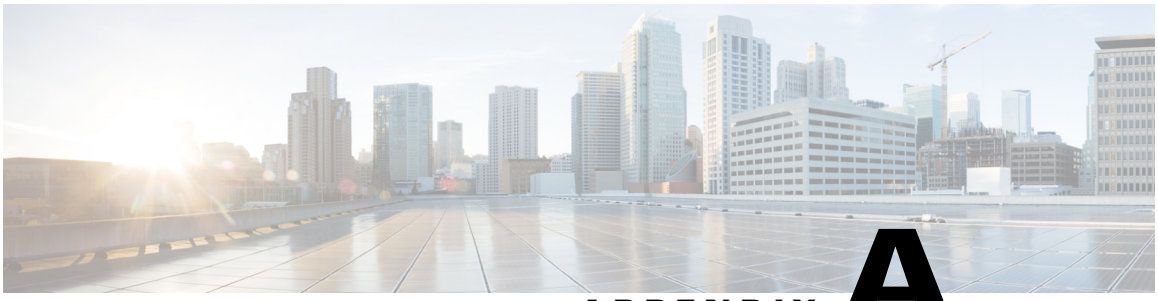
Group	Examples
Letters (uppercase and lowercase)	A, B, C, D and a, b, c, d
Numerals	0, 1, 2, 3
Symbols (all characters not defined as letters or numerals)	Exclamation point (!), asterisk (*), colon (:)

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

Procedure for Users and Security

This section lists the procedure related to users and security.

- NTP-G23 Create Users and Assign Security. Refer to the chapter "Turn Up a Node" in the .
- NTP-G88 Modify Users and Change Security



APPENDIX A

CPT Error Messages

This appendix describes the CPT error messages.

Error Messages

The following table lists all the error or warning message identifiers (IDs), messages, and a brief description of each message. The table lists two types of messages—error messages (EID-*nnnn*) and warning messages (WID-*nnnn*). Error messages are alerts that an unexpected or undesirable operation has occurred that either indicates the risk of traffic loss or an inability to properly manage devices in the network. Warnings are alerts that the requested operation could lead to an error. Warnings are sometimes used to convey important information.

Error/Warning ID	Error/Warning Message	Description
EID–1050	Connection failed on node {0}.	This error message is displayed when the nodes are disconnected in Layer2+ > Topology > Trace L2 Topology.
EID–3246	The wizard was not able to validate the data.	Refer to the error message text.
EID–4039	The MA profile does not exist.	Refer to the error message text.
EID–4046	Service ID syntax error: {0}.	This error message is displayed when you specify an invalid service ID format during Ethernet Virtual Circuit (EVC) query.
EID–5130	Connection failed on node {0}.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID–5148	Unable to set the SRLG for Router {0}.	This error message is displayed when you are unable to set the Shared Risk Link Group (SRLG) for the specified router.
EID–5190	Unable to trace Layer 2 topology. The root link may have been deleted.	This error message is displayed when the Layer 2 topology view is refreshed.
WID–5191	All the EFP configurations will be lost. Are you sure you want to continue?	This warning message is displayed when you click the Reset button in the EFP configuration dialog box. All the saved Ethernet Flow Point (EFP) configurations will be cleared.
WID–5192	The Label Data has changed. Please use Apply to save.	This warning message is displayed when you edit the Multiprotocol Label Switching – Transport Profile (MPLS–TP) labels and click Finish before saving them.
WID–5193	The Labels on the route could not be computed.	This warning message is displayed when CTC cannot compute the labels during MPLS–TP tunnel creation or LSP addition.
EID–5194	The MAC Address mentioned is invalid.	Refer to the error message text.
EID–5195	The Static MAC Address provisioning on EFP failed.	This error message is displayed when an error occurs while configuring a static MAC address on EFP.
WID–5196	You have not selected any nodes for discovery query. This may result in slow performance to discover the services of interest from the entire network. Do you wish to proceed?	This warning message is displayed when you have not selected any nodes during the Layer 2 services query. The query is issued to the entire network that slows down the discovery process.
EID–5197	The specified IP address is invalid.	This error message is displayed during an explicit path creation when the IP address specified for the unmanaged node is invalid.

Error/Warning ID	Error/Warning Message	Description
EID–5198	An interface has to be selected.	This error message is displayed during an explicit path creation when you do not specify the interface for each managed node.
EID–5199	TPE nodes cannot be used as SPE.	This error message is displayed during pseudowire creation. The Terminating Provider Edge (TPE) nodes that are used as source and destination nodes cannot be used as Switch Provider Edge (SPE) nodes.
EID–5200	A valid router ID must be selected.	This error message is displayed when you do not specify a valid router ID during Multiprotocol Label Switching – Traffic Engineering (MPLS-TE) tunnel creation or pseudowire creation.
EID–5201	A valid route cannot be found for the circuit creation request. Do you want to continue anyway?	This error message is displayed during pseudowire creation. This error message is displayed when there are no MPLS-TE or MPLS-TP tunnels that can be used by the pseudowire.
EID–5202	Sanity Check Failed on the LSP being added.	This error message is displayed when the labels modified by the user are incorrect.
EID–5203	EFP Configuration Error : {0}.	This error message is displayed when the outer VLAN Tag and the inner VLAN Tag tries to use same list/range simultaneously.
EID–5204	The Static MAC Address retrieval on EFP failed.	This error message is displayed when the EFP fails to retrieve the static MAC address.
EID–5205	Unable to clear the proactive protection on the router.	This error message is displayed during proactive protection clearing operation on Cisco ASR 9000 Series Router or Carrier Routing System.

Error/Warning ID	Error/Warning Message	Description
WID–5206	Unable to clear proactive protection on the router. Do it manually.	This warning message is displayed during proactive protection clearing operation on Cisco ASR 9000 Series Router or Carrier Routing System.
EID–5207	Specified Multicast IP Address does not fall within the valid range.	Refer to the error message text.
EID-5228	Deleting an LSP might impact the tunnel status	This error message is displayed when you try to delete an LSP. The following message is displayed in the warning dialog box: Deleting an LSP might impact the tunnel status. Do you want to delete the selected LSP?
WID–6506	Deleting the loopback interface the MPLS functionalities will be affected. Do you want to continue?	This warning message is displayed when you try to delete the loopback address.
WID–5239	It is not recommended to do any service provisioning on a dual-homed ring via PRC when the WRC is down. It may get lost when the WRC becomes active again. Do you wish to proceed?	This warning message is displayed when you try to provision any service on a CPT 50 in a ring through the PRC, when the WRC is down.
WID–5240	One or more selected services exist on a dual-homed ring where the WRC is down. It is not recommended to do any service provisioning on a dual-homed ring via PRC when the WRC is down. It may get lost when the WRC becomes active again. Do you wish to proceed?	This warning message is displayed when you try to provision the service that exist on a dual-homed ring through the PRC, when the WRC is down.
EID–6519	Only show commands are admitted.	This error message is displayed when you enter non-show commands.
EID–6520	BFD Template Name cannot be null.	This error message is displayed when you try to create a Bidirectional Fault Detection (BFD) template without entering the template name.

Error/Warning ID	Error/Warning Message	Description
EID–6521	BFD Template Multiplier cannot be null.	This error message is displayed when you try to create a BFD template without entering a value for the multiplier. The multiplier value specifies the number of consecutive BFD control packets that can be missed before BFD declares a peer as unavailable.
EID–6522	BFD Template Tx/Rx Interval cannot be null.	This error message is displayed when you try to create a BFD template without entering the values for the transmit and receive intervals.
EID–6523	Link Number cannot be null.	This error message is displayed when you try to configure a link without specifying the link number.
EID–6524	Port cannot be null.	This error message is displayed when the port is not selected under the Service Level Alarm tab in Packet Transport System View.
EID–6525	IP Address is invalid.	This error message is displayed when the next hop address specified during the link number configuration is invalid.
EID–6526	Static OAM Class name cannot be null.	This error message is displayed when you try to create a static OAM class without entering the class name.
EID–6527	Static OAM Timer values cannot be null.	This error message is displayed when you try to create a static OAM class without specifying how often the static OAM packets must be sent out.
EID–6528	MPLS Label Range cannot be null.	This error message is displayed when you do not specify a value for the minimum and maximum MPLS label range. The minimum and maximum label values specified apply to MPLS-TP tunnels and static pseudowires.

Error/Warning ID	Error/Warning Message	Description
EID–6529	MPLS Label Range must be from [16 - 8000].	This error message is displayed when you specify an MPLS label value that is outside the valid label range.
EID–6530	Fault OAM Refresh Timer cannot be null.	This error message is displayed when you try to configure the global settings for the MPLS-TP without specifying the value in the Refresh Timer field. The refresh timer field specifies how often the static OAM packets must be sent out.
EID–6531	Fault OAM Refresh Timer value must be between 1 and 255.	This error message is displayed when you try to configure the global settings for the MPLS-TP without specifying the valid values in the Refresh Timer field.
EID–6532	Node value specified is not valid.	Refer to the error message text.
EID–6533	BFD Interval range must be between 4 and 999 milliseconds.	This error message is displayed when you try to create a BFD template without entering valid values (in milliseconds) for the transmit and receive intervals.
EID–6534	BFD Interval range must be between 3300 and 999000 microseconds.	This error message is displayed when you try to create a BFD template without entering valid values (in microseconds) for the transmit and receive intervals.
EID–6535	BFD Template Multiplier must be between 3 and 50.	This error message is displayed when you try to create a BFD template without entering valid values for the multiplier. The multiplier value specifies the number of consecutive BFD control packets that can be missed before BFD declares a peer as unavailable. To enter value for BFD Template Multiplier follow the path: PTS view > Provisioning tab > MPLS TP > BFD Template. **Note** From Release 9.5.x BFD template multiplier must be between 2 and 50.

Error/Warning ID	Error/Warning Message	Description
EID–6536	The TE/TP Tunnel Number must be between 0 and 999.	This error message is displayed when you try to create a MPLS-TE or MPLS-TP tunnel without specifying the valid values for the tunnel number.
EID–6537	Pseudowire Class name cannot be null.	This error message is displayed when you try to create a pseudowire class without entering the class name.
EID–6538	Protocol should be None for TP Tunnel in the preferred path.	Refer to the error message text.
EID–6540	Either of Static OAM class and BFDoVCCV with status signalling can be used for signalling with static Tunnels.	Refer to the error message text.
EID–6541	BFDoVCCV cannot be used for status signalling with LDP based Tunnels.	Refer to the error message text.
EID–6542	Static OAM class cannot be used for signalling with LDP based Tunnels.	Refer to the error message text.
EID–6543	Syslog is not Enabled.	Refer to the error message text.
EID–6547	Valid License is not available on this card.	This error message is displayed during port creation when all the available licenses have been used.
EID–6548	License Operation Error.	This error message is displayed when you receive an unexpected error during the license operation. Some of the error situations are as follows: • Better license exists. • Duplicate license. • License is already revoked. • Precedence of the selected license line is in incorrect state. • Unique Device Identifier (UDI) in the license line does not match with the local UDI.

Error/Warning ID	Error/Warning Message	Description
EID–6550	The Product ID of the card does not support Licensing.	Refer to the error message text.
EID–6551	The card is not in provisioned state, hence this license data cannot be fetched currently.	This error message is displayed when the license data cannot be retrieved because the card is not provisioned.
EID–6552	License operation failed due to Communication failure with the line card.	Refer to the error message text.
EID–6553	Please select/enter valid values for InterfaceType/InterfaceNumber.	Refer to the error message text.
EID–6554	The MAC Address mentioned is invalid.	Refer to the error message text.
EID–6555	The minimum value of the range for H/W protected tunnels must be from 1-4095.	Refer to the error message text.
EID–6556	The maximum number of H/W protected tunnels is 1024.	Refer to the error message text.
EID–6558	Service Alarm cannot be null.	This error message is displayed when a service alarm is not selected before querying the service-level alarms.
EID–6559	Service Type cannot be null.	This error message is displayed when a service type is not selected before querying the service-level alarms.
EID–6560	Service ID cannot be null.	This error message is displayed when a service ID is not selected before querying the service-level alarms.
EID–6561	Selected router is not {0}.	This error message is displayed when a Cisco ASR 9000 Series Router or Carrier Routing System is not selected during control channel creation.
EID–6562	License file size has exceeded the limit.	This error message is displayed when the license file is larger than the maximum supported size.

Error/Warning ID	Error/Warning Message	Description
WID–6563	Removing the {0} might be traffic affecting. Do you want to continue?	This warning message is displayed when you try to delete targeted LDP sessions.
EID–6565	Cannot retrieve the MAC table from the node as either or both uplinks are not present or are in invalid state.	Refer to the error message text.
EID–6566	BFDoVCCV requires Control Word to be Enabled.	This error message is displayed when creating a pseudowire class. This error message is displayed when you enable BFD Control Channel over Virtual Circuit Connection Verification (VCCV) without enabling the control word.
EID–6567	Min Label cannot be more than Maximum Label.	Refer to the error message text.
EID–6568	Local label is in use.	This error message is displayed when the specified local label is already being used by an MPLS-TE or MPLS-TP tunnel. Use the other unused label.
EID–6569	Local label is out of range.	This error message is displayed when the specified local label is outside the MPLS static label range.
EID–6570	VC ID is in use.	This error message is displayed when the specified Virtual Circuit (VC) ID during pseudowire creation is already in use.
EID–6571	Either Next Hop or Unicast Tx-Mac required for Non-P2P (shared) Interface.	This error message is displayed when you try to configure a link without specifying the next hop IP address or MAC address.
EID–6399	The MIP Provisioning Failed.	Refer to the error message text.
EID–6401	The Provisioning Failed. An MIP or MEP is configured on the interface.	This error message is displayed when you try to delete the maintenance association (MA) profile that is associated with a Maintenance Intermediate Point (MIP) or Maintenance End Point (MEP).

Error/Warning ID	Error/Warning Message	Description
EID–6620	The {0} field cannot exceed {1} characters.	This error message is displayed when the length of the maintenance domain name or maintenance association profile name exceeds the threshold value.
EID–6624	The start interval cannot exceed hold interval and hold interval cannot exceed maximum interval.	This error message is displayed when the start interval and hold interval values in Link-state Advertisement (LSA) and Shortest Path First (SPF) areas exceed the hold interval and maximum interval values respectively.
EID–5220	MA Profile name should not exceed 50 characters.	This error message is displayed when the length of MA profile name exceeds 50 characters.
EID–5222	An error occurred while deleting the NEIGHBOR.	This error message is displayed when you try to delete a neighbor pseudowire for a given node in the Edit > End Point Pseudowire tab of the Virtual Private LAN Service (VPLS) circuit.
EID–5223	The last NEIGHBOR cannot be deleted.	This error message is displayed when you try to delete the last neighbor pseudowire for a given node in the Edit > End Point Pseudowire tab of the VPLS circuit.
EID–6599	The selected bandwidth is not available.	This error message is displayed when the bandwidth of the pseudowire exceeds the available bandwidth on the MPLS–TE or MPLS–TP tunnel.
EID–6621	MP-ID cannot be Empty.	This error message is displayed when a value to query for Connectivity Fault Management (CFM) based on Maintenance Point Identifier (MP ID) is not entered in the MP ID field of the Maintenance > Service Statistics tab.

Error/Warning ID	Error/Warning Message	Description
EID–6622	VC-ID cannot be Empty.	This error message is displayed when a value to query for MPLS statistics is not entered in the VC ID field of the Maintenance > Service Statistics tab.
EID–6623	Service Name cannot be Empty.	This error message is displayed when a value to query for CFM based on the domain name and service name is not entered in the Service Name field of the Maintenance > Service Statistics tab.
EID–2016	Circuit deletion failed.	This error message is displayed when you try to delete a VPLS circuit that has some EFPs associated.
EID–6610	The MPID Number must be between 1 and 8191.	This error message is displayed when an incorrect value is entered in the MP ID field of the Maintenance > OAM tab during the ping operation for an EVC service.
EID–6611	The COS Number must be between 0 and 7.	This error message is displayed when an incorrect value is entered in the COS field of the Maintenance > OAM tab during the ping operation for an EVC service.
EID–6612	The Source Number must be between 1 and 8191.	This error message is displayed when an incorrect value is entered in the Source field of Maintenance > OAM tab during the ping operation for an EVC service.
EID–6617	Discard Class value should be between 0 to 2.	This error message is displayed when an incorrect value is entered in the Discard Class field of Provisioning > QoS > Table Map > Create Table Map.

Error/Warning ID	Error/Warning Message	Description
EID–6618	Qos Group value should be between 0 to 7.	This error message is displayed when an incorrect value is entered in the QoS Group field of Provisioning > QoS > Table Map > Create Table Map.
EID–6613	Qos Group value should be less than 8.	This error message is displayed when an incorrect value is entered in the QoS Group field of Provisioning > QoS > Table Map > Create Table Map.
EID-6626	FOG deletion failed	This error message is displayed when an attempt to delete a Fan-Out Group (FOG) has failed.
EID-6627	No {0} was configured	This error message is displayed when a port span is created with an incorrect span source, EFP span source, or a span destination. The {0} in the error message is a: • Source, if a port span is created without configuring a span source. • EFP Source, if an EFP span is created without configuring any EFP source. • Destination, if a span is created without configuring any span destination. To enter a value for span source, EFP source, and destination follow the path: PTS view> Provisioning> Span> Create
EID-6628	The Service ID field cannot be empty	This error message is displayed when there is no value entered in the service ID field.
EID-6629	The {0} interface is in use.\n	This error message is displayed when a attempt is made to reuse an already in-use interface.

Error/Warning ID	Error/Warning Message	Description
EID-6630	Ip SLA ID must be in the range 1-2147483647	This error message is displayed when the Ip SLA ID value entered is outside the defined range. To enter a value in the Ip SLA ID field follow the path: PTS view > DM Config> Provisioning tab > Y1731 tab > Delay Measurement tab > Configuration tab.
EID-6631	Domain name cannot be empty	This error message is displayed when no domain name is specified. To enter a value in the domain name field, follow the path: PTS view > DM Config> Provisioning tab > Y1731 tab > Delay Measurement tab > Configuration tab
EID-6632	Age out must be in the range 1-2073600	This error message is displayed when the Ageout value entered is outside the defined range. To enter a value in the Ageout field, follow the path: PTS view > DM Config > Provisioning tab > Y1731 tab > Delay Measurement tab > Schedule tab with Ageout value beyond the range 1-2073600.
EID-6633	Life value must be entered	This error message is displayed when there is no value entered in the Life field. To enter a value in the Life field, follow the path: PTS view > DM Config > Provisioning tab > Y1731 tab > Delay Measurement tab > Schedule tab with no value in the Life field.
EID-6634	Frame size must be in the range 64-384	This error message is displayed when the frame size value you have entered is outside the defined range. To enter a value in the Frame size field, follow the path: PTS view > DM Config> Provisioning tab > Y1731 tab > Delay Measurement tab > Configuration tab.

Error/Warning ID	Error/Warning Message	Description
EID-6635	Frame interval must be 100 msec or 1 sec	This error message is displayed when an invalid frame interval value is entered. To enter a value in the Frame interval field, follow the path: PTS view > DM Config> Provisioning tab > Y1731 tab > Delay Measurement tab > Configuration tab.
EID-6636	Aggregate interval must be in the range 1-65535	This error message is displayed when the aggregate interval value entered is outside the defined range. To enter a value in the Aggregate Interval Value field, follow the path: PTS view > DM Config> Provisioning tab > Y1731 tab > Delay Measurement tab > Configuration tab.
EID-6637	Maximum delay must be in the range 1-65535	This error message is displayed when the maximum delay value entered is outside the defined range. To enter a value in the Maximum Delay value field, follow the path: PTS view > DM Config> Provisioning tab > Y1731 tab > Delay Measurement tab > Configuration tab.
EID-6642	CFM Disabled on Interface	This error message is displayed when CFM is disabled on the interface. To enable CFM, click Provisioning > CFM > Global Settings > Ethernet Interfaces > Enable CFM
EID-6644	No Such Service	This error message is displayed when CTC queries for a service, that does not exist.

Error/Warning ID	Error/Warning Message	Description
EID-6645	Enter proper Service ID	This error message is displayed when a invalid value is entered in the Service ID field. To enter the Service ID, follow the path: PTS view> provisioning > Y1731 > Configuration tab.
EID-6646	Fog Name length should be less than 255 characters	This error message is displayed when the name length of the Fan-Out group exceed the defined characters limit.
EID-6648	The minimum threshold cannot be empty	This error message is displayed when the value in the Reaction Type field is specified as Immediate and no value is entered in the Falling Threshold field. To configure the Reaction type and Falling Threshold fields, follow the path: PTS view > DM Config > Provisioning tab > Y1731 tab > Delay Measurement tab > Configuration tab.
EID-6649	The maximum threshold cannot be empty	This error message is displayed when the value in the Reaction Type field is specified as Immediate and no value is entered in the Rising Threshold field. To configure the Reaction Type and Rising Threshold fields, follow the path: PTS view > DM Config > Provisioning tab > Y1731 tab > Delay Measurement tab > Configuration tab.

Error/Warning ID	Error/Warning Message	Description
EID-6653	Minimum threshold value must be in the range 1-60000	This error message is displayed when the value in the Reaction Type field is specified as Immediate and the value specified in the Falling Threshold field is outside the defined range that is, 1-60000. To configure the Reaction type and Falling Threshold fields, follow the path: PTS view > DM Config Provisioning tab > Y1731 tab > Delay Measurement tab > Configuration tab.
EID-6654	Maximum threshold value must be in the range 1-60000	This error message is displayed when the value in the Reaction type field is specified as Immediate and value specified in the Rising Threshold field is outside the defined range that is, 1-60000. To configure the Reaction type and Rising Threshold fields, follow the path: PTS view > DM Config> Provisioning tab > Y1731 tab > Delay Measurement tab > Configuration tab.
EID-2099	An error occurred while ring switching	Refer to the error message text.
EID-2113	The extension byte for the ring cannot be set	Refer to the error message text.
EID-2116	The extension byte setting for the ring is invalid	Refer to the error message text.
EID-2118	The ring cannot be deleted. A protection operation is set. All protection operations must be clear for ring to be deleted.	Refer to the error message text.
EID-2121	The ring cannot be upgraded	This error message is displayed when the CPT 50 upgrade is been initiated which are present inside a ring but failed.
EID-2122	The ring speed for is inadequate for the upgrade procedure. Only 0 or higher 1 can be upgraded to four-fiber	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-2130	The ring ID value is not valid. Please enter a valid number between 0 and 9999	Refer to the error message text.
EID-2207	You cannot add this span. Either the ring name is too long that is, ring name length is greater than 0 or the endpoints do not support alphanumeric IDs.	Refer to the error message text.
EID-5244	It is not recommended to do any service provisioning on a dual-homed ring via PRC when the WRC is down. It may get lost when the WRC becomes active again. Do you wish to proceed	Refer to the error message text.
EID-5245	One or more selected services exist on a dual-homed ring where the WRC is down. It is not recommended to do any service provisioning on a dual-homed ring via PRC when the WRC is down. It may get lost when the WRC becomes active again. Do you wish to proceed	Refer to the error message text.
EID-4055	Disable the service state before upgrading the CPT50	This error message is displayed when the CPT 50 needs to be upgraded but since the service state is enabled on that CPT 50, it cannot be upgraded.
EID-4058	Invalid Device Identifier	This error message is displayed when the device identifier entered is incorrect.
EID-4059	Invalid Device Description	This error message is displayed when the device description entered is incorrect.
EID-4061	CPT50 with same Device Identifier already exists	This error message is displayed when the device identifier entered for a particular CPT 50 already exists.
EID-6693	CPT50 deletion failed	This error message is displayed when the deletion of CPT 50 is attempted but unsuccessful.

Error/Warning ID	Error/Warning Message	Description
EID-6694	Maximum number of CPT50s allowed in a ring is 0	Refer to the error message text.
EID-6696	The corresponding CPT 50 box is not connected physically. Connect the CPT 50 with the given ID to open its PTS view	Refer to the error message text.
EID-6704	Device Identifier length cannot excced 31 characters	This error message is displayed when the entered device identifier length is greater than 31 characters.
EID-6705	Device Description length cannot exceed 31 characters	This error message is displayed when the entered device description length is greater than 31 characters.
EID-6706	The maximum number of CPT50s that can be upgraded simultaneously is 10.Please select upto 10 CPT50s for upgrade	Refer to the error message text.
EID-6695	CPT50 deletion failed due to one of the following reason. CPT50 is busy. Please try again later. Services are configured on the CPT50. Delete service and then try again later	Refer to the error message text.
EID-6701	Ring deletion failed as CPT50 are available in the segment	This error message is displayed when the deletion of a particular ring is attempted but unsuccessful since CPT 50s are present inside the ring.
EID-4062	Node role should be set as single home to create single-homed rings	This error message is displayed when the dingle home ring creation is initiated and the node role has not been selected as single-homed.
EID-6690	Port is already used in rings, OTN should not be enabled	This error message is displayed when the specific ports are already used in ring configuration and cannot be considered as OTN ports.
EID-6691	You cannot select XFP ports as east and west port in a Ring	This error message is displayed when you select XFP ports for creating ring.

Error/Warning ID	Error/Warning Message	Description
EID-6692	REP cannot be enabled on Ring Ports	This error message is displayed when the user tries to enable REP on the ring ports.
EID-6698	No actual ring exist corresponding to the selected preprovisioned ring	Refer to the error message text.
EID-4057	East port cannot be same as west port in a Ring	This error message is displayed when the east port is selected same as west port or vice-versa.
EID-4060	Ring deletion failed	This error message is displayed when the deletion of ring is initiated and is unsuccessful.
EID-6702	Ring deletion failed as no segment exists with given segment id	This error message is displayed when the ring deletion is initiated for a particular segment id which does not exists.
EID-6703	The Ring Name length cannot exceed 49 characters	This error message is displayed when the ring name entered is exceeding 49 characters.
EID-4056	Please provide node role for WRC/PRC	Refer to the error message text.
EID-6699	No actual topology exists since PRC is standby and WRC is down	Refer to the error message text.
EID-6700	No actual topology exists at CTC since both WRC and PRC are down/not present in the network	Refer to the error message text.
EID-6778	It is not recommended to do any provisioning on a dual-homed ring via PRC when WRC is down. It would be lost when WRC becomes active again.Do you wish to continue	Refer to the error message text.
EID-6777	WRC is already Active hence switchover not allowed	This error message is displayed when the switchover for a WRC node is initiated which is already in active state.
EID-6687	CPT50 with same Device Identifier already exists	This error message is displayed when the device identifier entered for a particular CPT 50 already exist.

Error/Warning ID	Error/Warning Message	Description
EID-6697	CPT50 deletion failed	Refer to the error message text.
EID-6733	The corresponding CPT 50 box is not connected physically. Connect the CPT 50 with the given ID to open its PTS view.	This error message is displayed when the PTS view is not getting opened for a particular CPT 50. It is connected in a ring but it is not physically connected to the node.
EID-6699	Services are configured/other configurations done on CPT50	Refer to the error message text.
EID-6790	Dynamic services are configured within the modified label range. Need to Reload the PTF card/CPT50	Refer to the error message text.
EID-3161	An error occurred while upgrading the ring.	This error message is displayed when the user tries to upgrade the already created ring but it failed in some circumstance.
EID-3361	The ring termination is in use. An error occurred while deleting the ring termination	This error message is displayed when the ring deletion is attempted for a ring which is in use.
EID-3362	An error occurred while deleting the ring termination	This error message is displayed when the ring termination deletion is attempted but failed.
EID-3363	No ring terminations were selected	Refer to the error message text.
EID-3364	An error occurred while creating the ring ID	This error message is displayed when the ring creation is in process but system is unable to assign the unique Ring ID for the newly created ring from the available pool.
EID-6693	Port is already used in rings, OTN should not be enabled	This error message is displayed when the specific ports are already used in ring configuration and cannot be considered as OTN ports.
EID-6694	OTN is enabled on this port. Disable OTN to use the port in ring creation	This error message is displayed when during ring creation, OTN ports are selected for ring ports but it is not allowed. OTN needs to be disabled on those ports for ring creation.

Error/Warning ID	Error/Warning Message	Description
EID-6698	Maximum number of CPT50s allowed in a ring is 40	Refer to the error message text.
EID-6730	A single home ring exists, so node role cannot be changed	This error message is displayed when the node role change is being performed but the single-homed ring is created for that node.
EID-6731	A Dual home ring exists, so node role and Peer IP cannot be changed	This error message is displayed when the modification of node role and Peer IP is performed but the Dual home ring already exist on that node.
EID-6732	Single home node should have peer ip as 0.0.0.0	This error message is displayed when the Peer IP is set different from 0.0.0.0 for single-homed ring.
EID-6733	The corresponding CPT 50 box is not connected physically.\n Connect the CPT 50 with the given ID to open its PTS view	Refer to the error message text.
EID-6736	No ring exists on this ring Id and slot/port.	This error message is displayed when the ring id does not exist in the database.
EID-6738	Inter link port exists on ring ports	Refer to the error message text.
EID-6739	An IClink is configured,So Node Role and Peer IP cannot be changed	This error message is displayed when the editing of node role and peer ip is attempted for the node where IClink exist.
EID-6788	IP Address cannot be assigned on the ring core port	Refer to the error message text.
EID-6789	It is not recommended to change the peer IP of the node on which the dual home ring is already created. Do you still wish to continue	Refer to the error message text.
EID-6682	Invalid Ring name	This error message is displayed when the device identifier entered does not match the valid criteria.

Error/Warning ID	Error/Warning Message	Description
EID-6683	East port cannot be same as west port in a Ring	This error message is displayed when the west port is selected similar to the east port while dual-homed ring creation.
EID-6685	Invalid CPT50 location	This error message is displayed when the device location for CPT 50 entered is incorrect.
EID-6686	Ring deletion failed	This error message is displayed when the attempt to delete a ring is failed.
EID-6710	You cannot select XFP ports as east and west port in a Ring	This error message is displayed when the XFP ports are selected as east or west port during ring creation.
EID-6728	Ring cannot be deleted since the Ring Preview/Show Actual topology window is already opened for this Ring.	Refer to the error message text.
EID-6303	Functional View Initialization Error.	This error message is displayed when the functional view of CTC is not getting open.
EID-2009	CTC was unable to download the package.	This error message is displayed when the CTC is unable to download the package due to some error.
EID-2023	CTC was unable to create a new user.	Refer to the error message text.
EID-2025	This feature cannot be used. Verify that each endpoint of this circuit is running software that supports this feature.	Refer to the error message text.
EID-2029	The requested operation is not supported.	This error message is displayed whenever you try to perform any operation which is not supported.
EID-2030	An error occurred during provisioning.	This error message is displayed in general whenever there is any provisioning error and provisioning is not done.

Error/Warning ID	Error/Warning Message	Description
EID-2033	An error occurred during validation.	This error message is displayed when the parameters entered during provisioning are incorrect.
EID-2056	A communication error occurred.	This error message is displayed when some internal error occurred during internal communication between the cards.
EID-2094	The password and confirmed password fields do not match.	Refer to the error message text.
EID-2095	The password is invalid.	Refer to the error message text.
EID-2126	An error occurred while provisioning the OSPF area.	Refer to the error message text.
EID-2186	The software download failed on node.	This error message is displayed when the user is trying to download a new software package on the node but it failed.
EID-2210	No package name was selected.	Refer to the error message text.
EID-2211	No node was selected for upgrade.	This error message is displayed when a user clicks on the upgrade button for PBR upgrade but no PBR is selected from the list.
EID-2215	An error occurred while leaving the page.	Refer to the error message text.
EID-2216	"An error occurred while entering the page.	Refer to the error message text.
EID-3041	An error occurred while applying the changes.	This error message is displayed when the provisioning changes has not been saved after clicking the apply button due to some internal error.
EID-3051	An error occurred while trying to save the file to your local file system.	Refer to the error message text.
EID-3215	An error occurred while refreshing.	This error message is displayed when you click the Refresh button but internal error occurred during refresh of the CTC pane.

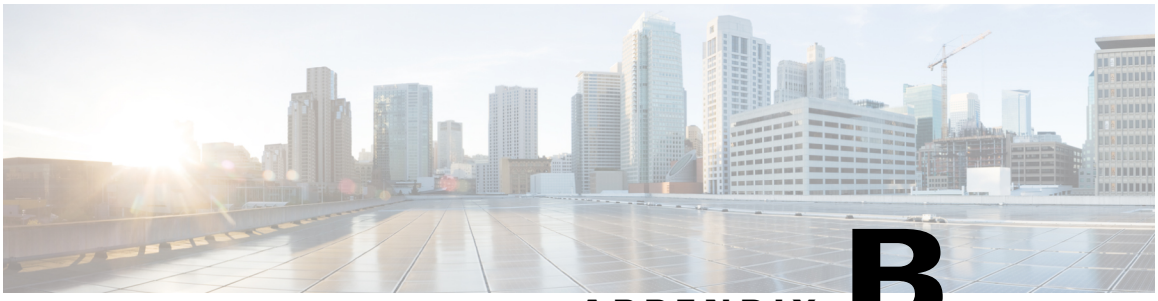
Error/Warning ID	Error/Warning Message	Description
EID-3227	A baseline could not be recorded. Performance metrics will remain unchanged.	Refer to the error message text.
EID-3252	No download has been initiated from this CTC session.	This error message is displayed when you click the cancel button in the Maintenance > Software tab and no download is in progress.
EID-3253	The reboot operation failed.	This error message is displayed when you try to reboot the CPT node but the operation failed due to internal error.
EID-4011	An error occurred during provisioning.	This error message is displayed when there is an internal error occurred during any provisioning on the CPT node.
EID-4037	Maximum number of MA Profiles already provisioned on the card.	This error message is displayed when the maximum number of MA profiles has already been provisioned on the card and the user is trying to create a new one.
EID-4038	The MA Profile already exists on the card.	This error message is displayed when you are trying to create a MA profile with the same name that already exist in the database.
EID-4040	The Domain Profile does not exist.	Refer to the error message text.
EID-4041	The Domain Profile already exists.	Refer to the error message text.
EID-4042	Maximum number of Domains exceeded.	Refer to the error message text.
EID-6697	EFP in VPLS circuit cannot be added on SPE Node.	Refer to the error message text.
EID-6699	No actual topology exists since PRC is standby and WRC is down.	Refer to the error message text.
EID-6700	No actual topology exists at CTC since both WRC and PRC are down/not present in the network.	Refer to the error message text.
EID-6702	Ring deletion failed as no segment exists with given segment id.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-6707	Vlan Edit not allowed as Service has CFM configured.	Refer to the error message text.
EID-6708	Vlan Edit not allowed as Service has Span configured.	Refer to the error message text.
EID-6709	Vlan Edit not allowed as Service has Y1731 configured.	Refer to the error message text.
EID-6710	Vlan Edit not allowed as Service has Qos configured.	Refer to the error message text.
EID-6711	Vlan Edit not allowed as Service has Mac configured.	Refer to the error message text.
EID-6677	Services exist on this port. Therefore, delete all services from this port before configuring TDM	This error message is displayed when the E1-CES or E3-CES pluggable is configured on the port where the services, which are not compatible with E1-CES or E3-CES pluggable, already exist.
EID-6678	Invalid Ring device identifier	This error message is displayed when the identifier entered in the Device Identifier field contains more than 50 characters, any special character, or only numerals.
EID-6679	East port cannot be same as west port in a Ring	This error message is displayed when you select the east port same as the west port while creating a ring with the topology type as Ring.
EID-6680	Invalid CPT 50 device identifier	This error message is displayed when the device identifier of CPT 50 entered in the Device Identifier field of the CPT 50 Attribute dialog contains more than 50 characters, any special characters, or only numerals.
EID-6681	Invalid CPT 50 location	This error message is displayed when the location of CPT 50 entered in the Location field of the CPT 50 Attribute dialog contains more than 50 characters.

Error/Warning ID	Error/Warning Message	Description
EID-6682	Ring deletion failed	This error message is displayed when you delete the ring on which a CPT 50 is already configured.
EID-6683	CPT 50 with the same device identifier already exists	This error message is displayed when you assign the name and location to a new CPT 50, same as the previously added CPT 50.
EID-6684	PWE with dynamic tunnel is not supported over TDM interface	This error message is displayed when pseudowire is created over the E1-CES or E3-CES interface and associated pseudowire class has TE as the tunnel type.
EID-6685	PWE with BFDoVCC is not supported over TDM interface	This error message is displayed when pseudowire is created over the E1-CES or E3-CES interface and associated pseudowire class is BFDoVCC enabled.
EID-6686	PWE with dynamic protocol is not supported over TDM interface	This error message is displayed when pseudowire is created over the E1-CES or E3-CES interface and the associated pseudowire class has LDP protocol.
EID-6687	PWE with OAM class is not supported over TDM interface	This error message is displayed when pseudowire is created over the E1-CES or E3-CES interfaceE1-CES or E3-CES pluggable and the associated pseudowire class is OAM enabled .
EID-6688	PWE with packet sequencing is not supported over TDM interface	This error message is displayed when pseudowire is created over the E1-CES or E3-CES interface and the associated pseudowire class is sequencing enabled.
EID-6690	Port is already in use. Delete the ring to configure the OTN on this port	This error message is displayed when you enable OTN on the port where ring is already created.
EID-6691	Port is already in use. Disable the OTN to create a ring on this port	This error message is displayed when you create a ring on the port where OTN is enabled.

Error/Warning ID	Error/Warning Message	Description
EID-6695	Maximum number of CPT 50s allowed in a ring, is 20	This error message is displayed when you add more than 20 CPT 50s, in a ring.
EID-6733	The corresponding CPT 50 box is not connected physically. Connect the CPT 50 with the given ID to open its PTS view.	This error message is displayed when you add more than 20 CPT 50s, in a ring.
EID-6729	Peer IP should not be same as Node IP	This error message is displayed when you entered the peer node IP same as the WRC IP.
EID-6730	A single home ring exists, so node role cannot be changed	This error message is displayed when a ring is already created on the node.
EID-6731	A Dual home ring exists, so node role cannot be changed	This error message is displayed when you modify the node role of a node where a dual-homed ring is already configured.
EID-6737	Inter link port already exists	This error message is displayed when you configure a new interconnect (IC) link on the node where an IC link is already configured.
EID-6738	Inter link port exists on ring ports	This error message is displayed when you configure a dual-homed ring on the node where an IC link is already configured.
EID-6739	An IC link is configured so Node Role and Peer IP can not be changed	This error message is displayed when you modify either the node role or the peer IP address of a node where a dual-homed ring is already configured.
EID-6677	Services exist on this port. Therefore, delete all services from this port before configuring TDM	This error message is displayed when the TDM pluggable is configured on the port where the services, which are not compatible with TDM, already exist.

Error/Warning ID	Error/Warning Message	Description
EID-6684	PWE with dynamic tunnel is not supported over TDM interface	This error message is displayed when pseudowire is created over the TDM interface and associated pseudowire class has TE as the tunnel type.
EID-6685	PWE with BFDoVCC is not supported over TDM interface	This error message is displayed when pseudowire is created over the TDM interface and associated pseudowire class is BFDoVCC enabled.
EID-6686	PWE with dynamic protocol is not supported over TDM interface	This error message is displayed when pseudowire is created over the TDM interface and the associated pseudowire class has LDP protocol.
EID-6687	PWE with OAM class is not supported over TDM interface	This error message is displayed when pseudowire is created over the TDM interface and the associated pseudowire class is OAM enabled.
EID-6688	PWE with packet sequencing is not supported over TDM interface	This error message is displayed when pseudowire is created over the TDM interface and the associated pseudowire class is sequencing enabled.
WID-5238	For node on which Vty option is enabled, Manually logout or kill the sessions	This error message is displayed when the Vty option is enabled and at the time of deleting the user, Logout before delete option is checked.
WID–6748	It is not recommended to do any provisioning on a dual-homed ring via PRC when the WRC is down. It would be lost when the WRC becomes active again. Do you wish to proceed?	This warning message is displayed when you try to provision any CPT 50 in a dual-homed ring through the PRC, when the WRC is down.



APPENDIX B

Support for MSTP Cards

This appendix lists the MSTP cards supported in the CPT 200 and CPT 600 chassis.

Support for MSTP Cards

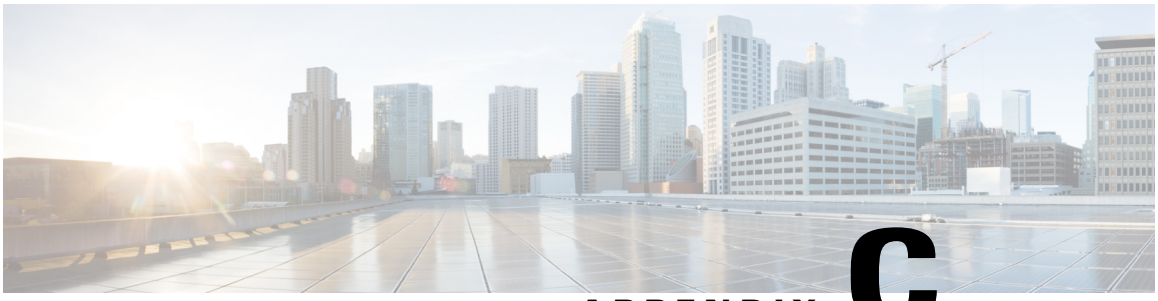
The CPT system supports Multiservice Transport Platform (MSTP) cards, thereby eliminating the requirement of a separate chassis for these DWDM cards.

Note CPT does not support multishelf management for these MSTP cards.

The following table lists the MSTP cards supported in the CPT 200 and CPT 600 chassis and provides references for more information about these MSTP cards.

MSTP Card	Where Documented
15454-40-SMR2-C=	15454-40-SMR2-C
15454-40-SMR1-C=	15454-40-SMR1-C
15454-AR-XP=	15454-AR-XP
15454-AR-XP-LIC=	15454-AR-XP-LIC
15454-AR-MXP=	15454-AR-MXP
15454-AR-MXP-LIC=	15454-AR-MXP-LIC
15454-OTU2-XP=	15454-OTU2-XP
15454-ADM-10G=	15454-ADM-10G
15454-OPT-AMP-17C=	15454-OPT-AMP-17C

MSTP Card	Where Documented
15454-OPT-AMP-C=	15454-OPT-AMP-C
15216-MD-40-ODD=	15216-MD-40-ODD
15216-MD-40-EVEN=	15216-MD-40-EVEN
15216-FLD-4-30.3=	15216-FLD-4-30.3
15216-FLD-4-33.4=	15216-FLD-4-30.4
15216-FLD-4-36.6=	15216-FLD-4-36.6
15216-FLD-4-39.7=	15216-FLD-4-39.7
15216-FLD-4-42.9=	15216-FLD-4-42.9
15216-FLD-4-46.1=	15216-FLD-4-46.1
15216-FLD-4-49.3=	15216-FLD-4-49.3
15216-FLD-4-52.5=	15216-FLD-4-52.5
15216-FLD-4-55.7=	15216-FLD-4-55.7
15216-FLD-4-58.9=	15216-FLD-4-58.9
15454-M-100G-LC-C=	15454-M-100G-LC-C
15454-M-CFP-LC=	15454-M-CFP-LC
15454-M10X10G-LC	15454-M10X10G-LC



APPENDIX C

Network Element Defaults

This appendix discusses the network elements that are supported on CPT 200 and CPT 600 platforms.

Network Element Defaults

This appendix describes the factory-configured (default) network element (NE) settings for the CPT 200 and CPT 600 platforms. It includes descriptions of card, node, and Cisco Transport Controller (CTC) default settings.

The NE defaults are preinstalled on each TNC and TSC cards. Cisco also ships a file named CPT200-Defaults.txt and CPT600-Defaults.txt on the CTC software CD if you want to import the defaults onto existing TNC and TSC cards. The NE defaults include card-level, CTC, and node-level defaults.

Manual card provisioning overrides default settings. If you use the CTC Defaults editor (on the node view Provisioning > Defaults tabs) or import a new defaults file, any changes to card or port settings that result only affect cards that are installed or preprovisioned after the defaults have changed.

Note Changing some node-level provisioning through NE defaults can cause CTC disconnection or a reboot of the node in order for the provisioning to take effect. Before you change a default, check in the Side Effects column of the Defaults editor (right-click a column header and select **Show Column > Side Effects**) and be prepared for the occurrence of any side effects listed for that default.

CPT 200 Network Element Default Settings

The following table lists the network element default settings for CPT 200.

Table 69: CPT 200 Network Element Default Settings

Default Name	Default Value	Default Domain
CTC.circuits. RouteAutomaticallyDefaultOverridable	TRUE	TRUE; FALSE
CTC.network.Map	United States	-none-; Germany; Japan; Netherlands; South Korea; United Kingdom; United States
NODE.circuits.SendPDIP	FALSE	TRUE; FALSE
NODE.circuits.State	IS;AINS	IS; OOS;DSBLD; OOS;MT; IS;AINS
NODE.general. AllowServiceAffectingPortChangeToDisabled	TRUE	FALSE; TRUE
NODE.general.AutoPM	FALSE	FALSE; TRUE
NODE.general.DefaultsDescription	Factory Defaults	Free form field
NODE.general.InsertAISVOnSDP	FALSE	TRUE; FALSE
NODE.general.NtpSntpServer	0.0.0.0	IP Address
NODE.general.RaiseConditionOnEmptySlot	FALSE	TRUE; FALSE
NODE.general. ReportLoopbackConditionsOnOOS-MTPorts	FALSE	FALSE; TRUE
NODE.general.SDPBER	1.00E-06	1E-5; 1E-6; 1E-7; 1E-8; 1E-9

Default Name	Default Value	Default Domain
NODE.general.TimeZone	(GMT-08:00) Pacific Time (US & Canada); Tijuana	

Default Name	Default Value	Default Domain
		(GMT-11:00) Midway Islands; Samoa; (GMT-10:00) Hawaiian Islands; Tahiti; (GMT-09:00) Anchorage - Alaska; (GMT-08:00) Pacific Time (US & Canada); Tijuana; (GMT-07:00) Mountain Time (US & Canada); (GMT-07:00) Phoenix - Arizona; (GMT-06:00) Central Time (US & Canada); (GMT-06:00) Mexico City; (GMT-06:00) Costa Rica; Managua; San Salvador; (GMT-06:00) Saskatchewan; (GMT-05:00) Bogota; Lima; Quito; (GMT-05:00) Eastern Time (US & Canada); (GMT-05:00) Havana; (GMT-05:00) Indiana (US); (GMT-04:00) Asuncion; (GMT-04:00) Caracas; La Paz; San Juan; (GMT-04:00) Atlantic Time (Canada); Halifax; Saint John; Charlottetown; (GMT-04:00) Santiago; (GMT-04:00) Thule (Qaanaaq); (GMT-03:30) St. John's - Newfoundland; (GMT-03:00) Brasilia; Rio de Janeiro; Sao Paulo; (GMT-03:00) Buenos Aires; Georgetown; (GMT-03:00) Godthab (Nuuk) - Greenland; (GMT-02:00) Mid-Atlantic; (GMT-01:00) Azores; Scoresbysund; (GMT-01:00) Praia - Cape Verde; (GMT 00:00) Casablanca; Reykjavik; Monrovia; (GMT) Greenwich Mean Time; (GMT 00:00) Dublin; Edinburgh; London; Lisbon; (GMT+01:00) Amsterdam; Berlin; Rome; Stockholm; Paris; (GMT+01:00) Belgrade; Bratislava; Budapest; Ljubljana; Prague; (GMT+01:00) Brussels; Copenhagen; Madrid; Vienna; (GMT+01:00) Sarajevo; Skopje; Sofija; Vilnius; Warsaw; Zagreb; (GMT+01:00) West Central Africa; Algiers; Lagos; Luanda; (GMT+01:00) Windhoek (Namibia); (GMT+02:00) Al Jizah; Alexandria; Cairo; (GMT+02:00) Amman; (GMT+02:00) Athens; Bucharest; Istanbul; (GMT+02:00) Beirut; (GMT+02:00) Cape Town; Harare; Johannesburg; Pretoria; (GMT+02:00) Jerusalem; (GMT+02:00) Kaliningrad; Minsk; (GMT+03:00) Aden; Antananarivo; Khartoum; Nairobi; (GMT+03:00) Baghdad; (GMT+03:00) Kuwait; Riyadh; (GMT+03:00) Moscow; St. Petersburg; Novgorod; (GMT+03:30) Tehran; (GMT+04:00) Abu Dhabi; Mauritius; Muscat; (GMT+04:00) Aqtau; T'bilisi; (GMT+04:00) Baku; (GMT+04:00) Yerevan; Samara; (GMT+04:30) Kabul; (GMT+05:00)

Default Name	Default Value	Default Domain
		Chelyabinsk; Prem; Yekaterinburg; Ufa; (GMT+05:00) Islamabad; Karachi; Tashkent; (GMT+05:30) Calcutta; Mumbai; New Delhi; Chennai; (GMT+05:45) Kathmandu; (GMT+06:00) Almaty; (GMT+06:00) Colombo; Dhaka; Astana; (GMT+06:00) Novosibirsk; Omsk; (GMT+06:30) Cocos; Rangoon; (GMT+07:00) Bangkok; Hanoi; Jakarta; (GMT+07:00) Krasnoyarsk; Norilsk; Novokuznetsk; (GMT+08:00) Irkutsk; Ulaan Bataar; (GMT+08:00) Beijing; Shanghai; Hong Kong; Urumqi; (GMT+08:00) Perth; (GMT+08:00) Singapore; Manila; Taipei; Kuala Lumpur; (GMT+09:00) Chita; Yakutsk; (GMT+09:00) Osaka; Sapporo; Tokyo; (GMT+09:00) Palau; Pyongyang; Seoul; (GMT+09:30) Adelaide; Broken Hill; (GMT+09:30) Darwin; (GMT+10:00) Brisbane; Port Moresby; Guam; (GMT+10:00) Canberra; Melbourne; Sydney; (GMT+10:00) Hobart; (GMT+10:00) Khabarovsk; Vladivostok; (GMT+10:30) Lord Howe Island; (GMT+11:00) Honiara; Magadan; Soloman Islands; (GMT+11:00) Noumea - New Caledonia; (GMT+11:30) Kingston - Norfolk Island; (GMT+12:00) Andyra; Kamchatka; (GMT+12:00) Auckland; Wellington; (GMT+12:00) Marshall Islands; Eniwetok; (GMT+12:00) Suva - Fiji; (GMT+12:45) Chatham Island; (GMT+13:00) Nuku'alofa - Tonga; (GMT+13:00) Rawaki; Phoenix Islands; (GMT+14:00) Line Islands; Kiritimati - Kiribati
NODE.general.UseDST	TRUE	TRUE; FALSE
NODE.general.mvAirFilterBasedFanEnable	FALSE	FALSE; TRUE
NODE.lmp.controlChannel.AdminState	OOS;DSBLD	IS; OOS;DSBLD

NODE.lmp.controlChannel.HelloDeadInterval	12000 (ms)	maximum_of(2000;MinHelloDeadInterval;
		product_of(HelloInterval;3));
		maximum_of(2000;
		MinHelloDeadInterval;product_of(HelloInterval;3)) + 1
		maximum_of(2000;MinHelloDeadInterval;
		product_of(HelloInterval;3)) +
		2 .. minimum_of (20000;MaxHelloDeadInterval)

Default Name	Default Value	Default Domain
NODE.lmp.controlChannel.HelloInterval	500 (ms)	maximum_of(300;MinHelloInterval); maximum_of(300; MinHelloInterval) + 1; maximum_of(300;MinHelloInterval) + 2 .. minimum_of(5000;MaxHelloInterval;quotient_of (HelloDeadInterval;3))
NODE.lmp.controlChannel. MaxHelloDeadInterval	20000 (ms)	maximum_of(2000;HelloDeadInterval; sum_of(MaxHelloInterval;1)); maximum_of(2000;HelloDeadInterval; sum_of(MaxHelloInterval;1)) + 1; maximum_of(2000;HelloDeadInterval; sum_of(MaxHelloInterval;1)) + 2 .. 20000
NODE.lmp.controlChannel. MinHelloDeadInterval	2000 (ms)	maximum_of(2000;sum_of(MinHelloInterval;1)); maximum_of(2000;sum_of(MinHelloInterval;1)) + 1; maximum_of(2000;sum_of(MinHelloInterval;1)) + 2 .. minimum_of(20000;HelloDeadInterval)
NODE.lmp.controlChannel.MaxHelloInterval	2000 (ms)	maximum_of(300;HelloInterval); maximum_of(300;HelloInterval) + 1; maximum_of(300;HelloInterval) + 2 .. minimum_of (5000;difference_of(MaxHelloDeadInterval;1))
NODE.lmp.controlChannel.MinHelloInterval	300 (ms)	300; 301; 302 .. minimum_of(5000;HelloInterval; difference_of(MinHelloDeadInterval;1))
NODE.lmp.dataLink.Type	Port	Port; Component
NODE.lmp.general.Allowed	TRUE	FALSE; TRUE
NODE.lmp.general.Enabled	FALSE	FALSE; TRUE when Allowed TRUE; FALSE when Allowed FALSE
NODE.lmp.general.LMP-WDM	TRUE	FALSE; TRUE
NODE.lmp.general.Role	OLS	PEER; OLS

Default Name	Default Value	Default Domain
NODE.lmp.teLink.AdminState	OOS;DSBLD	IS; OOS;DSBLD
NODE.lmp.teLink.DWDM	TRUE	FALSE; TRUE
NODE.lmp.teLink.MuxCapability	Lambda Switch	Packet Switch - Level 1; Packet Switch - Level 2; Packet Switch - Level 3; Packet Switch - Level 4; Layer 2 Switch; TDM Cross-connect; Lambda Switch; Fiber Switch
NODE.network.general. AlarmMissingBackplaneLAN	FALSE	TRUE; FALSE
NODE.network.general. CtcIpDisplaySuppression	FALSE	TRUE; FALSE
NODE.network.general.GatewaySettings	None	LeaveAsIs; None; ENE; GNE; ProxyOnlyNode
NODE.network.general.LcdSetting	Allow Configuration	Allow Configuration; Display Only; Suppress Display
NODE.osi.greTunnel.OspfCost	110	110 - 65535
NODE.osi.greTunnel.SubnetMask	24 (bits)	8; 9; 10 .. 32
NODE.osi.lapd.MTU	512	512; 513; 514 .. 1500
NODE.osi.lapd.Mode	AITS	AITS; UITS
NODE.osi.lapd.Role	Network	Network; User
NODE.osi.lapd.T200	200 (ms)	200; 300; 400 .. 20000
NODE.osi.lapd.T203	10000 (ms)	4000; 4100; 4200 .. 120000
NODE.osi.mainSetup.L1L2LSPBufferSize	512 (bytes)	512 - 1500
NODE.osi.mainSetup.L1LSPBufferSize	512 (bytes)	512 - 1500
NODE.osi.mainSetup.NodeRoutingMode	Intermediate System Level 1	End System; Intermediate System Level 1; Intermediate System Level 1/Level 2
NODE.osi.subnet.DISPriority	63	1; 2; 3 .. 127
NODE.osi.subnet.ESH	10 (sec)	10; 20; 30 .. 1000
NODE.osi.subnet.GCCISISCost	60	1; 2; 3 .. 63
NODE.osi.subnet.IIH	3 (sec)	1; 2; 3 .. 600
NODE.osi.subnet.ISH	10 (sec)	10; 20; 30 .. 1000
NODE.osi.subnet.LANISISCost	20	1; 2; 3 .. 63
NODE.osi.subnet.LDCCISISCost	40	1; 2; 3 .. 63

Default Name	Default Value	Default Domain
NODE.osi.subnet.OSCISISCost	60	1; 2; 3 .. 63
NODE.osi.subnet.SDCCISISCost	60	1; 2; 3 .. 63
NODE.osi.tarp.L1DataCache	TRUE	FALSE; TRUE
NODE.osi.tarp.L2DataCache	FALSE	FALSE; TRUE
NODE.osi.tarp.LANStormSuppression	TRUE	FALSE; TRUE
NODE.osi.tarp.LDB	TRUE	FALSE; TRUE
NODE.osi.tarp.LDBEntry	5 (min)	1 - 10
NODE.osi.tarp.LDBFlush	5 (min)	0 - 1440
NODE.osi.tarp.PDUsL1Propagation	TRUE	FALSE; TRUE
NODE.osi.tarp.PDUsL2Propagation	TRUE	FALSE; TRUE
NODE.osi.tarp.PDUsOrigination	TRUE	FALSE; TRUE
NODE.osi.tarp.T1Timer	15 (sec)	0 - 3600
NODE.osi.tarp.T2Timer	25 (sec)	0 - 3600
NODE.osi.tarp.T3Timer	40 (sec)	0 - 3600
NODE.osi.tarp.T4Timer	20 (sec)	0 - 3600
NODE.osi.tarp.Type4PDUDelay	0 (sec)	0 - 255
NODE.powerMonitor.EHIBATVG	-56.5 (Vdc)	-54.0; -54.5; -55.0; -55.5; -56.0; -56.5
NODE.powerMonitor.ELWBATVG	-40.5 (Vdc)	-40.5; -41.0; -41.5; -42.0; -42.5; -43.0; -43.5; -44.0
NODE.powerMonitor.HIBATVG	-54.0 (Vdc)	-44.0; -44.5; -45.0 .. -56.5
NODE.powerMonitor.LWBATVG	-44.0 (Vdc)	-40.5; -41.0; -41.5 .. -54.0
NODE.security.dataComm. CtcBackplaneIpDisplaySuppression	TRUE	FALSE; TRUE when isSecureModeSupportedOnControlCard TRUE; (NOT SUPPORTED) when isSecureModeSupportedOnControlCard FALSE
NODE.security.dataComm. DefaultTCCEthernetIP	10.10.0.1	IP Address
NODE.security.dataComm. DefaultTCCEthernetIPNetmask	24 (bits)	8; 9; 10 .. 32

Default Name	Default Value	Default Domain
NODE.security.dataComm. LcdBackplaneIpSetting	Display Only	Allow Configuration; Display Only; Suppress Display when isSecureModeSupportedOnControlCard TRUE; (NOT SUPPORTED) when isSecureModeSupportedOnControlCard FALSE
NODE.security.dataComm.SecureModeLocked	FALSE	FALSE; TRUE when isSecureModeSupportedOnControlCard TRUE; (NOT SUPPORTED) when isSecureModeSupportedOnControlCard FALSE
NODE.security.dataComm.SecureModeOn (May reboot node)	FALSE	FALSE; TRUE when isSecureModeSupportedOnControlCard TRUE; (NOT SUPPORTED) when isSecureModeSupportedOnControlCard FALSE
NODE.security.dataComm. isSecureModeSupportedOnControlCard	TRUE	FALSE; TRUE
NODE.security.emsAccess.AccessState	NonSecure	NonSecure; Secure
NODE.security.emsAccess.IIOPListenerPort (May reboot node)	57790 (port #)	0 - 65535
NODE.security.grantPermission. ActivateRevertSoftware	Superuser	Provisioning; Superuser
NODE.security.grantPermission. PMClearingPrivilege	Provisioning	Provisioning; Superuser
NODE.security.grantPermission.RestoreDB	Superuser	Provisioning; Superuser
NODE.security.grantPermission. RetrieveAuditLog	Superuser	Provisioning; Superuser
NODE.security.idleUserTimeout.Maintenance	01:00 (hours:mins)	00:00; 00:01; 00:02 .. 16:39
NODE.security.idleUserTimeout.Provisioning	00:30 (hours:mins)	00:00; 00:01; 00:02 .. 16:39
NODE.security.idleUserTimeout.Retrieve	00:00 (hours:mins)	00:00; 00:01; 00:02 .. 16:39
NODE.security.idleUserTimeout.Superuser	00:15 (hours:mins)	00:00; 00:01; 00:02 .. 16:39
NODE.security.lanAccess.LANAccess (May disconnect CTC from node)	Front & EMS	No LAN Access; Front Only; EMS Only; Front & EMS
NODE.security.lanAccess.RestoreTimeout	5 (minutes)	0 - 60

Default Name	Default Value	Default Domain
NODE.security.legalDisclaimer. LoginWarningMessage	This system is restricted to authorized users for business purposes. Unauthorized access is a violation of the law. This service may be monitored for administrative and security reasons. By proceeding, you consent to this monitoring.	Free form field
NODE.security.other.DisableInactiveUser	FALSE	FALSE; TRUE
NODE.security.other.InactiveDuration	45 (days)	1; 2; 3 .. 99 when nothing TRUE; 45 when nothing FALSE
NODE.security.other. PreventInactiveSuperuserDisable	FALSE	TRUE; FALSE
NODE.security.other. SingleSessionPerUser	FALSE	TRUE; FALSE
NODE.security.passwordAging. EnforcePasswordAging	FALSE	TRUE; FALSE
NODE.security.passwordAging. maintenance.AgingPeriod	45 (days)	20 - 90
NODE.security.passwordAging. maintenance.WarningPeriod	5 (days)	2 - 20

Default Name	Default Value	Default Domain
NODE.security.passwordAging.provisioning.AgingPeriod	45 (days)	20 - 90
NODE.security.passwordAging.provisioning.WarningPeriod	5 (days)	2 - 20
NODE.security.passwordAging.retrieve.AgingPeriod	45 (days)	20 - 90
NODE.security.passwordAging.retrieve.WarningPeriod	5 (days)	2 - 20
NODE.security.passwordAging.superuser.AgingPeriod	45 (days)	20 - 90
NODE.security.passwordAging.superuser.WarningPeriod	5 (days)	2 - 20
NODE.security.passwordChange.CannotChangeNewPassword	FALSE	TRUE; FALSE
NODE.security.passwordChange.CannotChangeNewPasswordForNDays	20 (days)	20 - 95
NODE.security.passwordChange.NewPasswordMustDifferFrom OldByNCharacters	1 (characters)	1 - 5
NODE.security.passwordChange.PreventReusingLastNPasswords	1 (times)	1 - 10
NODE.security.passwordChange.RequirePasswordChange OnFirstLoginToNewAccount	FALSE	TRUE; FALSE
NODE.security.passwordComplexity.IdenticalConsecutiveCharactersAllowed	3 or more	0-2; 3 or more
NODE.security.passwordComplexity.MaximumLength	20	20; 80

Default Name	Default Value	Default Domain
NODE.security.passwordComplexity. MinimumLength	6	6; 8; 10; 12
NODE.security.passwordComplexity. MinimumRequiredCharacters	1 num; 1 letter & 1 TL1 special	1 num; 1 letter & 1 TL1 special; 1 num; 1 letter & 1 special; 2 each of any 2 of num; upper; lower & TL1 special; 2 each of any 2 of num; upper; lower & special
NODE.security.passwordComplexity. ReverseUserIdAllowed	TRUE	TRUE; FALSE
NODE.security.pseudoIOSAccess.AccessState	NonSecure	Disabled; NonSecure; Secure
NODE.security.pseudoIOSAccess.Port	65000	1024 - 65535
NODE.security.pseudoIOSAccess.SecurePort	64000	1024 - 65535
NODE.security.radiusServer.AccountingPort	1813 (port)	0 - 32767
NODE.security.radiusServer.AuthenticationPort	1812 (port)	0 - 32767
NODE.security.radiusServer. EnableNodeAsFinalAuthenticator	TRUE	FALSE; TRUE
NODE.security.serialCraftAccess.EnableCraftPort	TRUE	TRUE; FALSE
NODE.security.shellAccess.AccessState	NonSecure	Disabled; NonSecure; Secure
NODE.security.shellAccess. EnableShellPassword	FALSE	TRUE; FALSE
NODE.security.shellAccess.TelnetPort	23	23 - 9999
NODE.security.snmpAccess.AccessState	NonSecure	Disabled; NonSecure
NODE.security.tl1Access.AccessState	NonSecure	Disabled; NonSecure; Secure
NODE.security.userLockout. FailedLoginsAllowedBeforeLockout	5 (times)	0 - 10
NODE.security.userLockout.LockoutDuration	00:30 (mins:secs)	00:00; 00:05; 00:10 .. 10:00
NODE.security.userLockout. ManualUnlockBySuperuser	FALSE	TRUE; FALSE
NODE.software.AllowDelayedUpgrades	FALSE	FALSE; TRUE
NODE.software.DefaultDelayedUpgrades	FALSE	FALSE; TRUE when AllowDelayedUpgrades TRUE; FALSE when AllowDelayedUpgrades FALSE

Default Name	Default Value	Default Domain
NODE.timing.general.Mode	External	External; Line; Mixed
NODE.timing.general.QualityOfRES	RES=DUS	PRS<RES; STU<RES<PRS; ST2<RES<STU; ST3<RES<ST2; SMC<RES<ST3; ST4<RES<SMC; RES<ST4; RES=DUS when SSMMessageSet Generation 1; PRS<RES; STU<RES<PRS; ST2<RES<STU; TNC<RES<ST2; ST3E<RES<TNC; ST3<RES<ST3E; SMC<RES<ST3; ST4<RES<SMC; RES<ST4; RES=DUS when SSMMessageSet Generation 2; N/A when SSMMessageSet N/A
NODE.timing.general.ReversionTime	5.0 (minutes)	0.5; 1.0; 1.5 .. 12.0
NODE.timing.general.Revertive	FALSE	TRUE; FALSE
NODE.timing.general.SSMMessageSet	Generation 1	Generation 1; Generation 2 when TimingStandard SONET; N/A when TimingStandard SDH
NODE.timing.general.TimingStandard	SONET	SONET; SDH
PTF-4.config.client.AINSSoakTime	08:00 (hours:mins)	00:00; 00:15; 00:30 .. 48:00
PTF-4.config.client.AdminState	OOS;DSBLD	IS; OOS;DSBLD
PTF-4.config.ppmPortAssignment	TEN-GE	UNASSIGNED; TEN-GE
PTF-4.config.ppmSlotAssignment	PPM (1 Port)	UNASSIGNED; PPM (1 Port)
PTF-4.config.trunk.AINSSoakTime	08:00 (hours:mins)	00:00; 00:15; 00:30 .. 48:00
PTF-4.config.trunk.AdminState	OOS;DSBLD	IS; OOS;DSBLD
PTF-4.opticalthresholds.client.10gethernet.10ger.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10ger.15min.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10ger.15min.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10ger.15min.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.client.10gethernet.10ger.15min.LowTxPower	-14.2 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.client.10gethernet.10ger.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10ger.1day.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10ger.1day.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10ger.1day.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10ger.1day.LowTxPower	-14.2 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.client.10gethernet.10ger.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10ger.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10ger.alarm.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10ger.alarm.LowRxPower	-16.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10ger.alarm.LowTxPower	-10.7 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.client.10gethernet.10glr.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10glr.15min.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10glr.15min.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.client.10gethernet.10glr.15min.LowRxPower	-15.8 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10glr.15min.LowTxPower	-10.7 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.client.10gethernet.10glr.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10glr.1day.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10glr.1day.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10glr.1day.LowRxPower	-15.8 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10glr.1day.LowTxPower	-10.7 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.client.10gethernet.10glr.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10glr.alarm.HighRxPower	1.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10glr.alarm.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10glr.alarm.LowRxPower	-18.3 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10glr.alarm.LowTxPower	-7.2 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.client.10gethernet.10gsr.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.15min.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.client.10gethernet.10gsr.15min.HighTxPower	4.7 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.15min.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10gsr.15min.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.client.10gethernet.10gsr.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.1day.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.1day.HighTxPower	4.7 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.1day.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10gsr.1day.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.client.10gethernet.10gsr.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.alarm.HighRxPower	1.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.alarm.HighTxPower	1.2 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.alarm.LowRxPower	-12.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10gsr.alarm.LowTxPower	-9.8 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.15min.HighTxPower	13.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.15min.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.15min.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.1day.HighTxPower	13.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.1day.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.1day.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.alarm.HighTxPower	9.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.alarm.LowRxPower	-16.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.alarm.LowTxPower	0.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.15min.HighTxPower	13.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.15min.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.15min.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.1day.HighTxPower	13.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.1day.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.1day.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.alarm.HighTxPower	9.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.alarm.LowRxPower	-16.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.alarm.LowTxPower	0.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.15min.HighTxPower	13.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.15min.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.15min.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.1day.HighTxPower	13.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.1day.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.1day.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.alarm.HighTxPower	9.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.alarm.LowRxPower	-16.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.alarm.LowTxPower	0.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.15min.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.15min.LowRxPower	-24.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.1day.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.1day.LowRxPower	-24.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.alarm.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.alarm.LowRxPower	-26.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.alarm.LowTxPower	-2.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.15min.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.15min.LowRxPower	-26.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.1day.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.1day.LowRxPower	-26.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.alarm.HighTxPower	5.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.alarm.LowRxPower	-29.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.alarm.LowTxPower	-2.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.15min.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.15min.LowRxPower	-26.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.1day.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.1day.LowRxPower	-26.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.alarm.HighTxPower	5.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.alarm.LowRxPower	-29.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.alarm.LowTxPower	-2.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.15min.HighRxPower	2.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.15min.HighTxPower	8.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.15min.LowRxPower	-15.8 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.15min.LowTxPower	-7.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.1day.HighRxPower	2.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.1day.HighTxPower	8.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.1day.LowRxPower	-15.8 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.1day.LowTxPower	-7.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.alarm.HighRxPower	4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.alarm.HighTxPower	4.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.alarm.LowRxPower	-18.3 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.alarm.LowTxPower	-3.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.15min.HighLaserBias	95.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.15min.HighRxPower	1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.15min.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.15min.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.15min.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.1day.HighLaserBias	96.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.1day.HighRxPower	1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.1day.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.1day.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.1day.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.alarm.HighTxPower	1.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.alarm.LowRxPower	-16.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.alarm.LowTxPower	-8.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.15min.HighLaserBias	95.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.15min.HighRxPower	1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.15min.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.15min.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.15min.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.1day.HighLaserBias	96.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.1day.HighRxPower	1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.1day.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.1day.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.1day.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.alarm.HighTxPower	1.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.alarm.LowRxPower	-16.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.alarm.LowTxPower	-8.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.15min.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.15min.LowRxPower	-24.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.1day.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.1day.LowRxPower	-24.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.alarm.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.alarm.LowRxPower	-26.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.alarm.LowTxPower	-2.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.15min.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.15min.LowRxPower	-27.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.15min.LowTxPower	-7.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.1day.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.1day.LowRxPower	-27.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.1day.LowTxPower	-7.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.alarm.HighTxPower	5.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.alarm.LowRxPower	-29.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.alarm.LowTxPower	-3.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.15min.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.15min.LowRxPower	-27.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.15min.LowTxPower	-7.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.1day.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.1day.LowRxPower	-27.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.1day.LowTxPower	-7.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.alarm.HighTxPower	5.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.alarm.LowRxPower	-29.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.alarm.LowTxPower	-3.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.15min.HighLaserBias	95.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.15min.HighRxPower	1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.15min.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.15min.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.15min.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.1day.HighLaserBias	96.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.1day.HighRxPower	1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.1day.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.1day.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.1day.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.alarm.HighTxPower	1.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.alarm.LowRxPower	-16.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.alarm.LowTxPower	-8.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.15min.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.15min.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.15min.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.15min.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.1day.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.1day.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.1day.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.1day.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.alarm.HighRxPower	1.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.alarm.HighTxPower	1.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.alarm.LowRxPower	-12.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.alarm.LowTxPower	-9.8 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.15min.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.15min.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.15min.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.15min.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.1day.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.1day.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.1day.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.1day.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.alarm.HighRxPower	1.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.alarm.HighTxPower	1.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.alarm.LowRxPower	-12.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.alarm.LowTxPower	-9.8 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.15min.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.15min.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.15min.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.15min.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.1day.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.1day.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.1day.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.1day.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.alarm.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.alarm.LowRxPower	-16.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.alarm.LowTxPower	-8.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.15min.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.15min.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.15min.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.15min.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.1day.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.1day.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.1day.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.1day.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.alarm.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.alarm.LowRxPower	-16.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.alarm.LowTxPower	-8.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.15min.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.15min.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.15min.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.15min.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.1day.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.1day.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.1day.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.1day.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.alarm.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.alarm.LowRxPower	-16.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.alarm.LowTxPower	-8.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.otn.g709thresholds.pm.farend.15min.BBE	85040 (count)	0 - 8850600
PTF-4.otn.g709thresholds.pm.farend.15min.ES	87 (seconds)	0 - 900
PTF-4.otn.g709thresholds.pm.farend.15min.FC	10 (count)	0 - 72
PTF-4.otn.g709thresholds.pm.farend.15min.SES	1 (seconds)	0 - 900
PTF-4.otn.g709thresholds.pm.farend.15min.UAS	3 (seconds)	0 - 900
PTF-4.otn.g709thresholds.pm.farend.1day.BBE	850400 (count)	0 - 849657600
PTF-4.otn.g709thresholds.pm.farend.1day.ES	864 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.pm.farend.1day.FC	40 (count)	0 - 6912
PTF-4.otn.g709thresholds.pm.farend.1day.SES	4 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.pm.farend.1day.UAS	10 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.pm.nearend.15min.BBE	85040 (count)	0 - 8850600

Default Name	Default Value	Default Domain
PTF-4.otn.g709thresholds.pm.nearend.15min.ES	87 (seconds)	0 - 900
PTF-4.otn.g709thresholds.pm.nearend.15min.FC	10 (count)	0 - 72
PTF-4.otn.g709thresholds.pm.nearend.15min.SES	1 (seconds)	0 - 900
PTF-4.otn.g709thresholds.pm.nearend.15min.UAS	3 (seconds)	0 - 900
PTF-4.otn.g709thresholds.pm.nearend.1day.BBE	850400 (count)	0 - 849657600
PTF-4.otn.g709thresholds.pm.nearend.1day.ES	864 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.pm.nearend.1day.FC	40 (count)	0 - 6912
PTF-4.otn.g709thresholds.pm.nearend.1day.SES	4 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.pm.nearend.1day.UAS	10 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.sm.farend.15min.BBE	10000 (count)	0 - 8850600
PTF-4.otn.g709thresholds.sm.farend.15min.ES	500 (seconds)	0 - 900
PTF-4.otn.g709thresholds.sm.farend.15min.FC	10 (count)	0 - 72
PTF-4.otn.g709thresholds.sm.farend.15min.SES	500 (seconds)	0 - 900
PTF-4.otn.g709thresholds.sm.farend.15min.UAS	500 (seconds)	0 - 900

Default Name	Default Value	Default Domain
PTF-4.otn.g709thresholds.sm.farend.1day.BBE	100000 (count)	0 - 849657600
PTF-4.otn.g709thresholds.sm.farend.1day.ES	5000 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.sm.farend.1day.FC	40 (count)	0 - 6912
PTF-4.otn.g709thresholds.sm.farend.1day.SES	5000 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.sm.farend.1day.UAS	5000 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.sm.nearend.15min.BBE	10000 (count)	0 - 8850600
PTF-4.otn.g709thresholds.sm.nearend.15min.ES	500 (seconds)	0 - 900
PTF-4.otn.g709thresholds.sm.nearend.15min.FC	10 (count)	0 - 72
PTF-4.otn.g709thresholds.sm.nearend.15min.SES	500 (seconds)	0 - 900
PTF-4.otn.g709thresholds.sm.nearend.15min.UAS	500 (seconds)	0 - 900
PTF-4.otn.g709thresholds.sm.nearend.1day.BBE	100000 (count)	0 - 849657600
PTF-4.otn.g709thresholds.sm.nearend.1day.ES	5000 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.sm.nearend.1day.FC	40 (count)	0 - 6912
PTF-4.otn.g709thresholds.sm.nearend.1day.SES	5000 (seconds)	0 - 86400

Default Name	Default Value	Default Domain
PTF-4.otn.g709thresholds.sm. nearend.1day.UAS	5000 (seconds)	0 - 86400
PTF-4.otn.otnLines.FEC	Standard	Disable; Standard; Enhanced when G709OTN Enable; Disable when G709OTN Disable
PTF-4.otn.otnLines.G709OTN	Enable	Disable; Enable
PTF-4.otn.otnLines.SDBER	1.00E-07	1E-5; 1E-6; 1E-7; 1E-8; 1E-9
PTM-4.config.10GE.AINSSoakTime	08:00 (hours:mins)	00:00; 00:15; 00:30 .. 48:00
PTM-4.config.10GE.AdminState	OOS;DSBLD	IS; OOS;DSBLD
PTM-4.config.ppmPortAssignment	TEN-GE	UNASSIGNED; TEN-GE
PTM-4.config.ppmSlotAssignment	PPM (1 Port)	UNASSIGNED; PPM (1 Port)
PTM-4.opticalthresholds.client.10gethernet. 10ger.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet. 10ger.15min.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet. 10ger.15min.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet. 10ger.15min.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet. 10ger.15min.LowTxPower	-14.2 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTM-4.opticalthresholds.client.10gethernet. 10ger.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet. 10ger.1day.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet. 10ger.1day.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet. 10ger.1day.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower

Default Name	Default Value	Default Domain
PTM-4.opticalthresholds.client.10gethernet.10ger.1day.LowTxPower	-14.2 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTM-4.opticalthresholds.client.10gethernet.10ger.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet.10ger.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10ger.alarm.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10ger.alarm.LowRxPower	-16.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10ger.alarm.LowTxPower	-10.7 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTM-4.opticalthresholds.client.10gethernet.10glr.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet.10glr.15min.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10glr.15min.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10glr.15min.LowRxPower	-15.8 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10glr.15min.LowTxPower	-10.7 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTM-4.opticalthresholds.client.10gethernet.10glr.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet.10glr.1day.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10glr.1day.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTM-4.opticalthresholds.client.10gethernet.10glr.1day.LowRxPower	-15.8 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10glr.1day.LowTxPower	-10.7 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTM-4.opticalthresholds.client.10gethernet.10glr.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet.10glr.alarm.HighRxPower	1.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10glr.alarm.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10glr.alarm.LowRxPower	-18.3 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10glr.alarm.LowTxPower	-7.2 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTM-4.opticalthresholds.client.10gethernet.10gsr.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.15min.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.15min.HighTxPower	4.7 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.15min.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10gsr.15min.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTM-4.opticalthresholds.client.10gethernet.10gsr.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.1day.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTM-4.opticalthresholds.client.10gethernet.10gsr.1day.HighTxPower	4.7 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.1day.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10gsr.1day.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTM-4.opticalthresholds.client.10gethernet.10gsr.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.alarm.HighRxPower	1.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.alarm.HighTxPower	1.2 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.alarm.LowRxPower	-12.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10gsr.alarm.LowTxPower	-9.8 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.config.10GE.AINSSoakTime	08:00 (hours:mins)	00:00; 00:15; 00:30 .. 48:00
PTSA.config.10GE.AdminState	IS	IS; OOS;DSBLD
PTSA.config.1GE.AINSSoakTime	08:00 (hours:mins)	00:00; 00:15; 00:30 .. 48:00
PTSA.config.1GE.AdminState	OOS;DSBLD	IS; OOS;DSBLD
PTSA.config.FE.AINSSoakTime	08:00 (hours:mins)	00:00; 00:15; 00:30 .. 48:00
PTSA.config.FE.AdminState	OOS;DSBLD	IS; OOS;DSBLD
PTSA.config.ppmPortAssignment	UNASSIGNED	UNASSIGNED; ONE-GE; FE
PTSA.config.ppmSlotAssignment	UNASSIGNED	UNASSIGNED; PPM (1 Port)
PTSA.opticalthresholds.client.1gethernet.cwdm.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0

Default Name	Default Value	Default Domain
PTSA.opticalthresholds.client.1gethernet.cwdm.15min.HighRxPower	-9.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.cwdm.15min.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.cwdm.15min.LowRxPower	-29.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.cwdm.15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.cwdm.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.cwdm.1day.HighRxPower	-9.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.cwdm.1day.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.cwdm.1day.LowRxPower	-29.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.cwdm.1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.cwdm.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.cwdm.alarm.HighRxPower	-6.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.cwdm.alarm.HighTxPower	8.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.cwdm.alarm.LowRxPower	-32.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.cwdm.alarm.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower

Default Name	Default Value	Default Domain
PTSA.opticalthresholds.client.1gethernet.lx.15min.HighLaserBias	81.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.lx.15min.HighRxPower	-3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.lx.15min.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.lx.15min.LowRxPower	-20.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.lx.15min.LowTxPower	-16.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.lx.1day.HighLaserBias	85.5 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.lx.1day.HighRxPower	-3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.lx.1day.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.lx.1day.LowRxPower	-20.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.lx.1day.LowTxPower	-16.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.lx.alarm.HighLaserBias	90.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.lx.alarm.HighRxPower	0.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.lx.alarm.HighTxPower	-1.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.lx.alarm.LowRxPower	-23.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower

Default Name	Default Value	Default Domain
PTSA.opticalthresholds.client.1gethernet.lx.alarm.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.sx.15min.HighLaserBias	81.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.sx.15min.HighRxPower	0.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.sx.15min.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.sx.15min.LowRxPower	-17.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.sx.15min.LowTxPower	-16.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.sx.1day.HighLaserBias	85.5 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.sx.1day.HighRxPower	0.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.sx.1day.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.sx.1day.LowRxPower	-17.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.sx.1day.LowTxPower	-16.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.sxalarm.HighLaserBias	90.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.sx.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.sx.alarm.HighTxPower	-2.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTSA.opticalthresholds.client.1gethernet.sx.alarm.LowRxPower	-20.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.sx.alarm.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.t.15min.HighLaserBias	100.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.t.15min.HighRxPower	30.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.t.15min.HighTxPower	30.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.t.15min.LowRxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.t.15min.LowTxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.t.1day.HighLaserBias	100.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.t.1day.HighRxPower	30.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.t.1day.HighTxPower	30.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.t.1day.LowRxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.t.1day.LowTxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.t.alarm.HighLaserBias	100.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.t.alarm.HighRxPower	30.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTSA.opticalthresholds.client.1gethernet.t.alarm.HighTxPower	30.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.t.alarm.LowRxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.t.alarm.LowTxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.zx.15min.HighLaserBias	100.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.zx.15min.HighRxPower	30.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.zx.15min.HighTxPower	30.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.zx.15min.LowRxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.zx.15min.LowTxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.zx.1day.HighLaserBias	100.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.zx.1day.HighRxPower	30.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.zx.1day.HighTxPower	30.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.zx.1day.LowRxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.zx.1day.LowTxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.zx.alarm.HighLaserBias	100.0 (%)	0.0; 0.1; 0.2 .. 100.0

Default Name	Default Value	Default Domain
PTSA.opticalthresholds.client.1gethernet.zx.alarm.HighRxPower	30.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.zx.alarm.HighTxPower	30.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.zx.alarm.LowRxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.zx.alarm.LowTxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.fastethernet.lx.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.fastethernet.lx.15min.HighRxPower	-8.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.lx.15min.HighTxPower	-2.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.lx.15min.LowRxPower	-28.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.fastethernet.lx.15min.LowTxPower	-21.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.fastethernet.lx.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.fastethernet.lx.1day.HighRxPower	-8.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.lx.1day.HighTxPower	-2.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.lx.1day.LowRxPower	-28.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.fastethernet.lx.1day.LowTxPower	-21.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower

Default Name	Default Value	Default Domain
PTSA.opticalthresholds.client.fastethernet.lx.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.fastethernet.lx.alarm.HighRxPower	-5.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.lx.alarm.HighTxPower	-5.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.lx.alarm.LowRxPower	-30.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.fastethernet.lx.alarm.LowTxPower	-17.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.fastethernet.sx.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.fastethernet.sx.15min.HighRxPower	-14.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.sx.15min.HighTxPower	-8.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.sx.15min.LowRxPower	-31.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.fastethernet.sx.15min.LowTxPower	-25.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.fastethernet.sx.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.fastethernet.sx.1day.HighRxPower	-14.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.sx.1day.HighTxPower	-8.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.sx.1day.LowRxPower	-31.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower

Default Name	Default Value	Default Domain
PTSA.opticalthresholds.client.fastethernet.sx.1day.LowTxPower	-25.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.fastethernet.sx.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.fastethernet.sx.alarm.HighRxPower	-11.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.sx.alarm.HighTxPower	-11.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.sx.alarm.LowRxPower	-33.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.fastethernet.sx.alarm.LowTxPower	-21.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.config.fe.AlsMode	Auto Restart	Disabled; Auto Restart
TNC.config.ge.AlsMode	Auto Restart	Disabled; Auto Restart
TNC.config.oc3.AlsMode	Auto Restart	Disabled; Auto Restart
TNC.opticalthresholds.1gethernet.cwdm.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.1gethernet.cwdm.15min.HighRxPower	-9.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.1gethernet.cwdm.15min.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.1gethernet.cwdm.15min.LowRxPower	-29.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.1gethernet.cwdm.15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.1gethernet.cwdm.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0

Default Name	Default Value	Default Domain
TNC.opticalthresholds.1gethernet.cwdm.1day.HighRxPower	-9.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.1gethernet.cwdm.1day.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.1gethernet.cwdm.1day.LowRxPower	-29.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.1gethernet.cwdm.1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.1gethernet.cwdm.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.1gethernet.cwdm.alarm.HighRxPower	-6.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.1gethernet.cwdm.alarm.HighTxPower	8.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.1gethernet.cwdm.alarm.LowRxPower	-32.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.1gethernet.cwdm.alarm.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.fastethernet.lx.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.fastethernet.lx.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.lx.15min.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.lx.15min.LowRxPower	-34.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.fastethernet.lx.15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower

Default Name	Default Value	Default Domain
TNC.opticalthresholds.fastethernet.lx.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.fastethernet.lx.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.lx.1day.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.lx.1day.LowRxPower	-34.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.fastethernet.lx.1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.fastethernet.lx.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.fastethernet.lx.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.lx.alarm.HighTxPower	7.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.lx.alarm.LowRxPower	-36.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.fastethernet.lx.alarm.LowTxPower	-2.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.fastethernet.ulh.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.fastethernet.ulh.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.ulh.15min.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.ulh.15min.LowRxPower	-43.0 (dBm)	-50.0; -49.9; -49.8 .. HighRxPower

Default Name	Default Value	Default Domain
TNC.opticalthresholds.fastethernet.ulh.15min.LowTxPower	-5.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.fastethernet.ulh.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.fastethernet.ulh.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.ulh.1day.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.ulh.1day.LowRxPower	-43.0 (dBm)	-50.0; -49.9; -49.8 .. HighRxPower
TNC.opticalthresholds.fastethernet.ulh.1day.LowTxPower	-5.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.fastethernet.ulh.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.fastethernet.ulh.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.ulh.alarm.HighTxPower	7.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.ulh.alarm.LowRxPower	-45.5 (dBm)	-50.0; -49.9; -49.8 .. HighRxPower
TNC.opticalthresholds.fastethernet.ulh.alarm.LowTxPower	-1.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.oc3.lr2.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.oc3.lr2.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.lr2.15min.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
TNC.opticalthresholds.oc3.lr2. 15min.LowRxPower	-34.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.oc3.lr2. 15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.oc3.lr2. 1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.oc3.lr2. 1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.lr2. 1day.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.lr2. 1day.LowRxPower	-34.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.oc3.lr2. 1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.oc3.lr2. alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.oc3.lr2. alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.lr2. alarm.HighTxPower	7.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.lr2. alarm.LowRxPower	-36.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.oc3.lr2. alarm.LowTxPower	-2.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.oc3.ulh. 15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.oc3.ulh. 15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
TNC.opticalthresholds.oc3.ulh.15min.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.ulh.15min.LowRxPower	-43.0 (dBm)	-50.0; -49.9; -49.8 .. HighRxPower
TNC.opticalthresholds.oc3.ulh.15min.LowTxPower	-5.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.oc3.ulh.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.oc3.ulh.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.ulh.1day.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.ulh.1day.LowRxPower	-43.0 (dBm)	-50.0; -49.9; -49.8 .. HighRxPower
TNC.opticalthresholds.oc3.ulh.1day.LowTxPower	-5.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.oc3.ulh.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.oc3.ulh.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.ulh.alarm.HighTxPower	7.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.ulh.alarm.LowRxPower	-45.5 (dBm)	-50.0; -49.9; -49.8 .. HighRxPower
TNC.opticalthresholds.oc3.ulh.alarm.LowTxPower	-1.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.pmthresholds.line.farend.15min.CV	1312 (B2 count)	0 - 137700

Default Name	Default Value	Default Domain
TNC.pmthresholds.line.farend.15min.ES	87 (seconds)	0 - 900
TNC.pmthresholds.line.farend.15min.FC	10 (count)	0 - 72
TNC.pmthresholds.line.farend.15min.SES	1 (seconds)	0 - 900
TNC.pmthresholds.line.farend.15min.UAS	3 (seconds)	0 - 900
TNC.pmthresholds.line.farend.1day.CV	13120 (B2 count)	0 - 13219200
TNC.pmthresholds.line.farend.1day.ES	864 (seconds)	0 - 86400
TNC.pmthresholds.line.farend.1day.FC	40 (count)	0 - 6912
TNC.pmthresholds.line.farend.1day.SES	4 (seconds)	0 - 86400
TNC.pmthresholds.line.farend.1day.UAS	10 (seconds)	0 - 86400
TNC.pmthresholds.line.nearend.15min.CV	1312 (B2 count)	0 - 137700
TNC.pmthresholds.line.nearend.15min.ES	87 (seconds)	0 - 900
TNC.pmthresholds.line.nearend.15min.FC	10 (count)	0 - 72
TNC.pmthresholds.line.nearend.15min.SES	1 (seconds)	0 - 900
TNC.pmthresholds.line.nearend.15min.UAS	3 (seconds)	0 - 900

Default Name	Default Value	Default Domain
TNC.pmthresholds.line.nearend.1day.CV	13120 (B2 count)	0 - 13219200
TNC.pmthresholds.line.nearend.1day.ES	864 (seconds)	0 - 86400
TNC.pmthresholds.line.nearend.1day.FC	40 (count)	0 - 6912
TNC.pmthresholds.line.nearend.1day.SES	4 (seconds)	0 - 86400
TNC.pmthresholds.line.nearend.1day.UAS	10 (seconds)	0 - 86400
TNC.pmthresholds.section.nearend.15min.CV	10000 (B1 count)	0 - 138600
TNC.pmthresholds.section.nearend.15min.ES	500 (seconds)	0 - 900
TNC.pmthresholds.section.nearend.15min.SEFS	500 (seconds)	0 - 900
TNC.pmthresholds.section.nearend.15min.SES	500 (seconds)	0 - 900
TNC.pmthresholds.section.nearend.1day.CV	100000 (B1 count)	0 - 13305600
TNC.pmthresholds.section.nearend.1day.ES	5000 (seconds)	0 - 86400
TNC.pmthresholds.section.nearend.1day.SEFS	5000 (seconds)	0 - 86400
TNC.pmthresholds.section.nearend.1day.SES	5000 (seconds)	0 - 86400

CPT 600 Network Element Default Settings

The following table lists the network element default settings for CPT 600.

Table 70: CPT 600 Network Element Default Settings

Default Name	Default Value	Default Domain
CTC.circuits.CreateLikeTL1	FALSE	TRUE; FALSE
CTC.circuits.RouteAutomatically	TRUE	TRUE; FALSE
CTC.circuits. RouteAutomaticallyDefaultOverridable	TRUE	TRUE; FALSE
CTC.network.Map	United States	-none-; Germany; Japan; Netherlands; South Korea; United Kingdom; United States
NODE.circuits.SendPDIP	FALSE	TRUE; FALSE
NODE.circuits.State	IS;AINS	IS; OOS;DSBLD; OOS;MT; IS;AINS
NODE.general. AllowServiceAffectingPortChangeToDisabled	TRUE	FALSE; TRUE
NODE.general.AutoPM	FALSE	FALSE; TRUE
NODE.general.DefaultsDescription	Factory Defaults	Free form field
NODE.general.InsertAISVOnSDP	FALSE	TRUE; FALSE
NODE.general.NtpSntpServer	0.0.0.0	IP Address
NODE.general.RaiseConditionOnEmptySlot	FALSE	TRUE; FALSE
NODE.general. ReportLoopbackConditionsOnOOS-MTPorts	FALSE	FALSE; TRUE
NODE.general.SDPBER	1.00E-06	1E-5; 1E-6; 1E-7; 1E-8; 1E-9

Default Name	Default Value	Default Domain
NODE.general.TimeZone	(GMT-08:00) Pacific Time (US & Canada); Tijuana	

Default Name	Default Value	Default Domain
		(GMT-11:00) Midway Islands; Samoa; (GMT-10:00) Hawaiian Islands; Tahiti; (GMT-09:00) Anchorage - Alaska; (GMT-08:00) Pacific Time (US & Canada); Tijuana; (GMT-07:00) Mountain Time (US & Canada); (GMT-07:00) Phoenix - Arizona; (GMT-06:00) Central Time (US & Canada); (GMT-06:00) Mexico City; (GMT-06:00) Costa Rica; Managua; San Salvador; (GMT-06:00) Saskatchewan; (GMT-05:00) Bogota; Lima; Quito; (GMT-05:00) Eastern Time (US & Canada); (GMT-05:00) Havana; (GMT-05:00) Indiana (US); (GMT-04:00) Asuncion; (GMT-04:00) Caracas; La Paz; San Juan; (GMT-04:00) Atlantic Time (Canada); Halifax; Saint John; Charlottetown; (GMT-04:00) Santiago; (GMT-04:00) Thule (Qaanaaq); (GMT-03:30) St. John's - Newfoundland; (GMT-03:00) Brasilia; Rio de Janeiro; Sao Paulo; (GMT-03:00) Buenos Aires; Georgetown; (GMT-03:00) Godthab (Nuuk) - Greenland; (GMT-02:00) Mid-Atlantic; (GMT-01:00) Azores; Scoresbysund; (GMT-01:00) Praia - Cape Verde; (GMT 00:00) Casablanca; Reykjavik; Monrovia; (GMT) Greenwich Mean Time; (GMT 00:00) Dublin; Edinburgh; London; Lisbon; (GMT+01:00) Amsterdam; Berlin; Rome; Stockholm; Paris; (GMT+01:00) Belgrade; Bratislava; Budapest; Ljubljana; Prague; (GMT+01:00) Brussels; Copenhagen; Madrid; Vienna; (GMT+01:00) Sarajevo; Skopje; Sofija; Vilnius; Warsaw; Zagreb; (GMT+01:00) West Central Africa; Algiers; Lagos; Luanda; (GMT+01:00) Windhoek (Namibia); (GMT+02:00) Al Jizah; Alexandria; Cairo; (GMT+02:00) Amman; (GMT+02:00) Athens; Bucharest; Istanbul; (GMT+02:00) Beirut; (GMT+02:00) Cape Town; Harare; Johannesburg; Pretoria; (GMT+02:00) Jerusalem; (GMT+02:00) Kaliningrad; Minsk; (GMT+03:00) Aden; Antananarivo; Khartoum; Nairobi; (GMT+03:00) Baghdad; (GMT+03:00) Kuwait; Riyadh; (GMT+03:00) Moscow; St. Petersburg; Novgorod; (GMT+03:30) Tehran; (GMT+04:00) Abu Dhabi; Mauritius; Muscat; (GMT+04:00) Aqtau; T'bilisi; (GMT+04:00) Baku; (GMT+04:00) Yerevan; Samara; (GMT+04:30) Kabul; (GMT+05:00) Chelyabinsk; Prem; Yekaterinburg; Ufa;

Default Name	Default Value	Default Domain
		(GMT+05:00) Islamabad; Karachi; Tashkent; (GMT+05:30) Calcutta; Mumbai; New Delhi; Chennai; (GMT+05:45) Kathmandu; (GMT+06:00) Almaty; (GMT+06:00) Colombo; Dhaka; Astana; (GMT+06:00) Novosibirsk; Omsk; (GMT+06:30) Cocos; Rangoon; (GMT+07:00) Bangkok; Hanoi; Jakarta; (GMT+07:00) Krasnoyarsk; Norilsk; Novokuznetsk; (GMT+08:00) Irkutsk; Ulaan Bataar; (GMT+08:00) Beijing; Shanghai; Hong Kong; Urumqi; (GMT+08:00) Perth; (GMT+08:00) Singapore; Manila; Taipei; Kuala Lumpur; (GMT+09:00) Chita; Yakutsk; (GMT+09:00) Osaka; Sapporo; Tokyo; (GMT+09:00) Palau; Pyongyang; Seoul; (GMT+09:30) Adelaide; Broken Hill; (GMT+09:30) Darwin; (GMT+10:00) Brisbane; Port Moresby; Guam; (GMT+10:00) Canberra; Melbourne; Sydney; (GMT+10:00) Hobart; (GMT+10:00) Khabarovsk; Vladivostok; (GMT+10:30) Lord Howe Island; (GMT+11:00) Honiara; Magadan; Soloman Islands; (GMT+11:00) Noumea - New Caledonia; (GMT+11:30) Kingston - Norfolk Island; (GMT+12:00) Andyra; Kamchatka; (GMT+12:00) Auckland; Wellington; (GMT+12:00) Marshall Islands; Eniwetok; (GMT+12:00) Suva - Fiji; (GMT+12:45) Chatham Island; (GMT+13:00) Nuku'alofa - Tonga; (GMT+13:00) Rawaki; Phoenix Islands; (GMT+14:00) Line Islands; Kiritimati - Kiribati
NODE.general.UseDST	TRUE	TRUE; FALSE
NODE.general.mvAirFilterBasedFanEnable	FALSE	FALSE; TRUE
NODE.lmp.controlChannel.AdminState	OOS;DSBLD	IS; OOS;DSBLD

NODE.lmp.controlChannel.HelloDeadInterval	12000 (ms)	maximum_of(2000;MinHelloDeadInterval;
		product_of(HelloInterval;3));
		maximum_of(2000;
		MinHelloDeadInterval;product_of(HelloInterval;3)) + 1
		maximum_of(2000;MinHelloDeadInterval;
		product_of(HelloInterval;3)) +
		2 .. minimum_of (20000;MaxHelloDeadInterval)

Default Name	Default Value	Default Domain
NODE.lmp.controlChannel.HelloInterval	500 (ms)	maximum_of(300;MinHelloInterval); maximum_of(300; MinHelloInterval) + 1; maximum_of(300;MinHelloInterval) + 2 .. minimum_of(5000;MaxHelloInterval;quotient_of (HelloDeadInterval;3))
NODE.lmp.controlChannel. MaxHelloDeadInterval	20000 (ms)	maximum_of(2000;HelloDeadInterval; sum_of(MaxHelloInterval;1)); maximum_of(2000;HelloDeadInterval; sum_of(MaxHelloInterval;1)) + 1; maximum_of(2000;HelloDeadInterval; sum_of(MaxHelloInterval;1)) + 2 .. 20000
NODE.lmp.controlChannel. MinHelloDeadInterval	2000 (ms)	maximum_of(2000;sum_of(MinHelloInterval;1)); maximum_of(2000;sum_of(MinHelloInterval;1)) + 1; maximum_of(2000;sum_of(MinHelloInterval;1)) + 2 .. minimum_of(20000;HelloDeadInterval)
NODE.lmp.controlChannel.MaxHelloInterval	2000 (ms)	maximum_of(300;HelloInterval); maximum_of(300;HelloInterval) + 1; maximum_of(300;HelloInterval) + 2 .. minimum_of (5000;difference_of(MaxHelloDeadInterval;1))
NODE.lmp.controlChannel.MinHelloInterval	300 (ms)	300; 301; 302 .. minimum_of(5000;HelloInterval; difference_of(MinHelloDeadInterval;1))
NODE.lmp.dataLink.Type	Port	Port; Component
NODE.lmp.general.Allowed	TRUE	FALSE; TRUE
NODE.lmp.general.Enabled	FALSE	FALSE; TRUE when Allowed TRUE; FALSE when Allowed FALSE
NODE.lmp.general.LMP-WDM	TRUE	FALSE; TRUE
NODE.lmp.general.Role	OLS	PEER; OLS
NODE.lmp.teLink.AdminState	OOS;DSBLD	IS; OOS;DSBLD

Default Name	Default Value	Default Domain
NODE.lmp.teLink.DWDM	TRUE	FALSE; TRUE
NODE.lmp.teLink.MuxCapability	Lambda Switch	Packet Switch - Level 1; Packet Switch - Level 2; Packet Switch - Level 3; Packet Switch - Level 4; Layer 2 Switch; TDM Cross-connect; Lambda Switch; Fiber Switch
NODE.network.general. AlarmMissingBackplaneLAN	FALSE	TRUE; FALSE
NODE.network.general. CtcIpDisplaySuppression	FALSE	TRUE; FALSE
NODE.network.general.GatewaySettings	None	LeaveAsIs; None; ENE; GNE; ProxyOnlyNode
NODE.network.general.LcdSetting	Allow Configuration	Allow Configuration; Display Only; Suppress Display
NODE.osi.greTunnel.OspfCost	110	110 - 65535
NODE.osi.greTunnel.SubnetMask	24 (bits)	8; 9; 10 .. 32
NODE.osi.lapd.MTU	512	512; 513; 514 .. 1500
NODE.osi.lapd.Mode	AITS	AITS; UITS
NODE.osi.lapd.Role	Network	Network; User
NODE.osi.lapd.T200	200 (ms)	200; 300; 400 .. 20000
NODE.osi.lapd.T203	10000 (ms)	4000; 4100; 4200 .. 120000
NODE.osi.mainSetup.L1L2LSPBufferSize	512 (bytes)	512 - 1500
NODE.osi.mainSetup.L1LSPBufferSize	512 (bytes)	512 - 1500
NODE.osi.mainSetup.NodeRoutingMode	Intermediate System Level 1	End System; Intermediate System Level 1; Intermediate System Level 1/Level 2
NODE.osi.subnet.DISPriority	63	1; 2; 3 .. 127
NODE.osi.subnet.ESH	10 (sec)	10; 20; 30 .. 1000
NODE.osi.subnet.GCCISISCost	60	1; 2; 3 .. 63
NODE.osi.subnet.IIH	3 (sec)	1; 2; 3 .. 600
NODE.osi.subnet.ISH	10 (sec)	10; 20; 30 .. 1000
NODE.osi.subnet.LANISISCost	20	1; 2; 3 .. 63
NODE.osi.subnet.LDCCISISCost	40	1; 2; 3 .. 63
NODE.osi.subnet.OSCISISCost	60	1; 2; 3 .. 63
NODE.osi.subnet.SDCCISISCost	60	1; 2; 3 .. 63

Default Name	Default Value	Default Domain
NODE.osi.tarp.L1DataCache	TRUE	FALSE; TRUE
NODE.osi.tarp.L2DataCache	FALSE	FALSE; TRUE
NODE.osi.tarp.LANStormSuppression	TRUE	FALSE; TRUE
NODE.osi.tarp.LDB	TRUE	FALSE; TRUE
NODE.osi.tarp.LDBEntry	5 (min)	1 - 10
NODE.osi.tarp.LDBFlush	5 (min)	0 - 1440
NODE.osi.tarp.PDUsL1Propagation	TRUE	FALSE; TRUE
NODE.osi.tarp.PDUsL2Propagation	TRUE	FALSE; TRUE
NODE.osi.tarp.PDUsOrigination	TRUE	FALSE; TRUE
NODE.osi.tarp.T1Timer	15 (sec)	0 - 3600
NODE.osi.tarp.T2Timer	25 (sec)	0 - 3600
NODE.osi.tarp.T3Timer	40 (sec)	0 - 3600
NODE.osi.tarp.T4Timer	20 (sec)	0 - 3600
NODE.osi.tarp.Type4PDUDelay	0 (sec)	0 - 255
NODE.powerMonitor.EHIBATVG	-56.5 (Vdc)	-54.0; -54.5; -55.0; -55.5; -56.0; -56.5
NODE.powerMonitor.ELWBATVG	-40.5 (Vdc)	-40.5; -41.0; -41.5; -42.0; -42.5; -43.0; -43.5; -44.0
NODE.powerMonitor.HIBATVG	-54.0 (Vdc)	-44.0; -44.5; -45.0 .. -56.5
NODE.powerMonitor.LWBATVG	-44.0 (Vdc)	-40.5; -41.0; -41.5 .. -54.0
NODE.protection.1+1.BidirectionalSwitching	FALSE	TRUE; FALSE
NODE.protection.1+1.DetectionGuardTimer	1 (seconds)	0; 0.05; 0.1; 0.5; 1; 2; 3; 4; 5
NODE.protection.1+1.RecoveryGuardTimer	1 (seconds)	0; 0.05; 0.1 .. 10
NODE.protection.1+1.ReversionTime	5.0 (minutes)	0.5; 1.0; 1.5 .. 12.0
NODE.protection.1+1.Revertive	FALSE	TRUE; FALSE
NODE.protection.1+1.VerifyGuardTimer	0.5 (seconds)	0.5; 1
NODE.protection.blsr.RingReversionTime	5.0 (minutes)	0.5; 1.0; 1.5 .. 12.0
NODE.protection.blsr.RingRevertive	TRUE	TRUE; FALSE
NODE.protection.blsr.SpanReversionTime	5.0 (minutes)	0.5; 1.0; 1.5 .. 12.0
NODE.protection.blsr.SpanRevertive	TRUE	TRUE; FALSE
NODE.protection.splitter.ReversionTime	5.0 (minutes)	0.5; 1.0; 1.5 .. 12.0
NODE.protection.splitter.Revertive	FALSE	TRUE; FALSE

Default Name	Default Value	Default Domain
NODE.protection.ycable.ReversionTime	5.0 (minutes)	0.5; 1.0; 1.5 .. 12.0
NODE.protection.ycable.Revertive	FALSE	TRUE; FALSE
NODE.security.dataComm. CtcBackplaneIpDisplaySuppression	TRUE	FALSE; TRUE when isSecureModeSupportedOnControlCard TRUE; (NOT SUPPORTED) when isSecureModeSupportedOnControlCard FALSE
NODE.security.dataComm. DefaultTCCEthernetIP	10.10.0.1	IP Address
NODE.security.dataComm. DefaultTCCEthernetIPNetmask	24 (bits)	8; 9; 10 .. 32
NODE.security.dataComm. LcdBackplaneIpSetting	Display Only	Allow Configuration; Display Only; Suppress Display when isSecureModeSupportedOnControlCard TRUE; (NOT SUPPORTED) when isSecureModeSupportedOnControlCard FALSE
NODE.security.dataComm.SecureModeLocked	FALSE	FALSE; TRUE when isSecureModeSupportedOnControlCard TRUE; (NOT SUPPORTED) when isSecureModeSupportedOnControlCard FALSE
NODE.security.dataComm.SecureModeOn (May reboot node)	FALSE	FALSE; TRUE when isSecureModeSupportedOnControlCard TRUE; (NOT SUPPORTED) when isSecureModeSupportedOnControlCard FALSE
NODE.security.dataComm. isSecureModeSupportedOnControlCard	TRUE	FALSE; TRUE
NODE.security.emsAccess.AccessState	NonSecure	NonSecure; Secure
NODE.security.emsAccess.IIOPListenerPort (May reboot node)	57790 (port #)	0 - 65535
NODE.security.grantPermission. ActivateRevertSoftware	Superuser	Provisioning; Superuser
NODE.security.grantPermission. PMClearingPrivilege	Provisioning	Provisioning; Superuser
NODE.security.grantPermission.RestoreDB	Superuser	Provisioning; Superuser
NODE.security.grantPermission. RetrieveAuditLog	Superuser	Provisioning; Superuser

Default Name	Default Value	Default Domain
NODE.security.idleUserTimeout.Maintenance	01:00 (hours:mins)	00:00; 00:01; 00:02 .. 16:39
NODE.security.idleUserTimeout.Provisioning	00:30 (hours:mins)	00:00; 00:01; 00:02 .. 16:39
NODE.security.idleUserTimeout.Retrieve	00:00 (hours:mins)	00:00; 00:01; 00:02 .. 16:39
NODE.security.idleUserTimeout.Superuser	00:15 (hours:mins)	00:00; 00:01; 00:02 .. 16:39
NODE.security.lanAccess.LANAccess (May disconnect CTC from node)	Front Craft & EMS	No LAN Access; Front & Craft; EMS Only; Front Craft & EMS
NODE.security.lanAccess.RestoreTimeout	5 (minutes)	0 - 60
NODE.security.legalDisclaimer. LoginWarningMessage	This system is restricted to authorized users for business purposes. Unauthorized access is a violation of the law. This service may be monitored for administrative and security reasons. By proceeding, you consent to this monitoring.	Free form field
NODE.security.other.DisableInactiveUser	FALSE	FALSE; TRUE
NODE.security.other.InactiveDuration	45 (days)	1; 2; 3 .. 99 when nothing TRUE; 45 when nothing FALSE
NODE.security.other. PreventInactiveSuperuserDisable	FALSE	TRUE; FALSE
NODE.security.other. SingleSessionPerUser	FALSE	TRUE; FALSE
NODE.security.passwordAging. EnforcePasswordAging	FALSE	TRUE; FALSE

Default Name	Default Value	Default Domain
NODE.security.passwordAging.maintenance.AgingPeriod	45 (days)	20 - 90
NODE.security.passwordAging.maintenance.WarningPeriod	5 (days)	2 - 20
NODE.security.passwordAging.provisioning.AgingPeriod	45 (days)	20 - 90
NODE.security.passwordAging.provisioning.WarningPeriod	5 (days)	2 - 20
NODE.security.passwordAging.retrieve.AgingPeriod	45 (days)	20 - 90
NODE.security.passwordAging.retrieve.WarningPeriod	5 (days)	2 - 20
NODE.security.passwordAging.superuser.AgingPeriod	45 (days)	20 - 90
NODE.security.passwordAging.superuser.WarningPeriod	5 (days)	2 - 20
NODE.security.passwordChange.CannotChangeNewPassword	FALSE	TRUE; FALSE
NODE.security.passwordChange.CannotChangeNewPasswordForNDays	20 (days)	20 - 95
NODE.security.passwordChange.NewPasswordMustDifferFromOldByNCharacters	1 (characters)	1 - 5
NODE.security.passwordChange.PreventReusingLastNPasswords	1 (times)	1 - 10
NODE.security.passwordChange.RequirePasswordChangeOnFirstLoginToNewAccount	FALSE	TRUE; FALSE

Default Name	Default Value	Default Domain
NODE.security.passwordComplexity.IdenticalConsecutiveCharactersAllowed	3 or more	0-2; 3 or more
NODE.security.passwordComplexity.MaximumLength	20	20; 80
NODE.security.passwordComplexity.MinimumLength	6	6; 8; 10; 12
NODE.security.passwordComplexity.MinimumRequiredCharacters	1 num; 1 letter & 1 TL1 special	1 num; 1 letter & 1 TL1 special; 1 num; 1 letter & 1 special; 2 each of any 2 of num; upper; lower & TL1 special; 2 each of any 2 of num; upper; lower & special
NODE.security.passwordComplexity.ReverseUserIdAllowed	TRUE	TRUE; FALSE
NODE.security.pseudoIOSAccess.AccessState	NonSecure	Disabled; NonSecure; Secure
NODE.security.pseudoIOSAccess.Port	65000	1024 - 65535
NODE.security.pseudoIOSAccess.SecurePort	64000	1024 - 65535
NODE.security.radiusServer.AccountingPort	1813 (port)	0 - 32767
NODE.security.radiusServer.AuthenticationPort	1812 (port)	0 - 32767
NODE.security.radiusServer.EnableNodeAsFinalAuthenticator	TRUE	FALSE; TRUE
NODE.security.serialCraftAccess.EnableCraftPort	TRUE	TRUE; FALSE
NODE.security.shellAccess.AccessState	NonSecure	Disabled; NonSecure; Secure
NODE.security.shellAccess.EnableShellPassword	FALSE	TRUE; FALSE
NODE.security.shellAccess.TelnetPort	23	23 - 9999
NODE.security.snmpAccess.AccessState	NonSecure	Disabled; NonSecure
NODE.security.tl1Access.AccessState	NonSecure	Disabled; NonSecure; Secure
NODE.security.userLockout.FailedLoginsAllowedBeforeLockout	5 (times)	0 - 10
NODE.security.userLockout.LockoutDuration	00:30 (mins:secs)	00:00; 00:05; 00:10 .. 10:00

Default Name	Default Value	Default Domain
NODE.security.userLockout. ManualUnlockBySuperuser	FALSE	TRUE; FALSE
NODE.software.AllowDelayedUpgrades	FALSE	FALSE; TRUE
NODE.software.DefaultDelayedUpgrades	FALSE	FALSE; TRUE when AllowDelayedUpgrades TRUE; FALSE when AllowDelayedUpgrades FALSE
NODE.timing.general.Mode	External	External; Line; Mixed
NODE.timing.general.QualityOfRES	RES=DUS	PRS<RES; STU<RES<PRS; ST2<RES<STU; ST3<RES<ST2; SMC<RES<ST3; ST4<RES<SMC; RES<ST4; RES=DUS when SSMMessageSet Generation 1; PRS<RES; STU<RES<PRS; ST2<RES<STU; TNC<RES<ST2; ST3E<RES<TNC; ST3<RES<ST3E; SMC<RES<ST3; ST4<RES<SMC; RES<ST4; RES=DUS when SSMMessageSet Generation 2; N/A when SSMMessageSet N/A
NODE.timing.general.ReversionTime	5.0 (minutes)	0.5; 1.0; 1.5 .. 12.0
NODE.timing.general.Revertive	FALSE	TRUE; FALSE
NODE.timing.general.SSMMessageSet	Generation 1	Generation 1; Generation 2 when TimingStandard SONET; N/A when TimingStandard SDH
NODE.timing.general.TimingStandard	SONET	SONET; SDH
PTF-4.config.client.AINSSoakTime	08:00 (hours:mins)	00:00; 00:15; 00:30 .. 48:00
PTF-4.config.client.AdminState	OOS;DSBLD	IS; OOS;DSBLD
PTF-4.config.ppmPortAssignment	TEN-GE	UNASSIGNED; TEN-GE
PTF-4.config.ppmSlotAssignment	PPM (1 Port)	UNASSIGNED; PPM (1 Port)
PTF-4.config.trunk.AINSSoakTime	08:00 (hours:mins)	00:00; 00:15; 00:30 .. 48:00
PTF-4.config.trunk.AdminState	OOS;DSBLD	IS; OOS;DSBLD
PTF-4.opticalthresholds.client.10gethernet. 10ger.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet. 10ger.15min.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.client.10gethernet.10ger.15min.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10ger.15min.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10ger.15min.LowTxPower	-14.2 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.client.10gethernet.10ger.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10ger.1day.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10ger.1day.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10ger.1day.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10ger.1day.LowTxPower	-14.2 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.client.10gethernet.10ger.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10ger.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10ger.alarm.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10ger.alarm.LowRxPower	-16.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10ger.alarm.LowTxPower	-10.7 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.client.10gethernet.10glr.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.client.10gethernet.10glr.15min.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10glr.15min.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10glr.15min.LowRxPower	-15.8 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10glr.15min.LowTxPower	-10.7 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.client.10gethernet.10glr.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10glr.1day.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10glr.1day.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10glr.1day.LowRxPower	-15.8 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10glr.1day.LowTxPower	-10.7 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.client.10gethernet.10glr.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10glr.alarm.HighRxPower	1.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10glr.alarm.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10glr.alarm.LowRxPower	-18.3 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10glr.alarm.LowTxPower	-7.2 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.client.10gethernet.10gsr.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.15min.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.15min.HighTxPower	4.7 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.15min.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10gsr.15min.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.client.10gethernet.10gsr.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.1day.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.1day.HighTxPower	4.7 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.1day.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.client.10gethernet.10gsr.1day.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.client.10gethernet.10gsr.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.alarm.HighRxPower	1.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.alarm.HighTxPower	1.2 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.client.10gethernet.10gsr.alarm.LowRxPower	-12.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.client.10gethernet.10gsr.alarm.LowTxPower	-9.8 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.15min.HighTxPower	13.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.15min.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.15min.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.1day.HighTxPower	13.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.1day.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.1day.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.alarm.HighTxPower	9.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.alarm.LowRxPower	-16.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.disabledfec.alarm.LowTxPower	0.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.15min.HighTxPower	13.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.15min.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.15min.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.1day.HighTxPower	13.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.1day.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.1day.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.alarm.HighTxPower	9.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.alarm.LowRxPower	-16.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.enhancedfec.alarm.LowTxPower	0.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.15min.HighTxPower	13.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.15min.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.15min.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.1day.HighTxPower	13.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.1day.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.1day.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.alarm.HighTxPower	9.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.alarm.LowRxPower	-16.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.cwdm40km.standardfec.alarm.LowTxPower	0.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.15min.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.15min.LowRxPower	-24.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.1day.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.1day.LowRxPower	-24.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.alarm.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.alarm.LowRxPower	-26.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.disabledfec.alarm.LowTxPower	-2.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.15min.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.15min.LowRxPower	-26.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.1day.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.1day.LowRxPower	-26.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.alarm.HighTxPower	5.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.alarm.LowRxPower	-29.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.enhancedfec.alarm.LowTxPower	-2.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.15min.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.15min.LowRxPower	-26.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.1day.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.1day.LowRxPower	-26.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.alarm.HighTxPower	5.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.alarm.LowRxPower	-29.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.dwdm.standardfec.alarm.LowTxPower	-2.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.15min.HighRxPower	2.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.15min.HighTxPower	8.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.15min.LowRxPower	-15.8 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.15min.LowTxPower	-7.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.1day.HighRxPower	2.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.1day.HighTxPower	8.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.1day.LowRxPower	-15.8 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.1day.LowTxPower	-7.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.alarm.HighRxPower	4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.alarm.HighTxPower	4.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.alarm.LowRxPower	-18.3 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.disabledfec.alarm.LowTxPower	-3.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.15min.HighLaserBias	95.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.15min.HighRxPower	1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.15min.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.15min.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.15min.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.1day.HighLaserBias	96.0 (%)	0.0; 0.1; 0.2 .. 100.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.1day.HighRxPower	1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.1day.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.1day.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.1day.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.alarm.HighTxPower	1.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.alarm.LowRxPower	-16.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.enhancedfec.alarm.LowTxPower	-8.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.15min.HighLaserBias	95.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.15min.HighRxPower	1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.15min.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.15min.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.15min.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.1day.HighLaserBias	96.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.1day.HighRxPower	1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.1day.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.1day.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.1day.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.alarm.HighTxPower	1.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.alarm.LowRxPower	-16.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.ir2.standardfec.alarm.LowTxPower	-8.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.15min.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.15min.LowRxPower	-24.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.1day.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.1day.LowRxPower	-24.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.alarm.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.alarm.LowRxPower	-26.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.disabledfec.alarm.LowTxPower	-2.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.15min.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.15min.LowRxPower	-27.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.15min.LowTxPower	-7.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.1day.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.1day.LowRxPower	-27.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.1day.LowTxPower	-7.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.alarm.HighTxPower	5.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.alarm.LowRxPower	-29.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.enhancedfec.alarm.LowTxPower	-3.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.15min.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.15min.LowRxPower	-27.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.15min.LowTxPower	-7.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.1day.HighTxPower	9.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.1day.LowRxPower	-27.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.1day.LowTxPower	-7.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.alarm.HighTxPower	5.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.alarm.LowRxPower	-29.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.lr2.standardfec.alarm.LowTxPower	-3.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.15min.HighLaserBias	95.0 (%)	0.0; 0.1; 0.2 .. 100.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.15min.HighRxPower	1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.15min.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.15min.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.15min.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.1day.HighLaserBias	96.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.1day.HighRxPower	1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.1day.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.1day.LowRxPower	-14.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.1day.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.alarm.HighTxPower	1.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.alarm.LowRxPower	-16.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.disabledfec.alarm.LowTxPower	-8.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.15min.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.15min.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.15min.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.15min.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.1day.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.1day.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.1day.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.1day.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.alarm.HighRxPower	1.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.alarm.HighTxPower	1.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.alarm.LowRxPower	-12.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.sr.enhancedfec.alarm.LowTxPower	-9.8 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.15min.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.15min.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.15min.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.15min.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.1day.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.1day.HighTxPower	5.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.1day.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.1day.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.alarm.HighRxPower	1.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.alarm.HighTxPower	1.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.alarm.LowRxPower	-12.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr.standardfec.alarm.LowTxPower	-9.8 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.15min.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.15min.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.15min.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.15min.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.1day.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.1day.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.1day.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.1day.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.alarm.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.alarm.LowRxPower	-16.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.disabledfec.alarm.LowTxPower	-8.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.15min.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.15min.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.15min.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.15min.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.1day.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.1day.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.1day.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.1day.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.alarm.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.alarm.LowRxPower	-16.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.enhancedfec.alarm.LowTxPower	-8.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.15min.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.15min.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.15min.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.15min.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.1day.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.1day.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.1day.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.1day.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower

Default Name	Default Value	Default Domain
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.alarm.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.alarm.LowRxPower	-16.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTF-4.opticalthresholds.trunk.10gethernet.sr1.standardfec.alarm.LowTxPower	-8.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTF-4.otn.g709thresholds.pm.farend.15min.BBE	85040 (count)	0 - 8850600
PTF-4.otn.g709thresholds.pm.farend.15min.ES	87 (seconds)	0 - 900
PTF-4.otn.g709thresholds.pm.farend.15min.FC	10 (count)	0 - 72
PTF-4.otn.g709thresholds.pm.farend.15min.SES	1 (seconds)	0 - 900
PTF-4.otn.g709thresholds.pm.farend.15min.UAS	3 (seconds)	0 - 900
PTF-4.otn.g709thresholds.pm.farend.1day.BBE	850400 (count)	0 - 849657600
PTF-4.otn.g709thresholds.pm.farend.1day.ES	864 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.pm.farend.1day.FC	40 (count)	0 - 6912
PTF-4.otn.g709thresholds.pm.farend.1day.SES	4 (seconds)	0 - 86400

Default Name	Default Value	Default Domain
PTF-4.otn.g709thresholds.pm.farend.1day.UAS	10 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.pm.nearend.15min.BBE	85040 (count)	0 - 8850600
PTF-4.otn.g709thresholds.pm.nearend.15min.ES	87 (seconds)	0 - 900
PTF-4.otn.g709thresholds.pm.nearend.15min.FC	10 (count)	0 - 72
PTF-4.otn.g709thresholds.pm.nearend.15min.SES	1 (seconds)	0 - 900
PTF-4.otn.g709thresholds.pm.nearend.15min.UAS	3 (seconds)	0 - 900
PTF-4.otn.g709thresholds.pm.nearend.1day.BBE	850400 (count)	0 - 849657600
PTF-4.otn.g709thresholds.pm.nearend.1day.ES	864 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.pm.nearend.1day.FC	40 (count)	0 - 6912
PTF-4.otn.g709thresholds.pm.nearend.1day.SES	4 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.pm.nearend.1day.UAS	10 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.sm.farend.15min.BBE	10000 (count)	0 - 8850600
PTF-4.otn.g709thresholds.sm.farend.15min.ES	500 (seconds)	0 - 900
PTF-4.otn.g709thresholds.sm.farend.15min.FC	10 (count)	0 - 72

Default Name	Default Value	Default Domain
PTF-4.otn.g709thresholds.sm.farend.15min.SES	500 (seconds)	0 - 900
PTF-4.otn.g709thresholds.sm.farend.15min.UAS	500 (seconds)	0 - 900
PTF-4.otn.g709thresholds.sm.farend.1day.BBE	100000 (count)	0 - 849657600
PTF-4.otn.g709thresholds.sm.farend.1day.ES	5000 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.sm.farend.1day.FC	40 (count)	0 - 6912
PTF-4.otn.g709thresholds.sm.farend.1day.SES	5000 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.sm.farend.1day.UAS	5000 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.sm.nearend.15min.BBE	10000 (count)	0 - 8850600
PTF-4.otn.g709thresholds.sm.nearend.15min.ES	500 (seconds)	0 - 900
PTF-4.otn.g709thresholds.sm.nearend.15min.FC	10 (count)	0 - 72
PTF-4.otn.g709thresholds.sm.nearend.15min.SES	500 (seconds)	0 - 900
PTF-4.otn.g709thresholds.sm.nearend.15min.UAS	500 (seconds)	0 - 900
PTF-4.otn.g709thresholds.sm.nearend.1day.BBE	100000 (count)	0 - 849657600
PTF-4.otn.g709thresholds.sm.nearend.1day.ES	5000 (seconds)	0 - 86400

Default Name	Default Value	Default Domain
PTF-4.otn.g709thresholds.sm.nearend.1day.FC	40 (count)	0 - 6912
PTF-4.otn.g709thresholds.sm.nearend.1day.SES	5000 (seconds)	0 - 86400
PTF-4.otn.g709thresholds.sm.nearend.1day.UAS	5000 (seconds)	0 - 86400
PTF-4.otn.otnLines.FEC	Standard	Disable; Standard; Enhanced when G709OTN Enable; Disable when G709OTN Disable
PTF-4.otn.otnLines.G709OTN	Enable	Disable; Enable
PTF-4.otn.otnLines.SDBER	1.00E-07	1E-5; 1E-6; 1E-7; 1E-8; 1E-9
PTM-4.config.10GE.AINSSoakTime	08:00 (hours:mins)	00:00; 00:15; 00:30 .. 48:00
PTM-4.config.10GE.AdminState	OOS;DSBLD	IS; OOS;DSBLD
PTM-4.config.ppmPortAssignment	TEN-GE	UNASSIGNED; TEN-GE
PTM-4.config.ppmSlotAssignment	PPM (1 Port)	UNASSIGNED; PPM (1 Port)
PTM-4.opticalthresholds.client.10gethernet.10ger.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet.10ger.15min.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10ger.15min.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10ger.15min.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10ger.15min.LowTxPower	-14.2 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTM-4.opticalthresholds.client.10gethernet.10ger.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet.10ger.1day.HighRxPower	0.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTM-4.opticalthresholds.client.10gethernet.10ger.1day.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10ger.1day.LowRxPower	-14.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10ger.1day.LowTxPower	-14.2 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTM-4.opticalthresholds.client.10gethernet.10ger.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet.10ger.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10ger.alarm.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10ger.alarm.LowRxPower	-16.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10ger.alarm.LowTxPower	-10.7 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTM-4.opticalthresholds.client.10gethernet.10glr.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet.10glr.15min.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10glr.15min.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10glr.15min.LowRxPower	-15.8 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10glr.15min.LowTxPower	-10.7 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTM-4.opticalthresholds.client.10gethernet.10glr.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0

Default Name	Default Value	Default Domain
PTM-4.opticalthresholds.client.10gethernet.10glr.1day.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10glr.1day.HighTxPower	10.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10glr.1day.LowRxPower	-15.8 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10glr.1day.LowTxPower	-10.7 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTM-4.opticalthresholds.client.10gethernet.10glr.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet.10glr.alarm.HighRxPower	1.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10glr.alarm.HighTxPower	6.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10glr.alarm.LowRxPower	-18.3 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10glr.alarm.LowTxPower	-7.2 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTM-4.opticalthresholds.client.10gethernet.10gsr.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.15min.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.15min.HighTxPower	4.7 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.15min.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10gsr.15min.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower

Default Name	Default Value	Default Domain
PTM-4.opticalthresholds.client.10gethernet.10gsr.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.1day.HighRxPower	-1.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.1day.HighTxPower	4.7 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.1day.LowRxPower	-9.9 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10gsr.1day.LowTxPower	-13.3 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTM-4.opticalthresholds.client.10gethernet.10gsr.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.alarm.HighRxPower	1.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.alarm.HighTxPower	1.2 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTM-4.opticalthresholds.client.10gethernet.10gsr.alarm.LowRxPower	-12.4 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTM-4.opticalthresholds.client.10gethernet.10gsr.alarm.LowTxPower	-9.8 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.config.10GE.AINSSoakTime	08:00 (hours:mins)	00:00; 00:15; 00:30 .. 48:00
PTSA.config.10GE.AdminState	IS	IS; OOS;DSBLD
PTSA.config.1GE.AINSSoakTime	08:00 (hours:mins)	00:00; 00:15; 00:30 .. 48:00
PTSA.config.1GE.AdminState	OOS;DSBLD	IS; OOS;DSBLD
PTSA.config.FE.AINSSoakTime	08:00 (hours:mins)	00:00; 00:15; 00:30 .. 48:00
PTSA.config.FE.AdminState	OOS;DSBLD	IS; OOS;DSBLD
PTSA.config.ppmPortAssignment	UNASSIGNED	UNASSIGNED; ONE-GE; FE

Default Name	Default Value	Default Domain
PTSA.config.ppmSlotAssignment	UNASSIGNED	UNASSIGNED; PPM (1 Port)
PTSA.opticalthresholds.client.1gethernet.cwdm.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.cwdm.15min.HighRxPower	-9.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.cwdm.15min.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.cwdm.15min.LowRxPower	-29.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.cwdm.15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.cwdm.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.cwdm.1day.HighRxPower	-9.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.cwdm.1day.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.cwdm.1day.LowRxPower	-29.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.cwdm.1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.cwdm.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.cwdm.alarm.HighRxPower	-6.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.cwdm.alarm.HighTxPower	8.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.cwdm.alarm.LowRxPower	-32.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower

Default Name	Default Value	Default Domain
PTSA.opticalthresholds.client.1gethernet.cwdm.alarm.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.lx.15min.HighLaserBias	81.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.lx.15min.HighRxPower	-3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.lx.15min.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.lx.15min.LowRxPower	-20.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.lx.15min.LowTxPower	-16.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.lx.1day.HighLaserBias	85.5 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.lx.1day.HighRxPower	-3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.lx.1day.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.lx.1day.LowRxPower	-20.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.lx.1day.LowTxPower	-16.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.lx.alarm.HighLaserBias	90.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.lx.alarm.HighRxPower	0.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.lx.alarm.HighTxPower	-1.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTSA.opticalthresholds.client.1gethernet.lx.alarm.LowRxPower	-23.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.lx.alarm.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.sx.15min.HighLaserBias	81.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.sx.15min.HighRxPower	0.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.sx.15min.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.sx.15min.LowRxPower	-17.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.sx.15min.LowTxPower	-16.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.sx.1day.HighLaserBias	85.5 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.sx.1day.HighRxPower	0.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.sx.1day.HighTxPower	3.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.sx.1day.LowRxPower	-17.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.sx.1day.LowTxPower	-16.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.sxalarm.HighLaserBias	90.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.sx.alarm.HighRxPower	3.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTSA.opticalthresholds.client.1gethernet.sx.alarm.HighTxPower	-2.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.sx.alarm.LowRxPower	-20.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.sx.alarm.LowTxPower	-12.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.t.15min.HighLaserBias	100.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.t.15min.HighRxPower	30.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.t.15min.HighTxPower	30.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.t.15min.LowRxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.t.15min.LowTxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.t.1day.HighLaserBias	100.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.t.1day.HighRxPower	30.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.t.1day.HighTxPower	30.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.t.1day.LowRxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.t.1day.LowTxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.t.alarm.HighLaserBias	100.0 (%)	0.0; 0.1; 0.2 .. 100.0

Default Name	Default Value	Default Domain
PTSA.opticalthresholds.client.1gethernet.t.alarm.HighRxPower	30.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.t.alarm.HighTxPower	30.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.t.alarm.LowRxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.t.alarm.LowTxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.zx.15min.HighLaserBias	100.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.zx.15min.HighRxPower	30.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.zx.15min.HighTxPower	30.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.zx.15min.LowRxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.zx.15min.LowTxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.1gethernet.zx.1day.HighLaserBias	100.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.zx.1day.HighRxPower	30.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.zx.1day.HighTxPower	30.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.zx.1day.LowRxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.zx.1day.LowTxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower

Default Name	Default Value	Default Domain
PTSA.opticalthresholds.client.1gethernet.zx.alarm.HighLaserBias	100.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.1gethernet.zx.alarm.HighRxPower	30.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.zx.alarm.HighTxPower	30.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.1gethernet.zx.alarm.LowRxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.1gethernet.zx.alarm.LowTxPower	-40.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.fastethernet.lx.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.fastethernet.lx.15min.HighRxPower	-8.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.lx.15min.HighTxPower	-2.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.lx.15min.LowRxPower	-28.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.fastethernet.lx.15min.LowTxPower	-21.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.fastethernet.lx.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.fastethernet.lx.1day.HighRxPower	-8.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.lx.1day.HighTxPower	-2.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.lx.1day.LowRxPower	-28.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower

Default Name	Default Value	Default Domain
PTSA.opticalthresholds.client.fastethernet.lx.1day.LowTxPower	-21.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.fastethernet.lx.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.fastethernet.lx.alarm.HighRxPower	-5.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.lx.alarm.HighTxPower	-5.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.lx.alarm.LowRxPower	-30.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.fastethernet.lx.alarm.LowTxPower	-17.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.fastethernet.sx.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.fastethernet.sx.15min.HighRxPower	-14.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.sx.15min.HighTxPower	-8.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.sx.15min.LowRxPower	-31.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.fastethernet.sx.15min.LowTxPower	-25.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.fastethernet.sx.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.fastethernet.sx.1day.HighRxPower	-14.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.sx.1day.HighTxPower	-8.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
PTSA.opticalthresholds.client.fastethernet.sx.1day.LowRxPower	-31.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.fastethernet.sx.1day.LowTxPower	-25.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
PTSA.opticalthresholds.client.fastethernet.sx.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
PTSA.opticalthresholds.client.fastethernet.sx.alarm.HighRxPower	-11.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.sx.alarm.HighTxPower	-11.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
PTSA.opticalthresholds.client.fastethernet.sx.alarm.LowRxPower	-33.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
PTSA.opticalthresholds.client.fastethernet.sx.alarm.LowTxPower	-21.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.config.fe.AlsMode	Auto Restart	Disabled; Auto Restart
TNC.config.ge.AlsMode	Auto Restart	Disabled; Auto Restart
TNC.config.oc3.AlsMode	Auto Restart	Disabled; Auto Restart
TNC.opticalthresholds.1gethernet.cwdm.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.1gethernet.cwdm.15min.HighRxPower	-9.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.1gethernet.cwdm.15min.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.1gethernet.cwdm.15min.LowRxPower	-29.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.1gethernet.cwdm.15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.1gethernet.cwdm.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0

Default Name	Default Value	Default Domain
TNC.opticalthresholds.1gethernet.cwdm.1day.HighRxPower	-9.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.1gethernet.cwdm.1day.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.1gethernet.cwdm.1day.LowRxPower	-29.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.1gethernet.cwdm.1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.1gethernet.cwdm.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.1gethernet.cwdm.alarm.HighRxPower	-6.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.1gethernet.cwdm.alarm.HighTxPower	8.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.1gethernet.cwdm.alarm.LowRxPower	-32.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.1gethernet.cwdm.alarm.LowTxPower	-3.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.fastethernet.lx.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.fastethernet.lx.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.lx.15min.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.lx.15min.LowRxPower	-34.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.fastethernet.lx.15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower

Default Name	Default Value	Default Domain
TNC.opticalthresholds.fastethernet.lx.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.fastethernet.lx.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.lx.1day.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.lx.1day.LowRxPower	-34.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.fastethernet.lx.1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.fastethernet.lx.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.fastethernet.lx.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.lx.alarm.HighTxPower	7.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.lx.alarm.LowRxPower	-36.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.fastethernet.lx.alarm.LowTxPower	-2.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.fastethernet.ulh.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.fastethernet.ulh.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.ulh.15min.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.ulh.15min.LowRxPower	-43.0 (dBm)	-50.0; -49.9; -49.8 .. HighRxPower

Default Name	Default Value	Default Domain
TNC.opticalthresholds.fastethernet.ulh.15min.LowTxPower	-5.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.fastethernet.ulh.1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.fastethernet.ulh.1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.ulh.1day.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.ulh.1day.LowRxPower	-43.0 (dBm)	-50.0; -49.9; -49.8 .. HighRxPower
TNC.opticalthresholds.fastethernet.ulh.1day.LowTxPower	-5.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.fastethernet.ulh.alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.fastethernet.ulh.alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.ulh.alarm.HighTxPower	7.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.fastethernet.ulh.alarm.LowRxPower	-45.5 (dBm)	-50.0; -49.9; -49.8 .. HighRxPower
TNC.opticalthresholds.fastethernet.ulh.alarm.LowTxPower	-1.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.oc3.lr2.15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.oc3.lr2.15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.lr2.15min.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
TNC.opticalthresholds.oc3.lr2. 15min.LowRxPower	-34.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.oc3.lr2. 15min.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.oc3.lr2. 1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.oc3.lr2. 1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.lr2. 1day.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.lr2. 1day.LowRxPower	-34.0 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.oc3.lr2. 1day.LowTxPower	-6.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.oc3.lr2. alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.oc3.lr2. alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.lr2. alarm.HighTxPower	7.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.lr2. alarm.LowRxPower	-36.5 (dBm)	-40.0; -39.9; -39.8 .. HighRxPower
TNC.opticalthresholds.oc3.lr2. alarm.LowTxPower	-2.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.oc3.ulh. 15min.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.oc3.ulh. 15min.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0

Default Name	Default Value	Default Domain
TNC.opticalthresholds.oc3.ulh. 15min.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.ulh. 15min.LowRxPower	-43.0 (dBm)	-50.0; -49.9; -49.8 .. HighRxPower
TNC.opticalthresholds.oc3.ulh. 15min.LowTxPower	-5.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.oc3.ulh. 1day.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.oc3.ulh. 1day.HighRxPower	-7.0 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.ulh. 1day.HighTxPower	11.0 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.ulh. 1day.LowRxPower	-43.0 (dBm)	-50.0; -49.9; -49.8 .. HighRxPower
TNC.opticalthresholds.oc3.ulh. 1day.LowTxPower	-5.0 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.opticalthresholds.oc3.ulh. alarm.HighLaserBias	98.0 (%)	0.0; 0.1; 0.2 .. 100.0
TNC.opticalthresholds.oc3.ulh. alarm.HighRxPower	-4.5 (dBm)	LowRxPower; LowRxPower + 0.1; LowRxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.ulh. alarm.HighTxPower	7.5 (dBm)	LowTxPower; LowTxPower + 0.1; LowTxPower + 0.2 .. 30.0
TNC.opticalthresholds.oc3.ulh. alarm.LowRxPower	-45.5 (dBm)	-50.0; -49.9; -49.8 .. HighRxPower
TNC.opticalthresholds.oc3.ulh. alarm.LowTxPower	-1.5 (dBm)	-40.0; -39.9; -39.8 .. HighTxPower
TNC.pmthresholds.line.farend. 15min.CV	1312 (B2 count)	0 - 137700

Default Name	Default Value	Default Domain
TNC.pmthresholds.line.farend. 15min.ES	87 (seconds)	0 - 900
TNC.pmthresholds.line.farend. 15min.FC	10 (count)	0 - 72
TNC.pmthresholds.line.farend. 15min.SES	1 (seconds)	0 - 900
TNC.pmthresholds.line.farend. 15min.UAS	3 (seconds)	0 - 900
TNC.pmthresholds.line.farend. 1day.CV	13120 (B2 count)	0 - 13219200
TNC.pmthresholds.line.farend. 1day.ES	864 (seconds)	0 - 86400
TNC.pmthresholds.line.farend. 1day.FC	40 (count)	0 - 6912
TNC.pmthresholds.line.farend. 1day.SES	4 (seconds)	0 - 86400
TNC.pmthresholds.line.farend. 1day.UAS	10 (seconds)	0 - 86400
TNC.pmthresholds.line.nearend. 15min.CV	1312 (B2 count)	0 - 137700
TNC.pmthresholds.line.nearend. 15min.ES	87 (seconds)	0 - 900
TNC.pmthresholds.line.nearend. 15min.FC	10 (count)	0 - 72
TNC.pmthresholds.line.nearend. 15min.SES	1 (seconds)	0 - 900
TNC.pmthresholds.line.nearend. 15min.UAS	3 (seconds)	0 - 900

Default Name	Default Value	Default Domain
TNC.pmthresholds.line.nearend.1day.CV	13120 (B2 count)	0 - 13219200
TNC.pmthresholds.line.nearend.1day.ES	864 (seconds)	0 - 86400
TNC.pmthresholds.line.nearend.1day.FC	40 (count)	0 - 6912
TNC.pmthresholds.line.nearend.1day.SES	4 (seconds)	0 - 86400
TNC.pmthresholds.line.nearend.1day.UAS	10 (seconds)	0 - 86400
TNC.pmthresholds.section.nearend.15min.CV	10000 (B1 count)	0 - 138600
TNC.pmthresholds.section.nearend.15min.ES	500 (seconds)	0 - 900
TNC.pmthresholds.section.nearend.15min.SEFS	500 (seconds)	0 - 900
TNC.pmthresholds.section.nearend.15min.SES	500 (seconds)	0 - 900
TNC.pmthresholds.section.nearend.1day.CV	100000 (B1 count)	0 - 13305600
TNC.pmthresholds.section.nearend.1day.ES	5000 (seconds)	0 - 86400
TNC.pmthresholds.section.nearend.1day.SEFS	5000 (seconds)	0 - 86400
TNC.pmthresholds.section.nearend.1day.SES	5000 (seconds)	0 - 86400

INDEX

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

W

Y