Cisco CPT Command Reference Guide–CTC and Documentation Release 9.3 and Cisco IOS Release 15.1(01)SA

First Published: July 19, 2011

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: 78-20206-01

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

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:

Revision History

Date	Notes
October 2012	Added miscellaneous commands in the Miscellaneous Command Reference, on page 355 chapter.

Document Objectives

This guide describes the commands available to configure and maintain the Cisco Carrier Packet Transport system.

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
EVC Command Reference, on page 1	Describes commands used to configure Ethernet Virtual Circuit (EVC).
MPLS Command Reference, on page 15	Describes commands to configure Multiprotocol Label Switching (MPLS).
MPLS TP Command Reference, on page 105	Describes commands to configure Multiprotocol Label Switching Transport Profile (MPLS TP).
Pseudowire Command Reference, on page 141	Describes commands used to configure the pseudowire.
QoS Command Reference, on page 177	Describes commands used to configure Quality of Service (QoS).
High Availability Command Reference, on page 229	Describes commands to configure high availability.
REP Command Reference, on page 267	Describes commands to configure Resilient Ethernet Protocol (REP).
LAG and LACP Command Reference, on page 285	Describes commands to configure Link Aggregation Group (LAG) and Link Aggregation Control Protocol (LACP).
MAC Learning Command Reference, on page 301	Describes commands to configure MAC learning.
IGMP Snooping Command Reference, on page 309	Describes commands used to configure Internet Group Management Protocol (IGMP) snooping.
MVR Command Reference, on page 319	Describes commands used to configure Multicast VLAN Registration (MVR).

Chapter	Description
RMON Command Reference, on page 329	Describes commands to configure Remote Network MONitoring (RMON).
CDP Command Reference, on page 345	Describes commands used to monitor the router and network using Cisco Discovery Protocol (CDP).
Miscellaneous Command Reference, on page 355	Describes miscellaneous commands used to configure CPT services.

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.
|	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.

Convention	Description
[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	**ЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ** **Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, которой следует опасаться телесных повреждений. Перед эксплуатацией оборудова выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявлен приведенным в конце каждого предупреждения, чтобы найти его переведенный вар 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 있습니 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되 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 σ τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή. ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ
אזהרה	**ת בטיחות חשובות** אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד , עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים ת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום ות הבטיחות המתורגמות שמצורפות להתקן. **הוראות אלה**
предупредување	ЖНИ 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 шт постои кај електричните кола и треба да ги познавате стандардните постапки за спречуван 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 standardowym 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 Configuration Guide–CTC and Documentation Release 9.3 and Cisco IOS Release 15.1(01)SA*
- *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*

Obtaining Optical Networking Information

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

Where to Find Safety and Warning Information

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

Cisco Optical Networking Product Documentation CD-ROM

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

Obtaining Documentation and Submitting a Service Request

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

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

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

Cisco CPT Documentation Roadmap

To quickly access publications of Cisco CPT Release 9.3, see the http://www.cisco.com/en/US/docs/optical/15000r9_3/doc_roadmap/onsroadmap93.html

EVC Command Reference

This chapter describes commands used to configure an Ethernet Virtual Circuit (EVC).

bridge-domain

To bind a service instance to a bridge domain instance, use the **bridge-domain** command in service instance configuration mode. To unbind a service instance from a bridge domain instance, use the **no** form of this command.

bridge-domain *bridge-id* [**split-horizon**]

no bridge-domain

Syntax Description

bridge-id	Numerical ID of the bridge domain instance. The range is from 1 to 16384.
split-horizon	(Optional) Configures a port or service instance as a member of a split-horizon group.

Command Default

Service instances are not bound to a bridge domain instance.

Command Modes

Service instance configuration (config-if-svc)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use the **bridge-domain** command to bind a service instance to a bridge domain.

Examples

The following example shows how to bind a bridge domain to a service instance using the **bridge-domain** command

```
Router> enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# bridge-domain 200
```

Related Commands

Command	Description
mode p2p	Configures the bridge domain in p2p or p2mp mode.

clear ethernet service instance

To clear Ethernet service instance attributes such as MAC addresses and statistics or to purge Ethernet service instance errors, use the **clear ethernet service instance** command in privileged EXEC mode.

clear ethernet service instance {id *identifier* **interface** *type number* {**errdisable** | **mac table** [*address*] | **stats**} | **interface** *type number* **stats**}

Syntax Description

id *identifier*	Indicates that a service instance is specified.
interface	Indicates that a specific interface is specified.
type	Type of interface.
number	Number of the interface.
errdisable	Indicates that a clear action for an error-disabled state is specified.
mac table	Indicates that a MAC table is specified.
address	Address in the specified MAC table.
stats	Indicates that the service instance statistics are specified.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use the **clear ethernet service instance** command to clear the service instance attributes that are not needed and to purge service instance errors.

Examples

The following example shows how to clear an error-disabled state on service instance 100 on interface TenGigabitEthernet 4/1 using the **clear ethernet service instance** command:

```
Router# clear ethernet service instance id 100 interface TenGigabitEthernet 4/1 errdisable
```

Related Commands

Command	Description
show ethernet service instance	Displays information about Ethernet service instances.

encapsulation

To define the matching criteria that maps the ingress dot1q, QinQ, or untagged frames on an interface to the appropriate service instance, use the **encapsulation dot1q** command in service instance configuration mode.

encapsulation dot1q {*any* | *vlan-id* [*vlan-id* [-*vlan-id*]]} **second-dot1q** {*any* | *vlan-id* [*vlan-id* [-*vlan-id*]]}

Syntax Description

dot1q	Specifies a 802.1Q tag at the ingress service instance.
any	Indicates that all VLANs are to be configured.
vlan-id	Integer in the range 1 to 4094 that identifies the VLAN.
second-dot1q	Specifies a different 802.1Q tag at the ingress service instance.

Command Default

Encapsulation is not configured.

Command Modes

Service instance configuration mode (config-if-srv)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to configure dot1q encapsulation.

```
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)#
```

l2protocol

To configure Layer 2 protocol tunneling for the interfaces, use the **l2protocol** command in interface configuration mode.

l2protocol [**drop**|**forward**|**peer**] [**cdp**|**dot1x**|**dtp**|**lacp**|**pagp**|**stp**|**vtp**]

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to define a Layer 2 protocol tunneling action for an interface.

```
Router> enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# l2protocol forward cdp
```

mode

To configure the bridge domain, use the **mode** command in global configuration mode. To remove the bridge domain from p2p mode, use the **no** form of this command.

mode [p2p]

Syntax Description

p2p	(Optional) Configures the bridge domain in point-to-point (p2p) mode.

Command Default

The default mode of the bridge domain is point-to-multipoint (p2mp).

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The p2p bridge domain can be used for Ethernet Private Line (EPL) and Ethernet Virtual Private Line (EVPL) services. The p2mp bridge domain can be used for Ethernet Private LAN (EPLAN) and Ethernet Virtual Private LAN (EVPLAN) services.

Examples

The following example shows how to configure the bridge domain in p2p mode.

```
Router> enable
Router# configure terminal
Router(config)# bridge-domain 12
Router(config)# mode p2p
```

Related Commands

Command	Description
bridge-domain	Binds a service instance to a bridge domain instance.

rewrite ingress tag

To specify the rewrite operation to be applied on the frame ingress to the service instance, use the **rewrite ingress** tag command in service instance configuration mode. To remove the rewrite operation, use the **no** form of this command.

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**}
no rewrite ingress tag

Syntax Description

push	Adds a tag to a packet.
dot1q	Specifies an IEEE 802.1Q tag.
vlan-id	Integer in the range 1 to 4094 that identifies the VLAN.
second-dot1q	Specifies a different 802.1Q tag at the ingress service instance.
dot1ad	Specifies an IEEE 802.1ad tag.
pop	Removes a tag from a packet.
{1 | 2}	Specifies either the outermost tag or the two outermost tags for removal from a packet.
translate	Translates, by VLAN ID, a tag or a pair of tags defined in the **encapsulation** command.
1-to-1	Translates a single tag defined by the **encapsulation** command to a single tag defined in the **rewrite ingress tag** command.
1-to-2	Translates a single tag defined by the **encapsulation** command to a pair of tags defined in the **rewrite ingress tag** command.
2-to-1	Translates, by VLAN ID, a pair of tags defined by the **encapsulation** command to a single tag defined in the **rewrite ingress tag** command.
2-to-2	Translates, by VLAN ID, a pair of tags defined by the **encapsulation** command to a pair of tags defined in the **rewrite ingress tag** command.
symmetric	(Optional) Indicates a reciprocal adjustment to be done in the egress direction. For example, if the ingress pops a tag, the egress pushes a tag and if the ingress pushes a tag, the egress pops a tag.

Command Default

The frame is left intact on ingress.

Command Modes

Service instance configuration (config-if-srv)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

- The EFP point–to–point service does not support the rewrite egress operation. It supports only the symmetric rewrite operation.
- The EFP multipoint–to–multipoint service supports rewrite ingress with the symmetric option. It does not support the rewrite egress operation.
- 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 for encapsulations involving VLAN range and list.

Examples

The following example shows how to specify the rewrite operation to be applied on the frame ingress to the service instance.

```
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
```

Related Commands

Command	Description
encapsulation	Sets the encapsulation method used by an interface.

service instance ethernet

To configure an Ethernet service instance on an interface and to enter Ethernet service configuration mode, use the **service instance ethernet** command in interface configuration mode. To delete a service instance, use the **no** form of this command.

service instance *id* **ethernet** [*evc-name*]
no service instance *id*

Syntax Description

id	Integer from 1 to 4294967295 that uniquely identifies a service instance on an interface.
evc-name	(Optional) String of a maximum of 100 bytes that associates an Ethernet virtual connection (EVC) to the service instance.

Command Default

No Ethernet service instances are defined.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

A service instance is a configuration object that holds all the management and control-plane attributes and parameters that apply to that service instance on a per-port basis. Different service instances that correspond to the same EVC must share the same name. Service instances are associated with a global EVC object through their shared name.

Examples

The following example shows how to define an Ethernet service instance and enter Ethernet service configuration mode for an EVC:

```
Router> enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# service instance 101 ethernet
Router(config-if-srv)#
```

Related Commands

Command	Description
show ethernet service instance	Displays information about configured Ethernet service instances.

show ethernet service instance

To display information about Ethernet service instances, use the **show ethernet service instance** command in privileged EXEC mode.

show ethernet service instance [**detail** | **id** *id* {**interface** *type number* [**detail** | **mac**] }] | **load-balance** | **platform** | **stats** | **interface** *type number* [**detail** | **load-balance** | **platform** | **stats** | **summary]** | **platform** | **policy-map** | **stats** | **summary**]

Syntax Description

detail	(Optional) Displays detailed information about service instances.
id	(Optional) Displays a specific service instance on an interface that does not map to a VLAN.
id	(Optional) Integer from 1 to 4294967295 that identifies a service instance on an interface that does not map to a VLAN.
interface	(Optional) Displays a specific interface selection for a specified service instance or displays all the service instances in the given interface.
type	(Optional) Type of interface.
number	(Optional) Number of the interface.
mac	(Optional) Displays MAC address data.
load-balance	(Optional) Displays manual load balancing configuration.
platform	(Optional) Displays the port channel EFPs that are currently using the manual or platform load balancing and the egress link.
stats	(Optional) Displays statistics for a specified service instance.
summary	(Optional) Displays summary information about service instances.
policy-map	(Optional) Displays the policy map for service instances.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command is useful for system monitoring and troubleshooting.

Examples

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
```

The following example shows how to 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
```

The following example shows how to display the port channel EFPs that are currently using the manual or platform load balancing and the egress link.

```
Router# show ethernet service instance platform
```

```
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
```

Related Commands

Command	Description
clear ethernet service instance	Clears Ethernet service instance attributes such as MAC addresses and statistics or to purge Ethernet service instance errors.

MPLS Command Reference

This chapter describes commands to configure Multiprotocol Label Switching (MPLS).

affinity

To specify affinity and affinity mask values for an LSP in an LSP attribute list, use the **affinity** command in LSP attributes configuration mode. To remove the specified attribute flags, use the **no** form of this command.

affinity *value* [**mask** *value*]

no affinity

Syntax Description

value	Attribute flag value required for links that make up an LSP. The attribute flag value can be either 0 or 1.
mask *value*	(Optional) 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.

Command Default

Attribute flag values are not specified.

Command Modes

LSP attributes configuration (config-lsp-attr)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The affinity value determines the attribute flags for links that make up the LSP, either 0 or 1. The attribute mask determines which attribute value the router should check. 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 LSP for that bit must match.

An LSP can use a link if the link affinity equals the attribute flag value and the affinity mask value.

Any value set to 1 in the affinity should also be set to 1 in the mask.

To associate the LSP affinity attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier of the specific LSP attribute list.

Examples

The following example shows how to specify the affinity value and affinity mask values for links comprising an LSP.

```
Router(config-lsp-attr)# affinity 0 mask 0
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

auto-bw

To specify an automatic bandwidth configuration for a LSP in an LSP attribute list, use the **auto-bw** command in LSP attributes configuration mode. To remove automatic bandwidth configuration, use the **no** form of this command.

auto-bw [**frequency** *secs*] [**max-bw** *kbps*] [**min-bw** *kbps*] [**collect-bw**]

no auto-bw

Syntax Description

frequency *secs*	(Optional) Specifies the interval between bandwidth adjustments. The specified interval ranges from 300 to 604800 seconds.
max-bw *kbps*	(Optional) Specifies the maximum automatic bandwidth for the path option. The value ranges from 0 to 4294967295 kbps.
min-bw *kbps*	(Optional) Specifies the minimum automatic bandwidth for the path option. The value ranges from 0 to 4294967295 kbps.
collect-bw	(Optional) Collects bandwidth output rate information for the path option, but does not adjust its bandwidth.

Command Default

The automatic bandwidth for the LSP is not enabled.

Command Modes

LSP attributes configuration (config-lsp-attr)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use this command to set an automatic bandwidth configuration for a LSP in an LSP attributes list.

To sample the bandwidth used by an LSP without automatically adjusting it, specify the **collect-bw** keyword in the **auto-bw** command in an LSP attribute list.

If you enter the **auto-bw** command without the **collect-bw** keyword, the bandwidth of the LSP is adjusted to the largest average output rate sampled for the LSP since the last bandwidth adjustment for the LSP was made.

To constrain the automatic bandwidth adjustment that can be made to an LSP in an LSP attribute list, use the **max-bw** or **min-bw** keyword and specify the permitted maximum allowable bandwidth or minimum allowable bandwidth, respectively.

The **no** form of the **auto-bw** command disables the automatic bandwidth adjustment for the tunnel and restores the configured bandwidth for the LSP where configured bandwidth is determined as follows:

- If the LSP bandwidth was explicitly configured with the **mpls traffic-eng lsp attributes lsp-id bandwidth** command after the running configuration was written to the startup configuration, the configured bandwidth is the bandwidth specified by that command.
- Otherwise, the configured bandwidth is the bandwidth specified for the tunnel in the startup configuration.

To associate the LSP automatic bandwidth adjustment attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier of the specific LSP attribute list.

Examples

The following example sets the automatic bandwidth configuration for an LSP in an LSP attribute list.

```
Router(config-lsp-attr)# auto-bw
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

bandwidth

To configure LSP bandwidth in an LSP attribute list, use the **bandwidth** command in LSP attributes configuration mode. To remove the configured bandwidth from the LSP attribute list, use the **no** form of this command.

bandwidth global *kbps*

no bandwidth

Syntax Description

global *kbps*	Indicates a global pool path option. *kbps*—Number of kilobits per second set aside for the path option. The range is from 1 to 4294967295 kbps.

Command Default

The LSP bandwidth is not configured in the LSP attribute list.

Command Modes

LSP attributes configuration (config-lsp-attr)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use this command to configure the LSP bandwidth in the LSP attribute list. The bandwidth configured can be associated with both dynamic and explicit path options.

To associate the LSP bandwidth and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier of the specific LSP attribute list.

The bandwidth configured in the LSP attribute list will override the bandwidth configured on the tunnel.

Examples

The following example shows how to specify an LSP bandwidth in the LSP attribute list.

```
Router(config-lsp-attr)# bandwidth global 1000
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

index

To insert or modify a path entry at a specific index, use the **index** command in IP explicit path configuration mode. To remove the path entry at the specified index, use the **no** form of this command.

index *index command*

no index *index*

Syntax Description

index	Index number at which the path entry will be inserted or modified. The valid values range from 0 to 65534.
command	An IP explicit path configuration command that creates or modifies a path entry.

Command Default

A path entry is not inserted for a specific index.

Command Modes

IP explicit path configuration (cfg-ip-expl-path)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to insert a path entry at index 6.

```
Router(cfg-ip-expl-path)# index 6 next-address 209.165.200.225

Explicit Path identifier 6:
    6: next-address 209.165.200.225
```

Related Commands

Command	Description
ip explicit-path	Enters the command mode for IP explicit paths and creates or modifies the specified path.
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

ip explicit-path

To enter the command mode for IP explicit paths and create or modify the specified path, use the **ip explicit-path** command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip explicit-path {**name** *word* | **identifier** *number*} [**enable** | **disable**]

no ip explicit-path {**name** *word* | **identifier** *number*}

Syntax Description

name *word*	Specifies the name of the explicit path.
identifier *number*	Specifies the number of the explicit path. The range is from 1 to 65535.
enable	(Optional) Enables the path.
disable	(Optional) Prevents the path from being used for routing while it is being configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path.

Examples

The following example shows how to enter the explicit path command mode for IP explicit paths.

```
Router(config)# ip explicit-path identifier 500
Router(config-ip-expl-path)#
```

Related Commands

Command	Description
index	Inserts or modifies a path entry at a specific index.
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

ip route

To establish a static route through a next hop IP address, physical interface, MPLS–TP tunnel, or MPLS–TE tunnel to the destination, use the **ip route** command in global configuration mode. To remove static routes, use the **no** form of this command.

ip route *destination mask* [*next-hop-address*] [**interface** *type number*] [*tunnel-id*] [*cost*]

no ip route *destination mask* [*next-hop-address*] [**interface** *type number*] [*tunnel-id*] [**cost**]

Syntax Description

destination	Destination IP address.
mask	Prefix mask for the destination.
next-hop-address	IP address of the next hop that can be used to reach the destination.
interface *type number*	Specifies the network interface type and interface number.
tunnel-id	ID of MPLS–TP tunnel or MPLS–TE tunnel.
cost	Cost to reach the destination.

Command Default

No static routes are established.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The establishment of a static route is appropriate when the CPT software cannot dynamically build a route to the destination.

Examples

The following example shows how to create a static route through a MPLS–TP tunnel using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# ip route 192.0.2.1 255.255.255.255 tunnel-tp1 2
Router(config)# ip route 192.0.2.1 255.255.255.255 tunnel-tp2 3
Router(config)# exit
```

The following example shows how to create a static route through a physical interface using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# ip route 192.0.2.1 255.255.255.255 TenGigabitEthernet4/1 5
Router(config)# exit
```

ip rsvp bandwidth

To enable Resource Reservation Protocol (RSVP) for IP on an interface, use the **ip rsvp bandwidth** command in interface configuration mode. To disable RSVP, use the **no** form of this command.

ip rsvp bandwidth [*interface-kbps* [*single-flow-kbps*]]
no ip rsvp bandwidth [*interface-kbps* [*single-flow-kbps*]]

Syntax Description

interface-kbps	(Optional) Maximum amount of bandwidth, in kbps, that may be allocated by RSVP flows. The range is from 1 to 10,000,000.
single-flow-kbps	(Optional) Maximum amount of bandwidth, in kbps, that may be allocated to a single flow. The range is from 1 to 10,000,000.

Command Default

RSVP is disabled by default. If the **ip rsvp bandwidth** command is entered without bandwidth values, a default bandwidth value is assumed for both the *interface-kbps* and *single-flow-kbps* arguments.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

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.

Examples

The following example shows how to enable RSVP for IP on an interface by specifying the bandwidth using Cisco IOS commands.

```
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# ip rsvp bandwidth 100
```

Related Commands

Command	Description
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database for a specified interface.
mpls traffic-eng tunnels	Enables MPLS traffic engineering tunnel signaling on an interface.

Command	Description
tunnel mpls traffic-eng bandwidth	Configures the bandwidth required for a MPLS-TE tunnel.
tp bandwidth	Configures the bandwidth for the MPLS–TP tunnel.

ip rsvp signalling hello graceful-restart neighbor

To enable Resource Reservation Protocol (RSVP) traffic engineering (TE) graceful restart capability on a neighboring router, use the **ip rsvp signalling hello graceful-restart neighbor** command in interface configuration mode. To disable RSVP-TE graceful restart capability, use the **no** form of this command.

ip rsvp signalling hello graceful-restart neighbor *ip-address*

no ip rsvp signalling hello graceful-restart neighbor *ip-address*

Syntax Description

ip-address	IP address of a neighbor on a given interface.

Command Default

No neighboring routers have RSVP-TE graceful restart capability enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use this command to enable support for graceful restart on routers helping their neighbors recover TE tunnels following stateful switchover (SSO).

Note You must issue this command on each interface of the neighboring router that you want to restart.

Examples

The following example shows how to configure RSVP-TE graceful restart on an interface of a neighboring router with the IP address 192.0.2.1.

```
Router# configure terminal
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# ip rsvp signalling hello graceful-restart neighbor 192.0.2.1
```

mpls ip (global configuration)

To configure MPLS hop-by-hop forwarding globally, use the **mpls ip** command in global configuration mode. To disable MPLS hop-by-hop forwarding, use the **no** form of this command.

mpls ip

no mpls ip

Syntax Description

This command has no arguments or keywords.

Command Default

The **mpls ip** command is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Globally enabling MPLS forwarding does not enable it on the interfaces. You must enable MPLS forwarding on the interfaces separately.

MPLS forwarding of packets along normally routed paths (also called dynamic label switching) is enabled by this command. For a given interface to perform dynamic label switching, this switching function must be enabled.

The **no** form of this command stops dynamic label switching for all the interfaces regardless of the interface configuration; it also stops distribution of labels for dynamic label switching. However, the **no** form of this command does not affect the sending of labeled packets through the LSP tunnels.

Examples

The following example shows how to globally configure MPLS hop-by-hop forwarding.

```
Router> enable
Router# configure terminal
Router(config)# mpls ip
```

Related Commands

Command	Description
mpls ip (interface configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for the associated interface.

mpls ip (interface configuration)

To configure MPLS hop-by-hop forwarding on a specific interface, use the **mpls ip** command in interface configuration mode. To disable MPLS hop-by-hop forwarding on a specific interface, use the **no** form of this command.

mpls ip

no mpls ip

Syntax Description

This command has no arguments or keywords.

Command Default

The **mpls ip** command is enabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

MPLS forwarding of IPv4 packets along normally routed paths is also called dynamic label switching. If dynamic label switching has been enabled when this command is issued on an interface, label distribution for the interface begins with the periodic transmission of neighbor discovery Hello messages on the interface. When the outgoing label for a destination routed through the interface is known, packets for the destination are labeled with that outgoing label and forwarded through the interface.

The **no** form of this command causes packets routed out through the interface to be sent unlabeled; this form of the command also terminates label distribution for the interface. However, the **no** form of the command does not affect the sending of labeled packets through any LSP tunnels that might use the interface.

Examples

The following example shows how to configure MPLS hop-by-hop forwarding on the interface.

```
Router> enable
Router# configure terminal
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# mpls ip
```

Related Commands

Command	Description
show mpls interfaces	Displays information about one or more interfaces that have been configured for label switching.

mpls label protocol ldp (global configuration)

To specify the MPLS Label Distribution Protocol (LDP) on all the interfaces, use the **mpls label protocol ldp** command in global configuration mode. To remove the label distribution protocol on all the interfaces, use the **no** form of this command.

mpls label protocol ldp

no mpls label protocol ldp

Syntax Description

This command has no arguments or keywords.

Command Default

LDP is the default label distribution protocol.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following command shows how to establish LDP as the label distribution protocol on all the interfaces.

```
Router(config)# mpls label protocol ldp
```

Related Commands

Command	Description
mpls label protocol ldp (interface configuration)	Specifies LDP for an interface.
show mpls interfaces	Displays information about one or more or all interfaces that are configured for label switching.

mpls label protocol ldp (interface configuration)

To specify the MPLS Label Distribution Protocol (LDP) for an interface, use the **mpls label protocol ldp** command in interface configuration mode. To remove the label distribution protocol from the interface, use the **no** form of this command.

mpls label protocol ldp

no mpls label protocol ldp

Syntax Description

This command has no arguments or keywords.

Command Default

If no protocol is explicitly configured for an interface, the label distribution protocol that was globally configured is used. To set the global label distribution protocol, use the global **mpls label protocol** command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

To successfully establish a session for label distribution for a link connecting two label switch routers (LSRs), the link interfaces on the LSRs must be configured to use the same label distribution protocol. If there are multiple links connecting two LSRs, all of the link interfaces connecting the two LSRs must be configured to use the same protocol.

Examples

The following example shows how to establish LDP as the label distribution protocol for an interface.

```
Router(config-if)# mpls label protocol ldp
```

Related Commands

Command	Description
mpls label protocol ldp (global configuration)	Specifies the LDP on all the interfaces.
show mpls interfaces	Displays information about one or more or all interfaces that are configured for label switching.

mpls ldp autoconfig

To enable MPLS Label Distribution Protocol (LDP) on interfaces for which an OSPF instance has been defined, use the **mpls ldp autoconfig** command in router configuration mode. To disable this configuration, use the **no** form of this command.

mpls ldp autoconfig [**area** *area-id*]

no mpls ldp autoconfig [**area** *area-id*]

Syntax Description

area *area-id*	(Optional) Enables LDP on the interfaces belonging to the specified OSPF area.

Command Default

LDP is not enabled on the interfaces.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

- You can specify this command multiple times to enable LDP on different routing areas with interfaces running OSPF.
- If LDP is disabled globally, the **mpls ldp autoconfig** command fails. LDP must be enabled globally by means of the global **mpls ip** command first.
- If the **mpls ldp autoconfig** command is configured, you cannot issue the global **no mpls ip** command. If you want to disable LDP, you must issue the **no mpls ldp autoconfig** command first.
- The **mpls ldp autoconfig** command is supported only with OSPF interior gateway protocols (IGPs).
- If an OSPF area is not specified, LDP is enabled on all the interfaces belonging to the OSPF process.

Examples

The following example shows how to autoconfigure MPLS LDP for OSPF area 5.

```
Router(config-router)# mpls ldp autoconfig area 5
```

Related Commands

Command	Description
mpls ip (global configuration)	Enables LDP globally.

Command	Description
show mpls interfaces	Displays information about the interfaces configured for LDP.
show mpls ldp discovery	Displays the status of the LDP discovery process.

mpls ldp backoff

To configure parameters for the MPLS label distribution protocol (LDP) backoff mechanism, use the **mpls ldp backoff** command in global configuration mode. To disable this configuration, use the **no** form of this command.

mpls ldp backoff *initial-backoff maximum-backoff*

no mpls ldp backoff *initial-backoff maximum-backoff*

Syntax Description

initial-backoff	Number ranging from 5 to 2147483, inclusive, that defines the initial backoff value in seconds. The default is 15 seconds.
maximum-backoff	Number ranging from 5 to 2147483, inclusive, that defines the maximum backoff value in seconds. The default value is 120 seconds.

Command Default

The LDP backoff mechanism parameters are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The LDP backoff mechanism prevents two incompatibly configured label switch routers (LSRs) from engaging in an unthrottled sequence of session setup failures.

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.

Examples

The following example shows how to set the initial backoff delay to 30 seconds and the maximum backoff delay to 240 seconds.

```
Router(config)# mpls ldp backoff 30 240
```

Related Commands

Command	Description
show mpls ldp backoff	Displays information about the configured session setup backoff parameters and any potential LDP peers with which session setup attempts are being throttled.

mpls ldp explicit-null

To enable the router to advertise an MPLS LDP Explicit Null label in situations where it would normally advertise an Implicit Null label, use the **mpls ldp explicit-null** command in global configuration mode. To disable this configuration, use the **no** form of this command.

mpls ldp explicit-null [**for** *prefix-acl* | **to** *peer-acl*]

no mpls ldp explicit-null

Syntax Description

for *prefix-acl*	(Optional) Specifies prefixes for which Explicit Null must be advertised in place of Implicit Null.
to *peer-acl*	(Optional) Specifies LDP peers to which Explicit Null must be advertised in place of Implicit Null.

Command Default

Explicit Null labels are not advertised.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Normally, LDP advertises an Implicit Null label for directly connected routes. The Implicit Null label causes the previous hop (penultimate) router to do penultimate hop popping. In certain cases, it is desirable to prevent the penultimate router from performing penultimate hop popping and to force it to replace the incoming label with the Explicit Null label.

When you issue the **mpls ldp explicit-null** command, Explicit Null is advertised in place of Implicit Null for directly connected prefixes permitted by the *prefix-acl* argument to peers permitted by the *peer-acl* argument.

If you do not specify the *prefix-acl* argument in the command, Explicit Null is advertised in place of Implicit Null for all directly connected prefixes.

If you do not specify the *peer-acl* argument in the command, Explicit Null is advertised in place of Implicit Null to all the peers.

Examples

The following command shows how to enable the Explicit Null label for all directly connected routes to all the LDP peers.

```
Router(config)# mpls ldp explicit-null
```

mpls ldp graceful-restart

To enable MPLS LDP graceful restart, use the **mpls ldp graceful-restart** command in global configuration mode. To disable LDP graceful restart, use the **no** form of this command.

mpls ldp graceful-restart

no mpls ldp graceful-restart

Syntax Description

This command has no arguments or keywords.

Command Default

MPLS LDP graceful restart is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

MPLS LDP graceful restart must be enabled before an LDP session is established. Use the **no** form of the command to disable the graceful restart on all the LDP sessions.

Examples

The following example shows how to enable LDP graceful restart.

```
Router(config)# mpls ldp graceful-restart
```

Related Commands

Command	Description
mpls ldp graceful-restart timers forwarding-holding	Specifies the amount of time the MPLS LDP forwarding state must be preserved after the control plane restarts.
mpls ldp graceful-restart timers max-recovery	Specifies the amount of time a router should hold stale label-FEC bindings after an MPLS LDP session has been reestablished.
mpls ldp graceful-restart timers neighbor-liveness	Specifies the amount of time a router should wait for an MPLS LDP session to be reestablished.

mpls ldp graceful-restart timers forwarding-holding

To specify the amount of time the MPLS forwarding state must be preserved after the control plane restarts, use the **mpls ldp graceful-restart timers forwarding-holding** command in global configuration mode. To revert to the default timer value, use the **no** form of this command.

mpls ldp graceful-restart timers forwarding-holding *secs*

no mpls ldp graceful-restart timers forwarding-holding

Syntax Description

secs	Amount of time (in seconds) that the MPLS forwarding state must be preserved after the control plane restarts. The default value is 600 seconds. The acceptable range of values is 30 to 600 seconds.

Command Default

The MPLS forwarding state is preserved for 600 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

If the timer expires, all the entries that are marked stale are deleted.

Examples

The following example shows how to specify the MPLS forwarding state to be preserved for 300 seconds.

```
Router(config)# mpls ldp graceful-restart timers forwarding-holding 300
```

Related Commands

Command	Description
mpls ldp graceful-restart	Enables MPLS LDP graceful restart.
mpls ldp graceful-restart timers max-recovery	Specifies the amount of time a router must hold stale label-FEC bindings after an MPLS LDP session has been reestablished.
mpls ldp graceful-restart timers neighbor-liveness	Specifies the amount of time a router must wait for an MPLS LDP session to be reestablished.

mpls ldp graceful-restart timers max-recovery

To specify the amount of time a router should hold stale label-Forwarding Equivalence Class (FEC) bindings after an MPLS LDP session has been reestablished, use the **mpls ldp graceful-restart timers max-recovery** command in global configuration mode. To revert to the default timer value, use the **no** form of this command.

mpls ldp graceful-restart timers max-recovery *secs*

no mpls ldp graceful-restart timers max-recovery *secs*

Syntax Description

secs	Amount of time (in seconds) that the router should hold stale label-FEC bindings after an LDP session has been reestablished. The default value is 120 seconds. The acceptable range of values is 15 to 600 seconds.

Command Default

Stale label-FEC bindings are held for 120 seconds after an LDP session has been reestablished.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

After the timer expires, all stale label-FEC bindings learned from the associated LDP session are removed, which results in the removal of any forwarding table entries that are based on those bindings.

Examples

The following example shows how to specify that the router must hold stale label-FEC bindings after an LDP session has been reestablished for 180 seconds.

```
Router(config)# mpls ldp graceful-restart timers max-recovery 180
```

Related Commands

Command	Description
mpls ldp graceful-restart	Enables MPLS LDP graceful restart.
mpls ldp graceful-restart timers forwarding-holding	Specifies the amount of time the MPLS LDP forwarding state should be preserved.
mpls ldp graceful-restart timers neighbor-liveness	Specifies the amount of time a router should wait for an MPLS LDP session to be reestablished.

mpls ldp graceful-restart timers neighbor-liveness

To specify the upper bound on the amount of time a router must wait for an MPLS LDP session to be reestablished, use the **mpls ldp graceful-restart timers neighbor-liveness** command in global configuration mode. To revert to the default timer value, use the **no** form of this command.

mpls ldp graceful-restart timers neighbor-liveness *secs*

no mpls ldp graceful-restart timers neighbor-liveness

Syntax Description

secs	Amount of time (in seconds) that the router must wait for an LDP session to be reestablished. The default value is 120 seconds. The range is from 5 to 300 seconds.

Command Default

The default value is 120 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The amount of time a router waits for an LDP session to be reestablished is the lesser of the following values:

- The value of the fault tolerant (FT) type length value (TLV) reconnect timeout of the peer.
- The value of the neighbor liveness timer.

If the router cannot reestablish an MPLS LDP session with the neighbor in the allotted time, the router deletes the stale label-FEC bindings received from that neighbor.

Examples

The following example shows how to set the amount of time that the router must wait for an MPLS LDP session to be reestablished to 30 seconds.

```
Router(config)# mpls ldp graceful-restart timers neighbor-liveness 30
```

Related Commands

Command	Description
mpls ldp graceful-restart	Enables MPLS LDP graceful restart.

Command	Description
mpls ldp graceful-restart timers forwarding-holding	Specifies the amount of time the MPLS LDP forwarding state must be preserved after the control plane restarts.
mpls ldp graceful-restart timers max-recovery	Specifies the amount of time a router must hold stale label-FEC bindings after an MPLS LDP session has been reestablished.

mpls ldp igp sync

To enable MPLS LDP-Interior Gateway Protocol (IGP) synchronization on an interface that belongs to an OSPF process, use the **mpls ldp igp sync** command in interface configuration mode. To disable MPLS LDP-IGP synchronization, use the **no** form of the command.

mpls ldp igp sync [**delay** *seconds*]

no mpls ldp igp sync [**delay**]

Syntax Description

delay *seconds*	(Optional) Sets a delay timer for MPLS LDP-IGP synchronization. The range is from 5 to 60 seconds.

Command Default

MPLS LDP-IGP synchronization is enabled by default on all the interfaces configured for the process. A delay timer is not set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command works with the **mpls ldp sync** command, which enables MPLS LDP-IGP synchronization on all the interfaces that belong to an OSPF process. To disable MPLS LDP-IGP synchronization on a selected interface, use the **no mpls ldp igp sync** command in the configuration for that interface.

Use the **mpls ldp igp sync delay** *seconds* command to configure a delay time for MPLS LDP and IGP synchronization on an interface-by-interface basis. To remove the delay timer from a specified interface, use the **no mpls ldp igp sync delay** command. This command sets the delay time to 0 seconds, but leaves MPLS LDP-IGP synchronization enabled.

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 that synchronization is still valid and notifies the OSPF process.
- If the delay time is not configured, synchronization is disabled or down, or an interface is removed from an IGP process, LDP stops the timer and immediately notifies the OSPF process.

Examples

The following example shows how to set a delay timer of 45 seconds for MPLS LDP-IGP synchronization on an interface.

```
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# mpls ldp igp sync delay 45
```

Related Commands

Command	Description
mpls ldp sync	Enables MPLS LDP-IGP synchronization on interfaces for an OSPF process.
show mpls ldp igp sync	Displays the status of the MPLS LDP-IGP synchronization process.

mpls ldp igp sync holddown

To specify how long an Interior Gateway Protocol (IGP) must wait for an MPLS LDP synchronization to be achieved, use the **mpls ldp igp sync holddown** command in global configuration mode. To disable the hold-down timer, use the **no** form of this command.

mpls ldp igp sync holddown *milliseconds*

no mpls ldp igp sync holddown

Syntax Description

milliseconds	Number of milliseconds an IGP must wait for an LDP session to be established. The valid range of values is from 1 to 2147483647 milliseconds.

Command Default

An IGP will wait indefinitely for LDP synchronization to be achieved.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command enables you to limit the amount of time an IGP waits for LDP synchronization to be achieved.

Examples

The following example shows how to configure the IGP to wait 10,000 milliseconds (10 seconds) for LDP synchronization.

```
Router(config)# mpls ldp igp sync holddown 10000
```

Related Commands

Command	Description
mpls ldp sync	Enables MPLS LDP-IGP synchronization on interfaces for an OSPF process.
show mpls ldp igp sync	Displays the status of the MPLS LDP-IGP synchronization process.

mpls ldp neighbor targeted

To set up a targeted session with a specified MPLS LDP neighbor, use the **mpls ldp neighbor targeted** command in global configuration mode. To disable a targeted session, use the **no** form of this command.

mpls ldp neighbor *ip-addr* **targeted ldp**

no mpls ldp neighbor *ip-addr* **targeted ldp**

Syntax Description

ip-addr	Router ID (IP address) that identifies a neighbor.
targeted ldp	Specifies Label Distribution Protocol (LDP) as the label protocol for the targeted session.

Command Default

A targeted session with a specified neighbor is not set up.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use the **mpls ldp neighbor targeted** command when you need to set up a targeted session and other means of establishing targeted sessions do not apply, such as configuring **mpls ip** on a traffic engineering (TE) tunnel. For example, you would use this command to set up a targeted session between directly connected MPLS label switch routers (LSRs) when MPLS label forwarding convergence time is an issue.

The **mpls ldp neighbor targeted** command can improve label convergence time for directly connected neighbor LSRs when the links directly connecting them are down. When the links between the neighbor LSRs are up, both the link and targeted Hellos maintain the LDP session. If the links between the neighbor LSRs go down, the targeted Hellos maintain the session, allowing the LSRs to retain labels learned from each other. When a link directly connecting the LSRs comes back up, the LSRs can immediately reinstall labels for forwarding use without having to reestablish their LDP session and exchange labels.

For the **no** form of the command, if the **targeted** keyword is not specified, all the configuration information for the specified neighbor reverts to the defaults and the neighbor record is deleted.

Examples

The following example shows how to set a targeted session with the neighbor 192.0.2.1.

```
Router(config)# mpls ldp neighbor 192.0.2.1 targeted ldp
```

Related Commands

Command	Description
show mpls ldp neighbor	Displays the status of Label Distribution Protocol (LDP) sessions.

mpls ldp router-id

To specify a preferred interface for the Label Distribution Protocol (LDP) router ID, use the **mpls ldp router-id** command in global configuration mode. To disable the interface from being used as the LDP router ID, use the **no** form of this command.

mpls ldp router-id *interface* **[force]**

no mpls ldp router-id *interface* **[force]**

Syntax Description

interface	Interface specified to be used as the MPLS LDP router ID, provided that the interface is operational.
force	(Optional) Alters the behavior of the **mpls ldp router-id** command, as described in the "Usage Guidelines" section.

Command Default

If the **mpls ldp router-id** command is not used, the router examines the IP addresses of all the operational interfaces. If these IP addresses include loopback interface addresses, the router selects the largest loopback address as the LDP router ID. Otherwise, the router selects the largest IP address pertaining to an operational interface as the LDP router ID.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

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.

Examples

The following example shows how to assign 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
```

Related Commands

Command	Description
show mpls ldp discovery	Displays the status of the LDP discovery process.

mpls ldp session protection

To enable MPLS LDP autoconfiguration for existing or new LDP sessions, use the **mpls ldp session protection** command in global configuration mode. To disable this configuration, use the **no** form of this command.

mpls ldp session protection [**for** *acl*] [**duration** {**infinite** | *seconds*}]

no mpls ldp session protection [**for** *acl*] [**duration** {**infinite** | *seconds*}]

Syntax Description

for *acl*	(Optional) Specifies a standard IP access control list that contains the prefixes that are to be protected.
duration	(Optional) Specifies the time that the LDP targeted hello adjacency must be retained after a link is lost. **Note** If you use this keyword, you must select either the **infinite** keyword or the *seconds* argument.
infinite	Specifies that the LDP targeted hello adjacency must be retained infinitely after a link is lost.
seconds	Time in seconds that the LDP targeted hello adjacency must be retained after a link is lost. The valid range of values is from 30 to 2,147,483 seconds.

Command Default

MPLS LDP session protection is not established.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

If you issue the **mpls ldp session protection** command without the **duration** keyword, then session protection is enabled for 86400 seconds (24 hours) meaning that the LDP targeted hello adjacency is retained for 24 hours after a link is lost. This is the default timeout.

If you issue the **mpls ldp session protection duration infinite** command, then session protection is enabled infinitely, which implies that the LDP targeted hello adjacency is retained infinitely after a link is lost.

If you issue the **mpls ldp session protection duration** *seconds* command, then session protection is enabled for the number of seconds indicated, which implies that the LDP targeted hello adjacency is retained for that amount of time. For example, if you issued **mpls ldp session protection duration 100**, then the LDP targeted hello adjacency is retained for 100 seconds after a link is lost.

Examples

The following example shows how to enable MPLS LDP autoconfiguration for LDP sessions for peers whose router IDs are listed in access control list *rtr4*.

```
Router(config)# mpls ldp session protection for rtr4
```

Related Commands

Command	Description
show mpls ldp neighbor	Displays the contents of the LDP.

mpls ldp sync

To enable MPLS LDP-Interior Gateway Protocol (IGP) synchronization on interfaces for an OSPF process, use the **mpls ldp sync** command in router configuration mode. To disable this synchronization, use the **no** form of this command.

mpls ldp sync

no mpls ldp sync

Syntax Description

This command has no arguments or keywords.

Command Default

MPLS LDP-IGP synchronization is not enabled on interfaces belonging to the OSPF process.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

If the **mpls ldp sync** command is configured, you cannot enter the global **no mpls ip** command. If you want to disable LDP synchronization, you must enter the **no mpls ldp igp sync** command first.

The **mpls ldp sync** command is supported with OSPF process.

Examples

The following example shows how to enable MPLS LDP-IGP synchronization for an OSPF process.

```
Router(config-router)# mpls ldp sync
```

Related Commands

Command	Description
mpls ldp igp sync	Enables MPLS LDP-IGP synchronization on an interface that belongs to an OSPF process.
no mpls ip	Disables MPLS hop-by-hop forwarding.
show mpls ldp igp sync	Displays the status of the MPLS LDP-IGP synchronization process.

mpls traffic-eng area

To configure a router running OSPF MPLS so that it floods traffic engineering for the indicated OSPF area, use the **mpls traffic-eng area** command in router configuration mode. To disable flooding of traffic engineering for the indicated OSPF area, use the **no** form of this command.

mpls traffic-eng area *number*

no mpls traffic-eng area *number*

Syntax Description

number	The OSPF area on which MPLS traffic engineering is enabled.

Command Default

Flooding is disabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command is in the routing protocol configuration tree and is supported for OSPF. The command affects the operation of MPLS traffic engineering only if MPLS traffic engineering is enabled for that routing protocol instance.

Examples

The following example shows how to configure a router running OSPF MPLS to flood traffic engineering for OSPF 0.

```
Router(config-router)# mpls traffic-eng area 0
```

Related Commands

Command	Description
mpls traffic-eng router-id	Specifies that the TE router identifier for the node is the IP address associated with a given interface.
router ospf	Configures an OSPF routing process on a router.
network area	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

mpls traffic-eng link-management timers periodic-flooding

To set the length of the interval for periodic flooding, use the **mpls traffic-eng link-management timers periodic-flooding** command in global configuration mode. To disable the specified interval length for periodic flooding, use the **no** form of this command.

mpls traffic-eng link-management timers periodic-flooding *interval*

no mpls traffic-eng link-management timers periodic-flooding

Syntax Description

interval	Length of the interval (in seconds) for periodic flooding. Valid values are from 0 to 3600. A value of 0 turns off periodic flooding. If you set this value from 1 to 29, it is treated as 30.

Command Default

180 seconds (3 minutes)

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use this command to advertise link state information changes that do not trigger immediate action. For example, a change to the amount of allocated bandwidth that does not cross a threshold.

Examples

The following example shows how to set the interval length for periodic flooding to 120 seconds:

```
Router(config)# mpls traffic-eng link-management timers periodic-flooding 120
```

Related Commands

Command	Description
mpls traffic-eng area *number*	Enables MPLS TE for the indicated OSPF area.

mpls traffic-eng lsp attributes

To create or modify a label switched path (LSP) attribute list, use the **mpls traffic-eng lsp attributes** command in global configuration mode. To remove a specified LSP attribute list from the device configuration, use the **no** form of this command.

mpls traffic-eng lsp attributes *string*

no mpls traffic-eng lsp attributes *string*

Syntax Description

string	Identifies a specific LSP attribute list.

Command Default

An LSP attribute list is not created unless you create one.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command sets up an LSP attribute list and enters LSP Attributes configuration mode, in which you can enter LSP attributes.

To associate the LSP attributes and LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

An LSP attribute referenced by the path option takes precedence over the values configured on the tunnel interface. If an attribute is not specified in the LSP attribute list, the devices takes the attribute from the tunnel configuration. LSP attribute lists do not have default values. If the attribute is not configured on the tunnel, then the device uses tunnel default values.

Once you type the **mpls traffic-eng lsp attributes** command, you enter the LSP Attributes configuration mode where you define the attributes for the LSP attribute list that you are creating.

The mode commands are as follows:

- **affinity**—Specifies attribute flags for links that make up an LSP.
- **auto-bw**—Specifies automatic bandwidth configuration.
- **bandwidth**—Specifies LSP bandwidth.
- **lockdown**—Disables reoptimization for the LSP.
- **priority**—Specifies LSP priority.
- **protection**—Enables failure protection.

- **record-route**—Records the route used by the LSP.

The following monitoring and management commands are also available in the LSP Attributes configuration mode:

- **exit**—Exits from LSP Attributes configuration mode.
- **list**—Relists all the entries in the LSP attribute list.
- **no**—Removes a specific attribute from the LSP attribute list.

Examples

The following example shows how to set up an LSP attribute list identified with the numeral 6 with the **bandwidth** and **priority** mode commands. The example also shows how to use the **list** mode command:

```
Router(config)# mpls traffic-eng lsp attributes 6
Router(config-lsp-attr)# bandwidth 500
Router(config-lsp-attr)# list
LIST 6
bandwidth 500
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# list
LIST 6
bandwidth 500
priority 1 1
Router(config-lsp-attr)# exit
```

Related Commands

Command	Description
show mpls traffic-eng lsp attributes	Displays global LSP attributes lists.

mpls traffic-eng router-id

To specify that the traffic engineering router identifier for the node is the IP address associated with a given interface, use the **mpls traffic-eng router-id** command in router configuration mode. To remove the traffic engineering router identifier, use the **no** form of this command.

mpls traffic-eng router-id *interface-name*

no mpls traffic-eng router-id

Syntax Description

interface-name	Interface whose primary IP address is the router's identifier.

Command Default

No traffic engineering router identifier is specified.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This router identifier acts as a stable IP address for the traffic engineering configuration. This IP address is flooded to all the nodes. For all traffic engineering tunnels originating at other nodes and ending at this node, you must set the tunnel destination to the traffic engineering router identifier of the destination node, because that is the address that the traffic engineering topology database at the tunnel head uses for its path calculation.

You should configure the same traffic engineering router id for all the IGP routing processes.

Examples

The following example shows how to specify the traffic engineering router identifier as the IP address associated with interface Loopback0:

```
Router(config-router)# mpls traffic-eng router-id Loopback0
```

Related Commands

Command	Description
mpls traffic-eng area *number*	Enables MPLS TE for the indicated OSPF area.

mpls traffic-eng tunnels (global configuration)

To enable MPLS traffic engineering tunnel signaling on a device, use the **mpls traffic-eng tunnels** command in global configuration mode. To disable MPLS traffic engineering tunnel signaling, use the **no** form of this command.

mpls traffic-eng tunnels

no mpls traffic-eng tunnels

Syntax Description

This command has no arguments or keywords.

Command Default

The command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command enables MPLS traffic engineering on a device. For you to use the feature, MPLS traffic engineering must also be enabled on the desired interfaces.

Examples

The following example shows how to enable MPLS traffic engineering tunnel signaling.

```
Router(config)# mpls traffic-eng tunnels
```

Related Commands

Command	Description
show mpls traffic-eng tunnels	Displays information about tunnels.

mpls traffic-eng tunnels (interface configuration)

To enable MPLS traffic engineering tunnel signaling on an interface (assuming that it is enabled on the device), use the **mpls traffic-eng tunnels** command in interface configuration mode. To disable MPLS traffic engineering tunnel signaling on the interface, use the **no** form of this command.

mpls traffic-eng tunnels

no mpls traffic-eng tunnels

Syntax Description

This command has no arguments or keywords.

Command Default

The MPLS TE is disabled on all the interfaces.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Before you enable MPLS TE on the interface, you must enable MPLS TE on the device. An enabled interface has its resource information flooded into the appropriate IGP link-state database and accepts traffic engineering tunnel signaling requests.

You can use this command to enable MPLS traffic engineering on an interface, thereby eliminating the need to use the **ip rsvp bandwidth** command. However, if your configuration includes Call Admission Control (CAC) for IPv4 Resource Reservation Protocol (RSVP) flows, you must use the **ip rsvp bandwidth** command.

Examples

The following example shows how to enable MPLS traffic engineering tunnel signaling on an interface.

```
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# mpls traffic-eng tunnels
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
mpls traffic-eng tunnels (global configuration)	Enables MPLS traffic engineering tunnel signaling on a device.

mpls traffic-eng path-option list

To configure a path option list, use the **mpls traffic-eng path-option list** command in global configuration mode. To disable this function, use the **no** form of this command.

mpls traffic-eng path-option list [**name** *pathlist-name* | **identifier** *pathlist-number*

no mpls traffic-eng path-option list [**name** *pathlist-name* | **identifier** *pathlist-number*

Syntax Description

name *pathlist-name*	Specifies the name of the path option list.
identifier *pathlist-number*	Specifies the identification number of the path option list. Valid values are from 1 through 65535.

Command Default

There are no path option lists.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

A path option list contains a list of backup paths for a primary path option. You can specify a path option list by entering its name or identifier.

After you enter the **mpls traffic-eng path-option list** command, the router enters path option list configuration mode and you can enter the following commands:

- **path-option**—Specifies the name or identification number of the next path option to add, edit, or delete.
- **list**—Lists all path options.
- **no**—Deletes a specified path option.
- **exit**—Exits from path option list configuration mode.

Then you can specify explicit backup paths by entering their name or identifier.

Examples

The following example configures the path option list named pathlist-01, adds path option 10, lists the backup path that is in the path option list, and exits from path option list configuration mode.

```
Router(config)# mpls traffic-eng path-option list name pathlist-01
Router(cfg-pathoption-list)# path-option 10 explicit name bk-path-01
Router(cfg-pathoption-list)# list
```

```
path-option 10 explicit name bk-path-01
Router(cfg-pathoption-list)# exit
```

Related Commands

Command	Description
tunnel mpls traffic-eng path option	Configures a path option for an MPLS TE tunnel.
tunnel mpls traffic-eng path-option protect	Configures a secondary path option or a path option list for an MPLS TE tunnel.

next-address

To specify the next IP address in the explicit path, use the **next-address** command in IP explicit path configuration mode.

next-address [**loose** | **strict**] *ip-address*

Syntax Description

loose	(Optional) Specifies that the previous address (if any) in the explicit path need not be directly connected to the next IP address, and that the router is free to determine the path from the previous address (if any) to the next IP address.
strict	(Optional) Specifies that the previous address (if any) in the explicit path must be directly connected to the next IP address.
ip-address	Next IP address in the explicit path.

Command Default

The next IP address in the explicit path is not specified.

Command Modes

IP explicit path configuration (cfg-ip-expl-path)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

To specify an explicit path that includes only the addresses specified, specify each address in sequence by using the **next-address** command without the **loose** keyword.

To use explicit paths for TE tunnels within an IGP area, you can specify a combination of both loose and strict hops. When specifying an explicit path for an MPLS TE tunnel, you can specify link or node addresses of the next-hop routers in an explicit path.

When specifying an explicit path, if you specify the “forward” address (the address of the interface that forwards the traffic to the next router) as the next-hop address, the explicit path might not be used. Using the forward address allows that entry to be treated as a loose hop for path calculation. Cisco recommends that you use the “receive”address (the address of the interface that receives traffic from the sending router) as the next-hop address.

Examples

The following example shows how to assign the number 60 to the IP explicit path, enable the path, and specify 10.3.27.3 as the next IP address in the list of IP addresses.

```
Router(config)# ip explicit-path identifier 60 enable
Router(cfg-ip-expl-path)# next-address 10.3.27.3
```

```
Explicit Path identifier 60:
    1: next-address 10.3.27.3
```

Related Commands

Command	Description
index	Inserts or modifies a path entry at a specified index.
ip explicit-path	Enters the subcommand mode for IP explicit paths and creates or modifies the specified path.
show ip explicit-paths	Displays the configured IP explicit paths.

ping mpls

To check MPLS label switched path (LSP) connectivity, use the **ping mpls** command in privileged EXEC mode.

ping mpls {*ipv4 destination-address*/*destination-mask-length* [**destination** *address-start address-end increment*] [**ttl** *time-to-live*] | **pseudowire** *ipv4-address vc-id* [**segment** [*segment-number*]] [**destination** *address-start address-end increment*] | **traffic-eng** *tunnel-interface tunnel-number* [**ttl** *time-to-live*]}

[**revision** {**1** | **2** | **3** | **4**}]

[**source** *source-address*]

[**repeat** *count*]

[**timeout** *seconds*]

[**size** *packet-size* | **sweep** *minimum maximum size-increment*]

[**pad** *pattern*]

[**reply dscp** *dscp-value*]

[**reply pad-tlv**]

[**reply mode** {**ipv4** | **router-alert**}]

[**interval** *ms*]

[**exp** *exp-bits*]

[**verbose**]

[**revision** *tlv-revision-number*]

[**force-explicit-null**]

[**output interface** *tx-interface* [**nexthop** *ip-address*]]

[**dsmap** [**hashkey** {**none** | **ipv4 bitmap** *bitmap-size*}]]

[**flags fec**]

Syntax Description

ipv4	Specifies the destination type as a LDP IPv4 address.
destination-address	Address prefix of the target to be tested.
/destination-mask-length	Number of bits in the network mask of the target address. The slash is required.
destination	(Optional) Specifies a network 127 address.
address-start	(Optional) Beginning network 127 address.
address-end	(Optional) Ending network 127 address.
increment	(Optional) Number by which to increment the network 127 address.
ttl *time-to-live*	(Optional) Specifies a time-to-live (TTL) value. The default is 225 seconds.

pseudowire	Specifies the destination type as an Any Transport over MPLS (AToM) virtual circuit (VC).
ipv4-address	IPv4 address of the AToM VC to be tested.
vc-id	Specifies the VC identifier of the AToM VC to be tested.
segment *segment-number*	(Optional) Specifies a segment of a multisegment pseudowire.
traffic-eng	Specifies the destination type as an MPLS-TE tunnel.
tunnel-interface	Tunnel interface to be tested.
tunnel-number	Tunnel interface number.
revision {**1** | **2** | **3** | **4**	(Optional) Selects the type, length, values (TLVs) version.
source *source-address*	(Optional) Specifies the source address or name. The default address is loopback0. This address is used as the destination address in the MPLS echo response.
repeat *count*	(Optional) Specifies the number of times to resend the same packet. The range is from 1 to 2147483647. The default is 1.
timeout *seconds*	(Optional) Specifies the timeout interval in seconds for an MPLS request packet. The range is from 0 to 3600. The default is 2 seconds.
size *packet-size*	(Optional) Specifies the size of the packet with the label stack imposed. Packet size is the number of bytes in each ping. The range is from 40 to 18024. The default is 100.
sweep	(Optional) Enables you to send a number of packets of different sizes, ranging from a start size to an end size.
minimum	(Optional) Minimum or start size for an MPLS echo packet. The lower boundary of the **sweep** range varies depending on the LSP type. The default is 100 bytes.
maximum	(Optional) Maximum or end size for an echo packet. The default is 17,986 bytes.
size-increment	(Optional) Number by which to increment the echo packet size. The default is 100 bytes.
pad *pattern*	(Optional) The pad TLV used to fill the datagram so that the MPLS echo request is the specified size. The default is 0xABCD.
reply dscp *dscp-value*	(Optional) Provides the capability to request a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value.
reply pad-tlv	(Optional) Tests the ability of the sender of an echo reply to support the copy pad TLV to echo reply.
reply mode {ipv4 | router-alert}	(Optional) Specifies the reply mode for the echo request packet. **ipv4**—Reply with an IPv4 UDP packet (default). **router-alert**—Reply with an IPv4 UDP packet with router alert.

interval *ms*	(Optional) Specifies the time, in milliseconds (ms), between successive MPLS echo requests. This parameter allows you to pace the transmission of packets so that the receiving router does not drop packets. Default is 0.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for an MPLS echo reply. Valid values are from 0 to 7. Default is 0.
verbose	(Optional) Displays the MPLS echo reply sender address of the packet and displays return codes.
revision *tlv-revision-number*	(Optional) Cisco TLV revision number.
force-explicit-null	(Optional) Forces an explicit null label to be added to the MPLS label stack even though the label was unsolicited.
output interface *tx-interface*	(Optional) Specifies the output interface for echo requests.
nexthop *ip-address*	(Optional) Causes packets to go through the specified next-hop address.
dsmap	(Optional) Interrogates a transit router for downstream mapping information.
hashkey {**none** | **ipv4 bitmap** *bitmap-size*	(Optional) Allows you to control the hash key and multipath settings. Valid values are: **none**—There is no multipath (type 0). **ipv4 bitmap** *bitmap-size*—Size of the IPv4 addresses (type 8) bitmap. If you enter the **none** keyword, multipath LSP traceroute acts like an enhanced LSP traceroute; that is, it uses multipath LSP traceroute retry logic and consistency checking.
flags fec	(Optional) Allows Forward Equivalence Class (FEC) checking on the transit router. A downstream map TLV containing the correct received labels must be present in the echo request for target FEC stack checking to be performed. Target FEC stack validation is always done at the egress router. Ensure to use this keyword in conjunction with the **ttl** keyword.

Command Default

You cannot check MPLS LSP connectivity.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command is introduced.

Usage Guidelines

Use the **ping mpls** command to validate, test, or troubleshoot IPv4 LDP LSPs, IPv4 RSVP TE tunnels, and AToM VCs.

The following keywords are not available with the **ping mpls pseudowire** command:

- **dsmap**
- **flags**
- **force-explicit-null**
- **output**
- **revision**
- **ttl**

Examples

The following example shows how to use the **ping mpls** command to test connectivity of an IPv4 LDP LSP.

```
Router# ping mpls ipv4 10.131.191.252/32 repeat 5 exp 5 verbose
```

```
Sending 5, 100-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:
Codes:
'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
! 10.131.191.230, return code 3
! 10.131.191.230, return code 3
! 10.131.191.230, return code 3
! 10.131.191.230, return code 3
! 10.131.191.230, return code 3
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/102/112
ms
```

Related Commands

Command	Description
trace mpls	Discovers MPLS LSP routes that packets will actually take when traveling to their destinations.

priority

To specify the LSP priority in an LSP attribute list, use the **priority** command in LSP Attributes configuration mode. To remove the specified priority, use the **no** form of this command.

priority *setup-priority* [*hold-priority*]

no priority

Syntax Description

setup-priority	Priority used when signaling an LSP to determine which existing LSPs can be preempted. 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.
hold-priority	(Optional) Priority associated with an LSP to determine if it should be preempted by other LSPs that are being signaled. Valid values are from 0 to 7, where a lower number indicates a higher priority.

Command Default

No priority is set in the attribute list.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use this command to configure setup and hold priority for an LSP in an LSP attribute list. Setup priority and hold priority are typically configured to be equal, and setup priority cannot be better (numerically smaller) than the hold priority.

To associate the LSP priority attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example shows how to set the LSP hold and setup property.

```
Router(config-lsp-attr)# priority 2 2
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.

Command	Description
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

record-route

To record the route used by the LSP, use the **record-route** command in LSP Attributes configuration mode. To stop the recording the route used by the LSP, use the **no** form of this command.

record-route

no record-route

Syntax Description

This command has no arguments or keywords.

Command Default

The LSP route is not recorded.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use this command to set up the recording of the route taken by the LSP in an LSP attribute list.

To associate the LSP record-route attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where **string** is the identifier for the specific LSP attribute list.

Examples

The following example shows how to set up LSP route recording in an LSP attribute list.

```
Router(config-lsp-attr)# record-route
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

show ip explicit-paths

To display the configured IP explicit paths, use the **show ip explicit-paths** command in user EXEC or privileged EXEC mode.

show ip explicit-paths [**name** *pathname* | **identifier** *number*] [**detail]**

Syntax Description

name *pathname*	(Optional) Displays the pathname of the explicit path.
identifier *number*	(Optional) Displays the number of the explicit path. Valid values are from 1 to 65535.
detail	(Optional) Displays, in the long form, information about the configured IP explicit paths.

Command Default

If you enter the command without entering an optional keyword, all configured IP explicit paths are displayed.

Command Modes

User EXEC (>) and Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path.

Examples

The following is sample output from the **show ip explicit-paths** command.

```
Router# show ip explicit-paths
```

```
PATH 200 (strict source route, path complete, generation 6)
     1: next-address 10.3.28.3
     2: next-address 10.3.27.3
```

Related Commands

Command	Description
index	Inserts or modifies a path entry at a specific index.
ip explicit-path	Enters the subcommand mode for IP explicit paths so that you can create or modify the named path.

Command	Description
next-address	Specifies the next IP address in the explicit path.

show ip rsvp sender

To display Resource Reservation Protocol (RSVP) PATH-related sender information currently in the database, use the **show ip rsvp sender** command in user EXEC or privileged EXEC mode.

show ip rsvp sender [**detail**] [**filter** [**session-type all**]]

Syntax Description

detail	(Optional) Specifies additional sender information.
filter	(Optional) Specifies a subset of the senders to display.
session-type	(Optional) Specifies the type of RSVP sessions to display.
all	(Optional) Specifies all the types of RSVP sessions.

Command Modes

User EXEC (>) and Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use the **show ip rsvp sender** command to display the RSVP sender (PATH) information currently in the database for a specified interface or for all the interfaces.

Examples

The following is sample output from the **show ip rsvp sender** command.

```
Router# show ip rsvp sender
```

```
  To            From     Pro DPort Sport Prev Hop    I/F           BPS
172.16.1.49 172.16.4.53 1   0     0  172.16.3.53 TenGEthernet4/1 80K
172.16.2.51 172.16.5.54 1   0     0  172.16.3.54 TenGEthernet4/2 80K
```

show mpls ldp backoff

To display information about the configured session setup backoff parameters and any potential LDP peers with which session setup attempts are being throttled, use the **show mpls ldp backoff** command in user EXEC or privileged EXEC mode.

show mpls ldp backoff [all]

Syntax Description

all	(Optional) Displays LDP discovery information for all VPNs.

Command Modes

User EXEC and Privileged EXEC

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following is sample output from the **show mpls ldp backoff** command.

```
Router# show mpls ldp backoff
```

```
LDP initial/maximum backoff: 30/240 sec
Backoff table: 2 entries
LDP Id         Backoff(sec)     Waiting(sec)
10.144.0.44:0    60               30
10.155.0.55:0    120              90
```

Related Commands

Command	Description
mpls ldp backoff	Configures session setup delay parameters for the LDP backoff mechanism.

show mpls traffic-eng lsp attributes

To display global LSP attribute lists, use the **show mpls traffic-eng lsp attributes** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng lsp attributes [**name** *string*] [**internal**]

Syntax Description

name	(Optional) Identifies a specific LSP attribute list.
string	Describes the string argument.
internal	(Optional) Displays LSP attribute list internal information.

Command Default

If no keywords or arguments are specified, all LSP attribute lists are displayed.

Command Modes

User EXEC (>) and Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use this command to display information about all LSP attribute lists or a specific LSP attribute list.

Examples

The following example shows output from the **show mpls traffic-eng lsp attributes** command.

```
Router# show mpls traffic-eng lsp attributes
```

```
LIST list1
    affinity 0xFF mask 0xFFFFFFFF
    auto-bw collect-bw
    bandwidth 12
    lockdown
    priority 2 2
    record-route LIST 2
    bandwidth 5000
LIST hipriority
    priority 0 0
!
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies a LSP attribute list.

show mpls traffic-eng tunnels

To display information about tunnels, use the **show mpls traffic-eng tunnels** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng tunnels [[**attributes** *list-name*] [**destination** *address*] [**down**] [**interface** *type number*] [**name** *name*] [**name-regexp** *reg-exp*] [**role** {**all** | **head** | **middle** | **remote** | **tail**}] [**source-id** {*ipaddress* [*tunnel-id*]}] [**suboptimal constraints** {**current** | **max** | **none**}] [**up**]] [**accounting** | **brief** | **protection**]

Syntax Description

attributes *list-name*	(Optional) Restricts the display to tunnels that use a matching attributes list.
destination *address*	(Optional) Restricts the display to tunnels destined to the specified IP address.
down	(Optional) Displays tunnels that are not active.
interface *type number*	(Optional) Displays information for the specified interface.
name *name*	(Optional) Displays the tunnel with the specified string. The tunnel string is derived from the interface description, if specified; otherwise, it is the interface name. The tunnel string is included in the signaling message so that it is available at all hops.
name-regexp *reg-exp*	(Optional) Displays tunnels whose descriptions match the specified regular expression.
role	Restricts the display to tunnels with the indicated role (all, head, middle, tail, or remote).
all	Displays all the tunnels.
head	Displays tunnels with their head at this router.
middle	Displays tunnels with a midpoint at this router.
remote	Displays tunnels with their head at some other router; this is a combination of middle and tail.
tail	Displays tunnels with a tail at this router.
source-id	(Optional) Restricts the display to tunnels with a matching source IP address or tunnel number.
ipaddress	Source IP address.
tunnel-id	Tunnel number. The range is from 0 to 65535.
suboptimal	(Optional) Displays information about tunnels using a suboptimal path.
constraints	Specifies constraints for finding the best comparison path.

current	Displays tunnels whose path metric is greater than the current shortest path, constrained by the tunnel's configured options. Selected tunnels would have a shorter path if they were reoptimized immediately.
max	Displays information for the specified tunneling interface.
none	Displays tunnels whose path metric is greater than the shortest unconstrained path. Selected tunnels have a longer path than the IGP shortest path.
up	(Optional) Displays tunnels if the tunnel interface is up. Tunnel midpoints and tails are typically up or not present.
accounting	(Optional) Displays accounting information (the rate of the traffic flow) for tunnels.
brief	(Optional) Specifies a format with one line per tunnel.
protection	(Optional) Displays information about the protection provided by each tunnel selected by other options specified with this command. The information includes whether protection is configured for the tunnel, the protection (if any) provided to the tunnel by this router, and the bandwidth protected.

Command Default

General information about each MPLS TE tunnel known to the router is displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

To select the tunnels for which information is displayed, use the **attributes**, **destination**, **interface**, **name**, **name-regexp**, **property**, **role**, **source-id**, **suboptimal constraints**, **up**, and **down** keywords singly or combined.

To select the type of information displayed about the selected tunnels, use the **accounting**, **protection**, **statistics**, and **summary** keywords.

The **name-regexp** keyword displays output for each tunnel whose name contains a specified string. For example, if there are tunnels named iou-100-t1, iou-100-t2, and iou-100-t100, the **show mpls traffic-eng tunnels name-regexp iou-100** command displays output for the three tunnels whose name contains the string iou-100.

If you specify the **name** keyword, there is command output only if the command name is an exact match; for example, iou-100-t1.

Examples

The following is sample output from the **show mpls traffic-eng tunnels brief** command. It displays brief information about every MPLS TE tunnel known to the router.

```
Router# show mpls traffic-eng tunnels brief
```

```
Signalling Summary:
    LSP Tunnels Process: running
    RSVP Process: running
    Forwarding: enabled
    Periodic reoptimization: every 3600 seconds, next in 1706 seconds
TUNNEL NAME     DESTINATION     UP IF        DOWN IF
STATE/PROT
Router_t1       10.112.0.12      -        TenGigabitEthernet4/1     up/up
Router_t2      10.112.0.12     -       TenGigabitEthernet4/1    up/down
Router_t3       10.112.0.12      -        TenGigabitEthernet4/1
admin-down
Router_t1000   10.110.0.10     -       TenGigabitEthernet4/1    up/down
Displayed 4 (of 4) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

The following is sample output from the **show mpls traffic-eng tunnels accounting** command. This command displays the rate of the traffic flow for the tunnels.

```
Router# Router# show mpls traffic-eng tunnels accounting
```

```
Tunnel1 (Destination 10.103.103.103; Name iou-100_t1)
5 minute output rate 0 kbits/sec, 0 packets/sec
Tunnel2 (Destination 10.103.103.103; Name iou-100_t2)
5 minute output rate 0 kbits/sec, 0 packets/sec Tunnel100 (Destination
10.101.101.101; Name iou-100_t100)
5 minute output rate 0 kbits/sec, 0 packets/sec Totals for 3 Tunnels
5 minute output rate 0 kbits/sec, 0 packets/sec
```

The following is sample output from the **show mpls traffic-eng tunnels tunnel** command. This command displays information about just a single tunnel.

```
Router# show mpls traffic-eng tunnels tunnel 1
```

```
Name: t1 (Tunnel1) Destination: 10.0.0.4
Status:
Admin: admin-down Oper: down Path: not valid Signalling: Down
path option 1, type explicit gi7/4-R4
Config Parameters:
Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
AutoRoute: disabled LockDown: disabled Loadshare: 0 bw-based
auto-bw: disabled
Shortest Unconstrained Path Info:
Path Weight: 2 (TE)
Explicit Route: 10.1.0.1 10.1.0.2 172.0.0.1 192.0.0.4
History:
Tunnel:
Time since created: 13 days, 52 minutes
Number of LSP IDs (Tun_Instances) used: 0
```

Related Commands

Command	Description
mpls traffic-eng tunnels	Enables MPLS traffic engineering tunnel signaling on a device.

show ip ospf mpls ldp interface

To display information about interfaces belonging to an OSPF process that is configured for MPLS LDP-IGP, use the **show ip ospf mpls ldp interface** command in privileged EXEC mode.

show ip ospf [*process-id*] **mpls ldp interface** [*interface*]

Syntax Description

process-id	(Optional) Process ID. Includes information only for the specified routing process.
interface	(Optional) Defines the interface for which MPLS LDP-IGP synchronization information is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command shows MPLS LDP-IGP synchronization information for specified interfaces or OSPF processes. If you do not specify an argument, information is displayed for each interface that was configured for MPLS LDP-IGP synchronization.

Examples

The following is a sample output of the **show ip ospf mpls ldp interface** command.

```
TenGigabitEthernet4/1
  Process ID 1, Area 0
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization: Yes
  Holddown timer is not configured
  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
```

Related Commands

Command	Description
show mpls ldp igp sync	Displays the status of the MPLS LDP-IGP synchronization process.

show mpls interfaces

To display information about one or more or all interfaces that are configured for label switching, use the **show mpls interfaces** command in user EXEC or privileged EXEC mode.

show mpls interfaces [*interface*] [**all**] [**detail**] [**internal**]

Syntax Description

interface	(Optional) Defines the interface about which to display label switching information.
all	(Optional) When the **all** keyword is specified alone in this command, information about the interfaces configured for label switching is displayed for all VPNs, including the VPNs in the default routing domain.
detail	(Optional) Displays detailed label switching information.
internal	(Optional) Indicates whether MPLS egress NetFlow accounting and other internal options are enabled.

Command Default

If no optional keyword or argument is specified in this command, summary information is displayed for each interface that has been configured for label switching in the default routing domain.

Command Modes

User EXEC (>) and Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command shows MPLS information about the specified interface, or about all the interfaces for which MPLS has been configured. If no optional keyword or argument is specified in this command, summary information is displayed for each interface configured for label switching.

Examples

The following example shows that LDP was enabled on the interface by both the **mpls ip** and **mpls ldp autoconfig** commands:

```
Router# show mpls interfaces TenGigabitEthernet4/1 detail
```

```
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
```

Related Commands

Command	Description
mpls label protocol ldp	Specifies the default label distribution protocol on all the interfaces.
mpls ip	Enables MPLS hop-by-hop forwarding on all the interfaces.
mpls traffic-eng tunnels	Enables MPLS traffic engineering tunnel signaling on a device.

show mpls ldp discovery

To display the status of the LDP discovery process, use the **show mpls ldp discovery** command in user EXEC or privileged EXEC mode.

show mpls ldp discovery [all] [detail]

Syntax Description

all	(Optional) Displays LDP discovery information for all VPNs, including those in the default routing domain.
detail	(Optional) Displays detailed information about all LDP discovery sources on a label switch router (LSR).

Command Default

This command displays neighbor discovery information for the default routing domain.

Command Modes

User EXEC and Privileged EXEC

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command displays neighbor discovery information for LDP. It generates a list of interfaces over which the LDP discovery process is running.

Examples

The following example displays the LDP router ID.

```
Router# show mpls ldp discovery
```

```
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
```

Related Commands

Command	Description
mpls label protocol	Specifies the default label distribution protocol.
mpls ldp neighbor	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
show mpls interfaces	Displays information about one or more interfaces that have been configured for label switching.
show mpls ldp neighbor	Displays the status of LDP sessions.

show mpls ldp igp sync

To display the status of the MPLS LDP-Interior Gateway Protocol (IGP) synchronization process, use the **show mpls ldp igp sync** command in user EXEC or privileged EXEC mode.

show mpls ldp igp sync [**all** | **interface** *type number*]

Syntax Description

all	(Optional) Displays all the MPLS LDP-IGP synchronization information available.
interface *type number*	(Optional) Displays the MPLS LDP-IGP synchronization information for the specified interface.

Command Modes

User EXEC(>) and Privileged EXEC(#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

If an optional argument is not specified, this command displays LDP synchronization for all the interfaces enabled for MPLS LDP-IGP synchronization.

Examples

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.

```
Router# show mpls ldp igp sync
```

```
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
```

Related Commands

Command	Description
mpls ldp igp sync	Enables MPLS LDP-IGP synchronization on an interface that belongs to an OSPF process.
mpls ldp igp sync holddown	Specifies how long an IGP should wait for LDP synchronization to be achieved.

Command	Description
mpls ldp sync	Enables MPLS LDP-IGP synchronization on interfaces for an OSPF process.

show mpls ldp neighbor

To display the status of LDP sessions, use the **show mpls ldp neighbor** command in user EXEC or privileged EXEC mode.

show mpls ldp neighbor [**all**] [*address* | *interface*] [**detail**] [**graceful-restart**]

Syntax Description

all	(Optional) Displays LDP neighbor information for all VPNs, including those in the default routing domain.
address	(Optional) Identifies the neighbor with this IP address.
interface	(Optional) Identifies the LDP neighbors accessible over this interface.
detail	(Optional) Displays information in long form, including password information for this neighbor.
graceful-restart	(Optional) Displays graceful restart information for each neighbor.

Command Default

This command displays information about LDP neighbors for the default routing domain.

Command Modes

User EXEC and Privileged EXEC

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The **show mpls ldp neighbor** command can provide information about all the LDP neighbors, or the information can be limited to the following:

- Neighbor with specific IP address
- LDP neighbors accessible over a specific interface

Note This command displays information about LDP neighbor sessions.

Examples

The following is sample output from the **show mpls ldp neighbor** command.

```
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
```

Related Commands

Command	Description
show mpls interfaces	Displays information about one or more interfaces that have been configured for label switching.
show mpls ldp discovery	Displays the status of the LDP discovery process.

trace mpls

To discover MPLS LSP routes that packets actually take when traveling to their destinations, use the **trace mpls** command in privileged EXEC mode.

trace mpls

{**ipv4** *destination-address/destination-mask-length*

| **traffic-eng Tunnel** *tunnel-number*

| **pseudowire** *destination-address vc-id* **segment** *segment-number* [*segment number*]}

[**timeout** *seconds*]

[**destination** *address-start* [*address-end* | *address-increment*]]

[**revision** {**1** | **2** | **3** | **4**}]

[**source** *source-address*]

[**exp** *exp-bits*]

[**ttl** *maximum-time-to-live*]

[**reply** {**dscp** *dscp-bits* | **mode** *reply-mode* {**ipv4** | **no-reply** | **router-alert**} | **pad-tlv**}]

[**force-explicit-null**]

[**output interface** *tx-interface* [**nexthop** *ip-address*]]

[**flags fec**]

[**revision** *tlv-revision-number*]

Syntax Description

ipv4	Specifies the destination type as a LDP IPv4 address.
destination-address	Address prefix of the target to be tested.
/destination-mask-length	Number of bits in the network mask of the target address. The slash is required.
traffic-eng Tunnel *tunnel-number*	Specifies the destination type as a MPLS-TE tunnel.
destination	(Optional) Specifies a network 127 address.
address-start	(Optional) Beginning network 127 address.
address-end	(Optional) Ending network 127 address.
increment	(Optional) Number by which to increment the network 127 address.
ttl *maximum-time-to-live*	(Optional) Specifies a maximum hop count. Default is 30.
pseudowire	Specifies the destination type as an Any Transport over MPLS (AToM) virtual circuit (VC).
ipv4-address	IPv4 address of the AToM VC to be tested.

vc-id	Specifies the VC identifier of the AToM VC to be tested.
segment *segment-number*	(Optional) Specifies a segment of a multisegment pseudowire.
revision {**1** | **2** | **3** | **4**	(Optional) Selects the type, length, values (TLVs) version.
source *source-address*	(Optional) Specifies the source address or name. The default address is loopback0. This address is used as the destination address in the MPLS echo response.
timeout *seconds*	(Optional) Specifies the timeout interval in seconds for an MPLS request packet. The range is from 0 to 3600. The default is 2 seconds.
reply dscp *dscp-bits*	(Optional) Provides the capability to request a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value.
reply pad-tlv	(Optional) Tests the ability of the sender of an echo reply to support the copy pad TLV to echo reply.
reply mode *reply-mode*	(Optional) Specifies the reply mode for the echo request packet. The *reply-mode* is one of the following: **ipv4**—Reply with an IPv4 UDP packet (default). **no-reply**—Do not send an echo request packet in response. **router-alert**—Reply with an IPv4 UDP packet with router alert.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for an MPLS echo reply. Valid values are from 0 to 7. Default is 0.
revision *tlv-revision-number*	(Optional) Cisco TLV revision number.
force-explicit-null	(Optional) Forces an explicit null label to be added to the MPLS label stack even though the label was unsolicited.
output interface *tx-interface*	(Optional) Specifies the output interface for echo requests.
nexthop *ip-address*	(Optional) Causes packets to go through the specified next-hop address.
flags fec	(Optional) Requests that target Forwarding Equivalence Class (FEC) stack validation be done at the egress router. A downstream map TLV containing the correct received labels must be present in the echo request for target FEC stack checking to be performed. Ensure to use this keyword in conjunction with the **ttl** keyword.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use the **trace mpls** command to validate, test, or troubleshoot IPv4 LDP LSPs and IPv4 RSVP TE tunnels.

The following keywords are not available with the **ping mpls pseudowire** command:

- **flags**
- **force-explicit-null**
- **output**
- **revision**
- **ttl**

Examples

The following example shows how to trace packets through a MPLS TE tunnel.

```
Router# trace mpls traffic-eng Tunnel 0
```

```
Tracing MPLS TE Label Switched Path on Tunnel0, timeout is 2 seconds
Codes:
'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
0 10.131.159.230 mtu 1500 [Labels: 22 Exp: 0]
R 1 10.131.159.225 mtu 1500 [Labels: 22 Exp: 6] 72 ms
R 2 10.131.191.229 mtu 1504 [implicit-null] 72 ms
! 3 10.131.191.252 92 ms
```

Related Commands

Command	Description
ping mpls	Checks MPLS LSP connectivity.

tunnel mode mpls traffic-eng

To set the mode of a tunnel to MPLS for traffic engineering, use the **tunnel mode mpls traffic-eng** command in interface configuration mode. To disable this feature, use the **no** form of this command.

tunnel mode mpls traffic-eng

no tunnel mode mpls traffic-eng

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command specifies that the tunnel interface is for an MPLS traffic engineering tunnel and enables the various tunnel MPLS configuration options.

Examples

The following example shows how to set the mode of the tunnel to MPLS traffic engineering.

```
Router(config-if)# tunnel mode mpls traffic-eng
```

Related Commands

Command	Description
tunnel mpls traffic-eng affinity	Configures an affinity for a MPLS traffic engineering tunnel.
tunnel mpls traffic-eng autoroute announce	Instructs the IGP to use the tunnel in its enhanced SPF algorithm calculation (if the tunnel is up).
tunnel mpls traffic-eng bandwidth	Configures the bandwidth required for a MPLS traffic engineering tunnel.
tunnel mpls traffic-eng path-option	Configures a path option.
tunnel mpls traffic-eng priority	Configures setup and reservation priority for a MPLS traffic engineering tunnel.

tunnel mpls traffic-eng path-option

To configure a path option for a MPLS–TE tunnel, use the **tunnel mpls traffic-eng path-option** command in interface configuration mode. To disable this function, use the **no** form of this command.

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**]}}

no tunnel mpls traffic-eng path-option *number*

Syntax Description

number	Preference for this path option. When you configure multiple path options, lower numbered options are preferred. Valid values are from 1 to 1000.
dynamic	Dynamically calculates the path of the LSP.
attributes *lsp-attributes*	(Optional) Identifies an LSP attribute list. The attribute list used must be the same as the primary path option being configured.
bandwidth *kbps*	(Optional) Overrides the bandwidth configured on the tunnel or the attribute list. The kbps is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295. The bandwidth value must be the same as the primary path option being configured.
lockdown	(Optional) Indicates that the LSP cannot be reoptimized.
verbatim	(Optional) Bypasses the topology database verification process.
explicit	Specifies that the path of the LSP is an IP explicit path.
name *path–name*	Specifies the path name of the IP explicit path that the tunnel uses with this option.
identifier *path–number*	Specifies the path number of the IP explicit path that the tunnel uses with this option. The range is from 1 to 65535.

Command Default

No path option for an MPLS TE tunnel is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

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. Path setup preference is for lower (not higher) numbers, so option 1 is preferred.

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.

Examples

The following example shows how to configure the tunnel to use a named IP explicit path.

```
Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name test
```

Related Commands

Command	Description
ip explicit-path	Enters the command mode for IP explicit paths and creates or modifies the specified path.
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show ip explicit-paths	Displays the configured IP explicit paths.
tunnel mpls traffic-eng path-option protect	Configures a secondary path option for a MPLS TE tunnel.

tunnel mpls traffic-eng autoroute announce

To specify that the IGP must use the tunnel in its enhanced shortest path first (SPF) calculation, use the **tunnel mpls traffic-eng autoroute announce** command in interface configuration mode. To disable this feature, use the **no** form of this command.

tunnel mpls traffic-eng autoroute announce

no tunnel mpls traffic-eng autoroute announce

Syntax Description

This command has no arguments or keywords.

Command Default

The IGP does not use the tunnel in its enhanced SPF calculation.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The only way to forward traffic onto a tunnel is by enabling this command or by explicitly configuring forwarding (for example, with an interface static route).

Examples

The following example shows how to specify that the IGP must use the tunnel in its enhanced SPF calculation if the tunnel is up.

```
Router(config-if)# tunnel mpls traffic-eng autoroute announce
```

Related Commands

Command	Description
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.

tunnel mpls traffic-eng bandwidth

To configure the bandwidth required for a MPLS-TE tunnel, use the **tunnel mpls traffic-eng bandwidth** command in interface configuration mode. To disable this bandwidth configuration, use the **no** form of this command.

tunnel mpls traffic-eng bandwidth *kbps*

no tunnel mpls traffic-eng bandwidth

Syntax Description

kbps	The bandwidth, in kilobits per second, set aside for the MPLS TE tunnel. The range is from 1 to 4294967295. The default value is 0.

Command Default

The default tunnel is a global pool tunnel.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

If automatic bandwidth is configured for the tunnel, the **tunnel mpls traffic-eng bandwidth** command configures the initial tunnel bandwidth, which will be adjusted by the autobandwidth mechanism.

Examples

The following example shows how to configure 100 kbps of bandwidth for the MPLS traffic engineering tunnel.

```
Router(config-if)# tunnel mpls traffic-eng bandwidth 100
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
show mpls traffic-eng tunnel	Displays information about tunnels.

tunnel mpls traffic-eng priority

To configure the setup and reservation priority for MPLS-TE tunnel, use the **tunnel mpls traffic-eng priority** command in interface configuration mode. To remove the specified setup and reservation priority, use the **no** form of this command.

tunnel mpls traffic-eng priority *setup-priority* [*hold-priority*]

no tunnel mpls traffic-eng priority *setup-priority* [*hold-priority*]

Syntax Description

setup-priority	The priority used when signaling a LSP for this tunnel to determine which existing tunnels can be preempted. 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.
hold-priority	(Optional) The priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signaled. Valid values are from 0 to 7, where a lower number indicates a higher priority.

Command Default

By default, the setup priority is 7. The value of hold priority is the same as the value of setup priority.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

When an LSP is being signaled and an interface does not currently have enough bandwidth available for that LSP, the lower-priority LSPs are pre-empted so that the new LSP can be admitted.

The new LSP's priority is its setup priority and the existing LSP's priority is its hold priority. The two priorities enables the signaling of an LSP with a low setup priority (so that the LSP does not preempt other LSPs on setup) but a high hold priority (so that the LSP is not preempted after it is established).

Setup priority and hold priority are typically configured to be equal, and setup priority cannot be better (numerically smaller) than the hold priority.

Examples

The following example shows how to configure a tunnel with a setup and hold priority of 1.

```
Router(config-if)# tunnel mpls traffic-eng priority 1 1
```

Related Commands

Command	Description
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.

tunnel mpls traffic–eng path–option protect

To configure a secondary path option for a MPLS–TE tunnel, use the **tunnel mpls traffic-eng path-option protect** command in interface configuration mode. To disable this function, use the **no** form of this command.

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**]]}

no tunnel mpls traffic-eng path-option protect *number*

Syntax Description

number	The primary path option being protected. Valid values are from 1 to 1000.
dynamic	Dynamically calculates the path of the LSP.
attributes *lsp-attributes*	(Optional) Identifies an LSP attribute list. The attribute list used must be the same as the primary path option being protected.
bandwidth *kbps*	(Optional) Overrides the bandwidth configured on the tunnel or the attribute list. The *kbps* value is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295. The bandwidth value must be the same as the primary path option being configured.
lockdown	(Optional) Indicates that the LSP cannot be reoptimized.
verbatim	(Optional) Bypasses the topology database verification process.
explicit	Specifies that the path of the LSP is an IP explicit path.
name *path–name*	Specifies the path name of the IP explicit path that the tunnel uses with this option.
identifier *path–number*	Specifies the path number of the IP explicit path that the tunnel uses with this option. The range is from 1 to 65535.

Command Default

The MPLS TE tunnel does not have a secondary path option.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Cisco recommends that the primary path options being protected use explicit paths.

Calculation of a dynamic path for the path protected LSP is not available. When configuring the IP explicit path for the path protected LSP, choose hops that minimize the number of links and nodes shared with the primary path option that is being protected.

If the path option being protected uses an attribute list, configure path protection to use the same attribute list.

If the path option being protected uses bandwidth override, configure path protection to use bandwidth override with the same values.

Examples

The following example shows how to configure the tunnel to use a named IP explicit path.

```
Router(config-if)# tunnel mpls traffic-eng path-option protect 1 explicit name test
```

The following example shows how to configure path option 1 to use an LSP attribute list identified with the numeral 1.

```
Router(config-if)# tunnel mpls traffic-eng path-option protect 1 explicit name test attributes
 1
```

The following example shows how to configure bandwidth for a path option to override the bandwidth configured on the tunnel.

```
Router(config-if)# tunnel mpls traffic-eng path-option protect 3 explicit name test bandwidth
 0
```

Related Commands

Command	Description
ip explicit-path	Enters the command mode for IP explicit paths and creates or modifies the specified path.
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show ip explicit-paths	Displays the configured IP explicit paths.
tunnel mpls traffic-eng path-option	Configures a primary path for an MPLS TE tunnel.

MPLS TP Command Reference

This chapter describes commands to configure Multiprotocol Label Switching Transport Profile (MPLS TP).

bfd-template

To create a Bidirectional Forwarding Detection (BFD) template and to enter BFD configuration mode, use the **bfd-template** command in global configuration mode. To disable a BFD template, use the **no** form of this command.

bfd-template single-hop *template-name*

no bfd-template single-hop *template-name*

Syntax Description

single-hop	Specifies a single-hop BFD template.
template-name	Name of the template.

Command Default

The BFD template does not exist.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The **bfd-template** command enables you to create a BFD template and enter BFD configuration mode. The template can be used to specify a set of BFD interval values. The BFD interval values specified as part of the BFD template are not specific to a single interface.

Examples

The following example shows how to create a BFD template and specify BFD interval values.

```
Router(config)# bfd-template single-hop node1
Router(config-bfd)# interval min-tx 120 min-rx 100 multiplier 3
```

Related Commands

Command	Description
interval (MPLS–TP)	Configures the transmit and receive intervals between BFD packets.

debug mpls tp

To display Multiprotocol Label Switching (MPLS) Transport Profile (TP) error messages, use the **debug mpls tp** command in privileged EXEC mode. To disable the display of the messages, use the **no** form of this command.

debug mpls tp [**all** | **cli** | **error** | **event** | **fault-oam** | **ha** | **init** | **link-num** | **lsp-db** | **lsp-ep** | **lsp-mp** | **mem** | **tun-db** | **tunnel**]

no debug mpls tp

Syntax Description

all	Displays all debug messages.
cli	Displays MPLS-TP CLI debug messages.
error	Displays MPLS-TP error debug messages.
event	Displays MPLS-TP event debug messages.
fault-oam	Displays MPLS-TP fault OAM debug messages.
ha	Displays MPLS-TP high availability (HA) debug messages.
init	Displays MPLS-TP initialization debug messages.
link-num	Displays MPLS-TP link management debug messages.
lsp-db	Displays MPLS-TP midpoint label switched path (LSP) database debug messages.
lsp-ep	Displays MPLS-TP endpoint (EP) LSP configuration and operation debug messages.
lsp-mp	Displays MPLS-TP midpoint (MP) LSP configuration and operation debug messages.
mem	Displays MPLS-TP memory allocation and usage debug messages.
tun-db	Displays MPLS-TP tunnel database debug messages.
tunnel	Displays MPLS-TP tunnel configuration and operation debug messages.

Command Default

Debug messages are not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example displays the MPLS–TP endpoint LSP configuration and operation debug messages.

```
Router# debug mpls tp lsp-ep
```

Related Commands

Command	Description
show mpls tp	Displays information about the MPLS TP tunnels.

interface tunnel-tp

To create a Multiprotocol Label Switching (MPLS) transport profile (TP) tunnel and configure its parameters, use the **interface tunnel-tp** command in global configuration mode.

interface tunnel-tp *number*

Syntax Description

number	Number of the MPLS-TP tunnel.

Command Default

MPLS-TP tunnel parameters are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use this command on the endpoint routers to specify the parameters of the MPLS-TP tunnel.

This command also enters interface configuration mode (config-if). From this mode, configure the following MPLS-TP parameters:

Command	Description
bfd *bfd-template*	Specifies the Bidirectional Forwarding Detection (BFD) template for the tunnel. • If the BFD template for an MPLS-TP tunnel is updated after the tunnel is brought up, a BFD session is brought up on both the working and, if configured, the protect LSPs. • If the BFD template for a tunnel is changed, the BFD sessions for the working and protect LSPs is brought down and then brought back up with the new BFD template. • If a BFD template is not configured on an MPLS-TP tunnel, the initial LSP state will be DOWN.

Command	Description
protect-lsp	Enters protect LSP interface configuration mode (config-if-protect). From this mode, configure the following parameters: • Incoming link number and label (**in-label** *num*). • Lock (**lockout**). • Number of the protect LSP (**lsp-number**). By default, the protect LSP number is 1. • Outgoing label and link numbers (**out-label** *num* **out-link** *num*). A protect LSP is a backup for a working LSP. If the working LSP fails, traffic is switched to the protect LSP until the working LSP is restored, at which time forwarding reverts to the working LSP. Traffic can be locked out on either the working LSP or the protect LSP but not both. When traffic is locked out of the working or protect LSP, no traffic is forwarded on that LSP. The lockout of the LSP is signaled from one endpoint to the other. When one end has locked out one LSP, the other end may only lockout the same LSP. It is strongly advised to lockout the LSP from both ends, so that both sides know (locally) that the LSP is locked out in the absence of further signaling, which may be the case if connectivity of the LSP is broken due to maintenance for an extended time. In the absence of connectivity, a single-ended lockout expires at the remote end in under 15 minutes (256 * 3.5 seconds).

Command	Description
protection trigger [**ais** | **ldi** | **lkr**]	(Optional) Specifies protection triggers for Alarm Indication Signal (AIS), Link Down Indication (LDI), Lock Report (LKR) messages. These should be used in rare cases. They help in specifying which of these fault notifications can trigger a protection switch. The default is to inherit the setting of the similar commands from the global settings of protection trigger. This command enables a tunnel to override the global settings. The default for the global settings is that protection is triggered on receipt of LDI and LKR, but not AIS. (AIS is a non-fatal indication of potential issues, which turns into LDI when it is known to be fatal.) This command is useful when other devices send AIS or LDI in unexpected ways. For example, a device from another vendor sends AIS when there are link failures and never sends AIS with the LDI flag . In this case, configure the **protection trigger ais** command. If a device sends LDI when there is no actual failure, but there is a possible failure, and the BFD must detect the actual failure and cause protection switching, configure the **no protection trigger ldi** command. To undo these configuration settings and resume inheriting the global settings, use the **default protection trigger** [**ais** | **ldi** | **lkr**] command.
tp bandwidth *num*	(Optional) Specifies the transmit bandwidth, in kilobytes. The valid range is from 1 to 10000000. The default is 0. With MPLS-TP, the **bandwidth** command cannot be used in interface configuration mode. Use the **tp bandwidth** command.
tp destination *node-id* [**tunnel-tp** *num*] [**global-id** *num*]	Specifies the destination MPLS-TP node ID. **tunnel-tp** *num*—(Optional) Indicates 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. **global-id** *num*—(Optional) Indicates the global ID used for the remote end of this MPLS-TP tunnel. The valid range is from 0 to 2147483647. The default is the global ID that is configured with the **mpls tp** command.

Command	Description
tp source *node-id* [**global-id** *num*]	(Optional) Specifies the source MPLS-TP tunnel node ID. This is the ID of the endpoint router being configured. The source ID can be specified to override the router ID configured in the global MPLS-TP configuration. The **tp source** command is optional and not typically used, because the global router ID and global ID can be used to identify the tunnel source at the endpoint. All tunnels on the router generally use the same (globally specified) source information. **global-id** *num*—(Optional) Indicates the global ID of the local endpoint for this tunnel. The valid range is from 0 to 2147483647. The default is the global global ID that is configured with the **mpls tp** command.
tp tunnel-name *name*	(Optional) Specifies the name of the MPLS-TP tunnel. The TP tunnel name is displayed in the **show mpls tp tunnel** command output. This command is useful for consistently identifying the tunnel at all endpoints and midpoints.

Command	Description
working-lsp	Enters working LSP interface configuration mode (config-if-working). From this mode, configure the following parameters: • Incoming link number and label (**in-label** *num*). • Lock (**lockout**) • Number of the working LSP (**lsp-number**). By default, the working LSP number is 0. • Outgoing label and link numbers (**out-label** *num* **out-link** *num*) A working LSP is the primary LSP. If the working LSP fails, traffic is switched to the protect LSP until the working LSP is restored, at which time forwarding reverts to the working LSP. The lockout of the LSP is signaled from one endpoint to the other. When one end has locked out one LSP, the other end may only lockout the same LSP. It is strongly advised to lockout the LSP from both ends, so that both sides know (locally) that the LSP is locked out in the absence of further signaling, which may be the case if connectivity of the LSP is broken due to maintenance for an extended time. In the absence of connectivity, a single-ended lockout expires at the remote end in under 15 minutes (256 * 3.5 seconds).

Examples

The following example shows how to specify the parameters for an MPLS-TP tunnel.

```
Router(config)# interface Tunnel-tp1
Router(config-if)# description "MPLS-TP tunnel # 1"
Router(config-if)# no ip address
Router(config-if)# no keepalive
Router(config-if)# tp bandwidth 10000
Router(config-if)# tp destination 10.1.1.1
Router(config-if)# bfd mpls-tp-bfd-2
Router(config-if)# working-lsp
Router(config-if-working)# in-label 211 out-label 112 out-link 1
Router(config-if-working)# exit
Router(config-if)# protect-lsp
Router(config-if-protect)# in-label 511 out-label 115 out-link 2
Router(config-if-protect)# exit
```

Related Commands

Command	Description
mpls tp	Specifies global values used across the MPLS TP implementation and applies to all the tunnels and midpoint LSPs.

interval (mpls–tp)

To configure the transmit and receive intervals between BFD packets and to specify the number of consecutive BFD control packets to miss before BFD declares that a peer is unavailable, use the **interval** command in BFD configuration mode. To disable interval values, use the **no** form of this command.

interval [**microseconds**] {**both** *time* | **min-tx** *time* **min-rx** *time*} [**multiplier** *multiplier-value*]

no interval

Syntax Description

microseconds	(Optional) Specifies, in microseconds, the rate at which BFD control packets are sent to and received from BFD peers. If the **microseconds** keyword is not specified, the interval defaults to milliseconds.
both *time*	Specifies the rate at which BFD control packets are sent to BFD peers and the rate at which BFD control packets are received from BFD peers.
min-tx *time*	Specifies the rate at which BFD control packets are sent to BFD peers.
min-rx *time*	Specifies, the rate at which BFD control packets are received from BFD peers.
multiplier *multiplier-value*	(Optional) Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The range is from 3 to 50. The default value is 3.

Command Default

The transmit and receive intervals between BFD packets are not set.

Command Modes

BFD configuration (config-bfd)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The **interval** command enables you to configure the session parameters for a BFD template.

Examples

The following example shows how to configure interval settings for the node1 BFD template.

```
Router(config)# bfd-template single-hop node1
Router(config-bfd)# interval min-tx 120 min-rx 100 multiplier 3
```

Related Commands

Command	Description
bfd-template	Creates a BFD template and enters BFD configuration mode.

local interface

To specify the pseudowire type when configuring static to dynamic pseudowires in an Mutliprotocol Label Switching Transport Protocol (MPLS-TP) network, use the **local interface** command in VFI neighbor configuration mode. To disable the pseudowire type, use the **no** form of this command.

local interface *pseudowire-type*

no local interface *pseudowire-type*

Syntax Description

pseudowire-type Specifies the pseudowire type by its number in hex format:

01 Frame Relay DLCI (Martini mode)

02 ATM AAL5 SDU VCC transport

03 ATM transparent cell transport

04 Ethernet Tagged mode

05 Ethernet

06 HDLC

07 PPP

08 SONET/SDH Circuit Emulation Service Over MPLS

09 ATM n-to-one VCC cell transport

0A ATM n-to-one VPC cell transport

0B IP Layer 2 transport

0C ATM one-to-one VCC Cell mode

0D ATM one-to-one VPC Cell mode

0E ATM AAL5 PDU VCC transport

0F Frame-Relay Port mode

10 SONET/SDH Circuit Emulation over Packet

11 Structure-agnostic E1 over Packet

12 Structure-agnostic T1 (DS1) over Packet

13 Structure-agnostic E3 over Packet

14 Structure-agnostic T3 (DS3) over Packet

15 CESoPSN basic mode

16 TDMoIP AAL1 Mode

17 CESoPSN TDM with CAS

Command Default

The pseudowire type is not defined in the MPLS-TP network.

Command Modes

VFI neighbor configuration

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to set the local interface virtual circuit (VC) type to Ethernet.

```
Router(config-vfi-neighbor)# local interface 5
```

medium p2p

To configure the interface as point-to-point, use the **medium p2p** command in interface configuration mode. To return the interface to its normal mode, use the **no** form of this command.

medium p2p

no medium p2p

Syntax Description

This command has no arguments or keywords.

Command Default

Interfaces are configured to connect to multiple devices.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command enables the router to send and receive all MPLS-TP packets using a common multicast MAC address knowing that it is communicating with only one other device.

Examples

The following example shows how to configure the interface as point-to-point:

```
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# medium p2p
```

Related Commands

Command	Description
mpls tp link	Configures MPLS–TP link parameters.

mpls tp

To configure Multiprotocol Label Switching (MPLS) transport profile (TP) parameters and enter MPLS-TP configuration mode, use the **mpls tp** command in global configuration mode. To remove all MPLS-TP parameters, use the **no** form of this command.

mpls tp
no mpls tp

Syntax Description

This command has no arguments or keywords.

Command Default

MPLS-TP parameters are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use this command to enter MPLS-TP configuration mode. From this mode, configure the following parameters:

Command	Description
fault-oam refresh-timer *secs*	(Optional) Specifies the maximum time between successive fault Operations, Administration, and Maintenance (OAM) messages specified in seconds. The range is from 1 to20. The default value is 20.
global-id *num*	(Optional) Specifies the default global ID used for all endpoints and midpoints. The range is from 0 to 2147483647. The default value is 0. This command makes the router-id globally unique in a multiprovider tunnel. Otherwise, the router-id is only locally meaningful. The **global-id** is an autonomous system number, which is a controlled number space by which providers can identify each other.

Command	Description
protection trigger [**ais** | **ldi** | **lkr**]	(Optional) Specifies protection triggers for Alarm Indication Signal (AIS), Link Down Indication (LDI), Lock Report (LKR) messages. These should be used in rare cases. They help in changing the default protection-switching behavior for fault notifications on all tunnels. The default for these global settings is to trigger protection on receipt of LDI and LKR, but not AIS. (AIS is a non-fatal indication of potential issues, which turns into LDI when it is known to be fatal.) This command is useful when other devices send AIS or LDI in unexpected ways. For example, configure the **protection trigger ais** command to interoperate with another vendor whose devices send AIS when there are link failures and never send AIS with the LDI flag. Another example is if a device sends LDI when there is no actual failure, but there is a possible failure, and the BFD must detect the actual failure and cause protection switching, configure the **no protection trigger ldi** command. To undo these configuration settings and revert to the default settings, use the **no protection trigger [ais | ldi | lkr]** command.
router-id *router-id*	(Required) Specifies the default MPLS-TP router ID, which is used as the source node ID for all MPLS-TP tunnels configured on the router. This is required for MPLS-TP forwarding. This router-id is used in fault OAM messaging to identify the source of a fault on a midpoint router.
wtr-timer	Specifies the wait-to-restore (WTR) timer. This timer controls the length of time to wait before reversion following the repair of a fault on the original working path.

Examples

The following example shows how to enter MPLS-TP configuration mode.

```
Router(config)# mpls tp
Router(config-mpls-tp)#
```

The following example shows how to set the default router ID from MPLS-TP configuration mode.

```
Router(config-mpls-tp)# router-id 10.10.10.10
```

Related Commands

Command	Description
mpls tp lsp	Specifies the parameters for two ends of the MPLS-TP tunnel from the tunnel midpoint.
interface tunnel-tp	Specifies the parameters for the MPLS tunnel.

mpls tp link

To configure Multiprotocol Label Switching (MPLS) transport profile (TP) link parameters, use the **mpls tp link** command in interface configuration mode.

mpls tp link *link-num* {**ipv4** *ip-address* | **tx-mac** *mac-address*} {**rx-mac** *mac-address*}

no mpls tp link *link-num*

Syntax Description

link-num	Number assigned to the link. It must be unique on the device. Only one link number can be assigned per interface. The range is from 1 to 2147483647.
ipv4 *ip-address*	Specifies the next-hop address that the Address Resolution Protocol (ARP) uses to discover the destination MAC address.
tx-mac {*mac-address*}	Specifies a per-interface transmit multicast MAC address. • *mac-address*—User-supplied MAC address. The **tx-mac** keyword is available only on point-to-point Ethernet interfaces. It is not available on serial interfaces.
rx-mac {*mac-address*}	Specifies a per-interface receive multicast MAC address. • *mac-address*—User-supplied MAC address. The **rx-mac** keyword is available only when the **tx-mac** keyword is used. It is not available on serial interfaces.

Command Default

MPLS-TP link parameters are not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The link number must be unique on the device. Only one link number can be assigned per interface.

MPLS-TP link numbers may be assigned to physical interfaces only. Bundled interfaces and virtual interfaces are not supported for MPLS-TP link numbers.

When an MPLS-TP link is configured without an IP address on an Ethernet interface, the Cisco IOS uses an IEEE Bridge Group MAC address (0180.c200.0000) for communication by default.

Examples

The following example shows how to create an MPLS-TP link without an IP address.

```
interface TenGigabitEthernet4/1
  medium p2p
  mpls tp link 1
```

The following example shows how to configure the unicast MAC address of the next-hop device.

```
interface TenGigabitEthernet4/1
  medium p2p
  mpls tp link 1 tx-mac 0000.0c00.1234
```

The following example shows how to configure the transmit and receive parameters for a different multicast address.

```
interface TenGigabitEthernet4/1
  medium p2p
  mpls tp link 1 tx-mac 0100.0c99.8877 rx-mac 0100.0c99.8877
```

Related Commands

Command	Description
medium p2p	Configures the interface as point-to-point.
mpls tp lsp	Specifies the parameters for two ends of the MPLS-TP tunnel from the tunnel midpoint.
interface tunnel-tp	Specifies the parameters for the MPLS tunnel.

mpls tp lsp

To configure Multiprotocol Label Switching (MPLS) transport profile (TP) midpoint connectivity, use the **mpls tp lsp** command in global configuration mode.

mpls tp lsp source *node-id* [**global-id** *num*] **tunnel-tp** *num* **lsp** {*lsp-num* | **protect** | **working**} **destination** *node-id* [**global-id** *num*] **tunnel-tp** *num*

Syntax Description

source *node-id*	Specifies the source node ID of the MPLS-TP tunnel.
global-id *num*	(Optional) Specifies the global ID of the tunnel source.
tunnel-tp *num*	Specifies the tunnel-TP number of MPLS-TP tunnel source.
lsp {*lsp-num* | **protect** | **working** }	Specifies the label switched path (LSP) within the MPLS-TP tunnel. • *lsp-num*—Specifies the number of the LSP • **protect**—Indicates that the LSP is a backup for the primary, or working, LSP. When you specify the **protect** keyword, the LSP number is 1. **working**—Indicates that the LSP is the primary LSP. When you specify the **working** keyword, the LSP number is 0. A protect LSP is a backup for a working LSP. When the working LSP fails, traffic is switched to the protect LSP until the working LSP is restored, at which time forwarding reverts to the working LSP.
destination *node-id*	Specifies the destination node ID of the MPLS-TP tunnel.
global-id *num*	(Optional) Specifies the global ID of the tunnel destination. The range is from 0 to 2147483647. The default value is 0.
tunnel-tp *num*	Specifies the tunnel-TP number of MPLS-TP tunnel destination.

Command Default

No MPLS-TP parameters are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use this command on midpoint routers to specify the source and destination parameters of the MPLS-TP tunnel. You can use the **mpls trace** command to validate that the traffic is traversing the correct tunnel at each midpoint.

This command also enters MPLS-TP LSP configuration mode (config-mpls-tp-lsp). From this mode, configure the following parameters:

Command	Parameter
forward-lsp *num*	Enters MPLS-TP LSP forward LSP configuration mode (config-mpls-tp-lsp-forw). From this mode, you can configure the following parameters: • Bandwidth (**bandwidth**) • Incoming label (**in-label**) and outgoing label and link numbers (**out-label out-link**)
reverse-lsp *name*	Enters MPLS-TP LSP reverse LSP configuration mode (config-mpls-tp-lsp-rev). From this mode, you can configure the following parameters: • Bandwidth (**bandwidth**) • Incoming label (**in-label**) and outgoing label and link numbers (**out-label out-link**)
tunnel-name *name*	Specifies the name of the MPLS-TP tunnel.

Examples

The following example shows how to configure a midpoint LSP carrying the working LSP of an MPLS-TP tunnel between node 209.165.200.225, tunnel-number 1 and 209.165.200.226, tunnel-number 2, using 1000 kbps bandwidth in both the directions:

```
Router(config)# mpls tp lsp source 209.165.200.225 tunnel-tp 1 lsp working destination
209.165.200.226 tunnel-tp 2
Router(config-mpls-tp-lsp)# forward-lsp
Router(config-mpls-tp-lsp-forw)# bandwidth 1000
Router(config-mpls-tp-lsp-forw)# in-label 20 out-label 40 out-link 10
Router(config-mpls-tp-lsp-forw)# exit
Router(config-mpls-tp-lsp)# reverse-lsp
Router(config-mpls-tp-lsp-rev)# bandwidth 1000
Router(config-mpls-tp-lsp-rev)# in-label 21 out-label 50 out-link 11
```

The following example shows how to configure a midpoint LSP on the protect LSP between node 2::209.165.200.225, tunnel 4 and 14::209.165.200.226, tunnel 2. No bandwidth is reserved:

```
Router(config)# mpls tp lsp source 209.165.200.225 global-id tunnel-tp 4 lsp protect
destination 10.11.11.11 global-id 14 tunnel-tp 12
Router(config-mpls-tp-lsp)# forward-lsp
Router(config-mpls-tp-lsp-forw)# in-label 30 out-label 100 out-link 37
Router(config-mpls-tp-lsp-forw)# exit
Router(config-mpls-tp-lsp)# reverse-lsp
Router(config-mpls-tp-lsp-rev)# in-label 31 out-label 633 out-link 30
```

Related Commands

Command	Description
mpls tp	Specifies the parameters of the MPLS-TP and enters MPLS-TP configuration mode.
interface tunnel-tp	Specifies the parameters for the MPLS tunnel.

ping mpls tp

To check Multiprotocol Label Switching (MPLS) transport protocol (TP) label switched path (LSP) connectivity, use the **ping mpls tp** command in privileged EXEC mode.

ping mpls tp tunnel-tp *num* **lsp** {**working** | **protect** | **active**}

[**ddmap** [**hashkey ipv4 bitmap** *bitmap-size* | **none**]

[**dsmap [hashkey ipv4 bitmap** *bitmap-size* | **none**]

[**destination** *ip-addr*]

[**exp** *num*]

[**flags fec**]

[**interval** *num*]

[**pad** *num*]

[**repeat** *num*]

[reply dscp *num* | **mode control channel**]

[**size** *num*]

[**source** *ip-addr*]

[**sweep** *num num num*]

[**timeout** *num*]

[**ttl** *num*]

[**verbose**]

Syntax Description

tunnel-tp *num*	Specifies the MPLS-TP tunnel number.
lsp {**working** | **protect** | **active**}	Specifies the type of MPLS-TP label switched path (LSP) on which to send echo request packets.
ddmap [**hashkey ipv4 bitmap** *bitmap-size*| **none**	Specifies the rate at which BFD control packets are sent to BFD peers. (Optional) Interrogates a transit router for downstream mapping (DDMAP) information. Allows you to control the hash key and multipath settings.Valid values are: **none**—There is no multipath (type 0). **ipv4 bitmap** *bitmap-size*—Size of the IPv4 addresses (type 8) bitmap. If you enter the **none** keyword, multipath LSP traceroute acts like enhanced LSP traceroute; that is, it uses multipath LSP traceroute retry logic and consistency checking.

dsmap [**hashkey ipv4 bitmap** *bitmap-size*| **none**	(Optional) Interrogates a transit router for downstream mapping (DSMAP) information. Allows you to control the hash key and multipath settings. Valid values are: **none**—There is no multipath (type 0). **ipv4 bitmap** *bitmap-size*—Size of the IPv4 addresses (type 8) bitmap. If you enter the **none** keyword, multipath LSP traceroute acts like enhanced LSP traceroute; that is, it uses multipath LSP traceroute retry logic and consistency checking.
destination *ip-addr*	(Optional) Specifies a network 127 address.
exp *num*	(Optional) Specifies the MPLS experimental field value in the MPLS header for an MPLS echo reply. The range is from 0 to 7. The default value is 0.
flags fec	(Optional) Allows Forward Equivalence Class (FEC) checking on the transit router. A downstream map TLV containing the correct received labels must be present in the echo request for target FEC stack checking to be performed. Target FEC stack validation is always done at the egress router. Be sure to use this keyword in conjunction with the ttl keyword.
interval *num*	(Optional) Specifies the time, in milliseconds (ms), between successive MPLS echo requests. This parameter allows you to pace the transmission of packets so that the receiving router does not drop packets. Default is 0.
pad *num*	(Optional) The pad TLV is used to fill the datagram so that the MPLS echo request (User Datagram Protocol [UDP] packet with a label stack) is the specified size. The default is 0xABCD.
repeat *num*	(Optional) Specifies the repeat count. Range: 1-2147483647
reply dscp *num* |**mode control channel**	(Optional) Provides the capability to request a specific quality of service (QoS) in an echo reply by providing a differentiated services code point (DSCP) value. The echo reply is returned with the IP header type of service (ToS) byte set to the value specified in the **reply dscp** command.
size *num*	Specifies the packet size.
source *ip-addr*	(Optional) Specifies the source address or name. The default address is loopback0. This address is used as the destination address in the MPLS echo response.
sweep *num num num*	(Optional) Enables you to send a number of packets of different sizes, ranging from a start size to an end size. This parameter is similar to the Internet Control Message Protocol (ICMP) ping sweep parameter.
timeout *num*	(Optional) Specifies the timeout interval in seconds for an MPLS request packet. The range is from 0 to 3600. The default is 2 seconds.
ttl *num*	(Optional) Specifies a time-to-live (TTL) value. The default is 225 seconds.

verbose	(Optional) Enables verbose output mode.

Command Default

Connectivity is not checked.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use the **ping mpls tp** command to validate, test, or troubleshoot MPLS TP LSPs.

Note The **ping mpls tp** command does not support interactive mode.

You can use ping and trace in an MPLS-TP network without IP addressing. However, no IP addresses are displayed in the output.

The following rules determine the source IP address:

1. Use the IP address of the TP interface
2. Use the global router ID.
3. Use router-id : A.B.C.D local node id in IPv4 address format. This is not an IP address. However, it is better to use a value rather than leave it as 0.0.0.0 and risk the packet being deemed invalid and dropped.

Examples

The following example checks connectivity of a MPLS-TP LSP.

```
Router# ping mpls tp tunnel-tp 1 repeat 1 ttl 2
```

```
Sending 1, 100-byte MPLS Echos to Tunnel-tp1,
   timeout is 2 seconds, send interval is 0 msec:
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 156/156/156
ms
```

Related Commands

Command	Description
trace mpls tp	Displays the MPLS LSP routes that packets take to their destinations.

pseudowire-static-oam class

To create an Operations, Administration, and Maintenance (OAM) class and specify the timeout intervals, use the **pseudowire-static-oam class** command in global configuration mode. To remove the specified class, use the **no** form of this command.

pseudowire-static-oam class *class-name*
no pseudowire-static-oam class *class-name*

Syntax Description

class-name	OAM class name. It creates an OAM class and enters static pseudowire OAM configuration mode, from which you can enter timeout intervals.

Command Default

OAM classes are not created.

Command Modes

Global configuration mode (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to create the class oam-class3 and enter static pseudowire OAM configuration mode.

```
Router(config)# pseudowire-static-oam class oam-class3
Router (config-st-pw-oam-class)# timeout refresh send ?
<1-4095> Seconds, default is 30
R1(config-st-pw-oam-class)# timeout refresh send 45 ?
```

Related Commands

Command	Description
status protocol notification static	Invokes the specified class as part of the static pseudowire.

pseudowire-tlv template

To create a template of pseudowire type, length, value (TLV) parameters to use in a MPLS-TP configuration, use the **pseudowire-tlv template** command in privileged EXEC configuration mode. To remove the template, use the **no** form of this command.

pseudowire-tlv template *template-name*
no pseudowire-tlv template *template-name*

Syntax Description

template-name	Name of the TLV template.

Command Default

TLV values are not specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to create a TLV template called tlv3.

```
Router(config)# pseudowire-tlv template tlv3
```

Related Commands

Command	Description
tlv template	Specifies a TLV template to use as part of the local interface configuration.

show mpls tp

To display information about Multiprotocol Label Switching (MPLS) transport profile (TP) tunnels, use the **show mpls tp** command in user EXEC or privileged EXEC mode.

show mpls tp [**link numbers**] [**lsps** [*node-id* [*options*]]] [**detail**] [**summary**] [**tunnel-tp** [*tunnel-num* [*options*]]] [**detail**]

Syntax Description

detail	Displays detailed output.
link-numbers	Displays information about the MPLS TP link number database.
lsps [*node-id*[*options*]]	Displays information about the MPLS TP label switched paths (LSPs), including those on midpoint and endpoint routers. • *node-id*—LSP information for that node ID. • *options*–LSP options: ◦ **endpoints**—Displays LSP information for the endpoint routers. ◦ **global-id** *num*—Displays LSP information for matching the global ID. ◦ **lsp** {*num* | **protect** | **working**}—Displays LSP information for a specific LSP. ◦ **midpoints**—Displays information about LSP midpoints configured on a router. ◦ **tunnel-name** *tunnel-tp-name*—Displays the information for a specific named tunnel. ◦ **tunnel-tp** *num*—Displays LSP information for a specific tunnel.
summary	Displays a summary of all link numbers.
tunnel-tp [*options*]	Displays information for MPLS-TP tunnels. Use a combination of any of the following options: • *tunnel-tp-number*—Displays the information for a specific numbered tunnel. • **lsps**—Displays LSP information for MPLS-TP tunnels. • *tunnel-tp-name*—Displays the information for a specific named tunnel.

Command Modes

User EXEC (>), Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following is a sample output from the **show mpls tp** command that displays MPLS–TP link number information.

```
Router> show mpls tp link-numbers
```

```
MPLS-TP Link Numbers:
Link    Interface                Next Hop        RX Macs
1       TenGigabitEthernet4/1  209.165.200.225
2       TenGigabitEthernet4/2  0180.c200.0000  0180.c200.0000
```

The following is a sample output from the **show mpls tp** command that displays information for MPLS–TP tunnels.

```
Router> show mpls tp tunnel-tp
```

```
MPLS-TP Tunnels:
Tunnel Peer                        Active Local  Out     Out       Oper
Number global-id::node-id::tun     LSP Label    Label  Interface  State
------ -----------------------     ------ ----- -----   ---------  -----
1      1::104.10.1.1::1            work 211      112      Ten4/1     up
2      20::104.10.1.1::2           work 221      122      Ten4/1     up
3      1::104.10.1.1::3            work 231      132      Ten4/1     up
4      0::10.20.20.4::4            work 241      142      Ten4/1     up
```

Related Commands

Command	Description
debug mpls tp	Displays MPLS TP debug messages.

status protocol notification static

To enable the timers set in the specified class name, use the **status protocol notification static** command in pseudowire-class configuration mode. To disable the use of the specified class, use the **no** form of this command.

status protocol notification static *class-name*
no status protocol notification static *class-name*

Syntax Description

class-name	OAM class that was created with the **pseudowire-static-oam-class** command.

Command Default

OAM classes are not specified.

Command Modes

Pseudowire-class (config-pw-class)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to enable the timers in class oam-class3.

```
Router(config-pw-class)# status protocol notification static oam-class3
```

Related Commands

Command	Description
pseudowire-static-oam class	Creates a class that defines the OAM parameters for the pseudowire.

tlv template

To use the pseudowire type, length, value (TLV) parameters created with the **pseudowire-tlv template** command, use the **tlv template** command in VFI neighbor interface configuration mode. To remove the TLV template, use the **no** form of this command.

tlv template *template-name*
no tlv template *template-name*

Syntax Description

template-name	Name of the TLV template that was created with the **pseudowire-tlv template** command.

Command Default

No TLV template is used.

Command Modes

VFI neighbor interface configuration mode (config-vfi-neighbor-interface)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Ensure that you create the template with the **pseudowire-tlv template** command before specifying the template as part of the local interface configuration.

Examples

The following example shows how to use a TLV template called net.

```
Router(config-vfi-neighbor-interface)# tlv template net
```

Related Commands

Command	Description
pseudowire-tlv template	Creates a template of TLV parameters to use in an MPLS-TP configuration.

trace mpls tp

To display the Multiprotocol Label Switching (MPLS) transport protocol (TP) label switched path (LSP) routes that packets take to their destinations, use the **trace mpls tp** command in privileged EXEC mode.

trace mpls tp tunnel-tp *num* **lsp** {**working** | **protect** | **active**}

[**destination** *ip-addr*]

[**exp** *num*]

[**flags fec**]

[reply dscp *num* | **mode control channel**]

[**source** *ip-addr*]

[**timeout** *num*]

[**ttl** *num*]

[**verbose**]

Syntax Description

tunnel-tp *num*	Specifies the MPLS-TP tunnel number.
lsp {**working** | **protect** | **active**}	Specifies the type of MPLS-TP label switched path (LSP) on which to send echo request packets.
destination *ip-addr*	(Optional) Specifies a network 127 address.
exp *num*	(Optional) Specifies the MPLS experimental field value in the MPLS header for an MPLS echo reply. Valid values are from 0 to 7. Default is 0.
flags fec	(Optional) Allows Forward Equivalence Class (FEC) checking on the transit router. A downstream map TLV containing the correct received labels must be present in the echo request for target FEC stack checking to be performed. Target FEC stack validation is always done at the egress router. Be sure to use this keyword in conjunction with the ttl keyword.
reply dscp *num* |**mode control channel**	(Optional) Provides the capability to request a specific quality of service (QoS) in an echo reply by providing a differentiated services code point (DSCP) value. The echo reply is returned with the IP header type of service (ToS) byte set to the value specified in the **reply dscp** command.
size *num*	Specifies the packet size.
source *ip-addr*	(Optional) Specifies the source address or name. The default address is loopback0. This address is used as the destination address in the MPLS echo response.
timeout *num*	(Optional) Specifies the timeout interval in seconds for an MPLS request packet. The range is from 0 to 3600. The default is 2 seconds.

ttl *num*	(Optional) Specifies a time-to-live (TTL) value. The default is 225 seconds.
verbose	(Optional) Enables verbose output mode.

Command Default

Connectivity is not checked.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use the **trace mpls tp** command to validate, test, or troubleshoot MPLS TP LSPs.

Note The **trace mpls tp** command does not support interactive mode.

You can use ping and trace in an MPLS-TP network without IP addressing. However, no IP addresses are displayed in the output.

The following rules determine the source IP address:

1. Use the IP address of the TP interface
2. Use the global router ID.
3. Use router-id : A.B.C.D local node id in IPv4 address format. This is not an IP address. However, it is better to use a value rather than leave it as 0.0.0.0 and risk the packet being deemed invalid and dropped.

Examples

The following example checks connectivity of an MPLS-TP LSP:

```
Router# trace mpls tp tunnel-tp 1 lsp working verbose
```

```
Tracing MPLS TP Label Switched Path on Tunnel-tp1, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
  0 1.1.1.5 127.0.0.1 MRU 1500 [Labels: 444 Exp: 0]
```

```
I 1 0.0.0.0 127.0.0.1 MRU 1500 [Labels: 300/13 Exp: 0/0] 1 ms, ret code
6
! 2 0.0.0.0 1 ms, ret code 3
```

Related Commands

Command	Description
ping mpls tp	Checks MPLS-TP LSP connectivity.

Pseudowire Command Reference

This chapter describes commands used to configure the pseudowire.

backup delay

To specify how long a backup pseudowire virtual circuit (VC) must wait before resuming operation after the primary pseudowire VC goes down, use the **backup delay** command in xconnect configuration mode.

backup delay *enable-delay* {*disable-delay* | **never**}

Syntax Description

enable-delay	Number of seconds that elapse after the primary pseudowire VC goes down before the secondary pseudowire VC is activated. The range is 0 to 180 seconds. The default value is 0 seconds.
disable-delay	Number of seconds that elapse after the primary pseudowire VC comes up before the secondary pseudowire VC is deactivated. The range is 0 to 180 seconds. The default value is 0 seconds.
never	Indicates that the secondary pseudowire VC will not fall back to the primary pseudowire VC if the primary pseudowire VC becomes available again unless the secondary pseudowire VC fails.

Command Modes

Xconnect configuration (config-if-xconn)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to create a xconnect with one redundant peer. After a switchover to the secondary VC occurs, there will be no fallback to the primary VC unless the secondary VC fails.

```
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-if)# xconnect 10.0.0.1 50 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 50
Router(config-if-xconn)# backup delay 0 never
```

Related Commands

Command	Description
backup peer	Configures a redundant peer for a pseudowire VC.

backup peer

To specify a redundant peer for a pseudowire virtual circuit (VC), use the **backup peer** command in xconnect configuration mode. To remove the redundant peer, use the **no** form of this command.

backup peer *peer-router-ip-addr vcid* [**pw-class** *pw-class-name*]

no backup peer *peer-router-ip-addr vcid*

Syntax Description

peer-router-ip-addr	IP address of the remote peer.
vcid	32-bit identifier of the virtual circuit between the routers at each end of the layer control channel.
pw-class	(Optional) Specifies the pseudowire class.
pw-class-name	(Optional) Name of the pseudowire class.

Command Default

A redundant peer is not established.

Command Modes

Xconnect configuration (config-if-xconn)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The combination of the *peer-router-ip-addr* and *vcid* arguments must be unique on the router.

Examples

The following example shows how to create an MPLS xconnect with one redundant peer.

```
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls

Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# xconnect 10.0.0.1 100 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 200
```

Related Commands

Command	Description
backup delay	Specifies how long the backup pseudowire VC must wait before resuming operation after the primary pseudowire VC goes down.

encapsulation (pseudowire)

To specify an encapsulation type for tunneling Layer 2 traffic over a pseudowire, use the **encapsulation** command in pseudowire class configuration mode.

encapsulation mpls

Syntax Description

mpls	Specifies that MPLS is used as the data encapsulation method.

Command Default

Encapsulation type for tunneling Layer 2 traffic is not configured.

Command Modes

Pseudowire-class configuration (config-pw-class)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to configure MPLS as the data encapsulation method for the pseudowire class ether-pw.

```
Router(config)# pseudowire-class ether-pw
Router(config-pw-class)# encapsulation mpls
```

Related Commands

Command	Description
xconnect	Binds an attachment circuit to a pseudowire for xconnect service and enters xconnect configuration mode.
pseudowire-class	Specifies the name of a pseudowire class and enters pseudowire class configuration mode.

interworking

To enable the L2VPN Interworking feature, use the **interworking** command in pseudowire class configuration mode. To disable the L2VPN Interworking feature, use the **no** form of this command.

interworking {**ethernet** | **vlan**}

no interworking {**ethernet** | **vlan**}

Syntax Description

ethernet	Enables Ethernet frames to be extracted from the attachment circuit and sent over the pseudowire. Ethernet end-to-end transmission is assumed. Attachment circuit frames that do not contain Ethernet frames are dropped. In the case of VLAN, the VLAN tag is removed, which leaves a pure Ethernet frame.
vlan	Enables Ethernet frames and the VLAN tag to be sent over the pseudowire. Ethernet end-to-end transmission is assumed. Attachment circuit frames that do not contain Ethernet frames are dropped.

Command Default

L2VPN interworking is not enabled.

Command Modes

Pseudowire class configuration (config-pw)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to create a pseudowire class configuration that enables the L2VPN Interworking feature.

```
Router(config)# pseudowire-class ip-interworking
Router(config-pw)# encapsulation mpls
Router(config-pw)# interworking ethernet
```

Related Commands

Command	Description
encapsulation mpls	Specifies that MPLS is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire.

l2 vfi point-to-point

To establish a point-to-point Layer 2 virtual forwarding interface (VFI) between two separate networks, use the **l2 vfi point-to-point** command in global configuration mode. To disable the connection, use the **no** form of this command.

l2 vfi *name* **point-to-point**

no l2 vfi *name* **point-to-point**

Syntax Description

name	Name of the connection between the two networks.

Command Default

Point-to-point Layer 2 virtual forwarding interfaces are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

If you disable L2VPN Pseudowire Stitching with the **no l2 vfi point-to-point** command, the virtual circuits (VCs) are deleted.

Examples

The following example shows how to establish a point-to-point Layer 2 VFI.

```
Router(config)# l2 vfi atomvfi point-to-point
```

Related Commands

Command	Description
neighbor (L2VPN Pseudowire Stitching)	Establishes the two routers with which to form a connection.

mpls control-word

To enable the MPLS control word in a static pseudowire connection, use the **mpls control-word** command in xconnect configuration mode. To disable the control word, use the **no** form of this command.

mpls control-word

no mpls control-word

Syntax Description

This command has no arguments or keywords.

Command Default

The control word is included in static pseudowire connections.

Command Modes

Xconnect configuration (config-if-xconn)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command is used when configuring static pseudowires. Because the control word is included by default, it may be necessary to explicitly disable this command in static pseudowire configurations.

When the **mpls control-word** command is used in static pseudowire configurations, the command must be configured the same way on both ends of the connection to work correctly. Otherwise, the provider edge routers cannot exchange control messages to negotiate inclusion or exclusion of the control word.

Examples

The following example shows the how to configure the control word in a static pseudowire connection.

```
Router# configure terminal
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# xconnect 10.131.191.251 100 encapsulation mpls manual pw-class mpls
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
```

Related Commands

Command	Description
mpls label	Configures a static pseudowire connection by defining local and remote pseudowire labels.
xconnect	Binds an attachment circuit to a pseudowire, and configures a static pseudowire.

Command	Description
show mpls l2transport vc	Displays information about virtual circuits and static pseudowires that are enabled to route Layer 2 packets on a router.

mpls label

To configure a static pseudowire connection by defining local and remote circuit labels, use the **mpls label** command in xconnect configuration mode. To remove the local and remote pseudowire labels, use the **no** form of this command.

mpls label *local-pseudowire-label remote-pseudowire-label*

no mpls label

Syntax Description

local-pseudowire-label	Static label that is unused within the range defined by the **mpls label range** command.
remote-pseudowire-label	Value of the local pseudowire label of the peer provider edge router.

Command Default

Default labels are not configured.

Command Modes

Xconnect configuration (config-if-xconn)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command is mandatory when configuring static pseudowires, and must be configured at both ends of the connection.

The **mpls label** command checks the validity of the local pseudowire label and will generate an error message if the label is invalid.

Examples

The following example shows how to configure both ends of a static pseudowire connection.

```
Router# configure terminal
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# no ip address
Router(config-if)# xconnect 10.131.191.251 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 100 150
Router(config-if-xconn)# exit
Router(config-if)# exit
```

```
Router# configure terminal
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# no ip address
Router(config-if)# xconnect 10.132.192.252 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 150 100
Router(config-if-xconn)# exit
Router(config-if)# exit
```

Related Commands

Command	Description
mpls control-word	Enables sending the MPLS control word in a static pseudowire connection.
show mpls l2transport vc	Displays information about virtual circuits and static pseudowires that have been enabled to route Layer 2 packets on a router.
xconnect	Binds an attachment circuit to a pseudowire, and configures a static pseudowire.

mtu

To adjust the maximum packet size or maximum transmission unit (MTU) size, use the **mtu** command in interface configuration mode. To revert the MTU value to its default value, use the **no** form of this command.

mtu bytes

no mtu

Syntax Description

bytes	MTU size, in bytes. The default value is 1500 bytes.

Command Default

The default MTU value for Ethernet is 1500 bytes.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Each interface has a default maximum packet size or MTU size. This number generally defaults to the largest size possible for that interface type.

Examples

The following example shows how to specify a MTU size.

```
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# mtu 1800
```

neighbor (L2VPN Pseudowire Stitching)

To specify the routers that must form a point-to-point Layer 2 virtual forwarding interface (VFI) connection, use the **neighbor** command in L2 VFI point-to-point configuration mode. To disconnect the routers, use the **no** form of this command.

neighbor *ip-address vcid* {**encapsulation mpls** | **pw-class** *pw-class-name*}

no neighbor *ip-address vcid* {**encapsulation mpls** | **pw-class** *pw-class-name*}

Syntax Description

ip-address	IP address of the VFI neighbor.
vc-id	Virtual circuit (VC) identifier.
encapsulation mpls	Specifies the encapsulation type.
pw-class	Specifies the pseudowire type.
pw-class-name	Name of the pseudowire you created when you established the pseudowire class.

Command Default

Routers do not form a point-to-point Layer 2 VFI connection.

Command Modes

L2 VFI point-to-point configuration (config-vfi)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

A maximum of two **neighbor** commands are allowed when you issue the **l2 vfi point-to-point** command.

Examples

The following example shows how to configure a Layer 2 VFI connection.

```
Router(config)# l2 vfi atom point-to-point
Router(config-vfi)# neighbor 10.10.10.10 1 encapsulation mpls
```

Related Commands

Command	Description
l2 vfi point-to-point	Establishes a point-to-point Layer 2 VFI between two separate networks.

preferred-path

To specify the Multiprotocol Label Switching Transport Profile (MPLS-TP) or MPLS Traffic Engineering (MPLS-TE) tunnel path that the traffic uses, use the **preferred-path** command in pseudowire configuration mode. To disable the tunnel path selection, use the **no** form of this command.

preferred-path {**interface tunnel** *tunnel-number* | **peer** {*ip-address* | *host-name*}} [**disable- fallback**]

no preferred-path {**interface tunnel** *tunnel-number* | **peer** {*ip-address* | *host-name*}} [**disable- fallback**]

Syntax Description

interface tunnel *tunnel-number*	Specifies a MPLS–TE or MPLS–TP tunnel interface.
peer *ip-address* | *host-name*	Specifies an IP address or DNS name configured on the peer provider edge (PE) router, which is reachable through a label switched path (LSP).
disable-fallback	(Optional) Disables the router from using the default path when the preferred path is unreachable.

Command Default

The tunnel path selection is not enabled.

Command Modes

Pseudowire configuration (config-pw)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The following guidelines provide more information about using this command:

- This command is available only if the pseudowire encapsulation type is MPLS.
- Tunnel selection is enabled when you exit from pseudowire configuration mode.
- The selected path must be an LSP destined to the peer PE router.
- The selected tunnel must be either an MPLS–TE or MPLS–TP tunnel.
- If you select a tunnel, the tunnel tail-end must be on the remote PE router.
- If you specify an IP address, that address must be the IP address of the loopback interface on the remote PE. The address must have a /32 mask.

Examples

The following example shows how to create a pseudowire class and specifies tunnel 1 as the preferred path.

```
Router(config)# pseudowire-class pw1
Router(config-pw)# encapsulation mpls
Router(config-pw)# preferred-path interface tunnel 1 disable-fallback
```

Related Commands

Command	Description
show mpls l2transport vc	Displays information about the virtual circuits that have been enabled to route Layer 2 packets on a router.

pseudowire-class

To specify the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode, use the **pseudowire-class** command in global configuration mode. To remove a pseudowire class configuration, use the **no** form of this command.

pseudowire-class [*pw-class-name*]

no pseudowire-class [*pw-class-name*]

Syntax Description

pw-class-name	(Optional) Name of a Layer 2 pseudowire class. If you want to configure more than one pseudowire class, you must enter a value for the *pw-class-name* argument.

Command Default

Pseudowire classes are not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The **pseudowire-class** command enables you to configure a pseudowire class template that consists of configuration settings used by all the attachment circuits bound to the class. A pseudowire class includes the following configuration settings:

- Data encapsulation type
- Control protocol
- Sequencing
- IP address of the local Layer 2 interface

After you enter the **pseudowire-class** command, the router switches to pseudowire class configuration mode, where pseudowire settings can be configured.

Examples

The following example shows how to enter pseudowire class configuration mode to configure a pseudowire configuration template named class1.

```
Router(config)# pseudowire-class class1
Router(config-pw)#
```

Related Commands

Command	Description
pseudowire	Binds an attachment circuit to a Layer 2 pseudowire for xconnect service.
xconnect	Binds an attachment circuit to a pseudowire for xconnect service and enters xconnect configuration mode.

pseudowire

To bind an attachment circuit to a Layer 2 pseudowire for xconnect service, use the **pseudowire** command in interface configuration mode.

pseudowire *peer-ip-address vcid* **pw-class** *pw-class-name* [**sequencing** {**transmit** | **receive** | **both**}]

Syntax Description

peer-ip-address	IP address of the remote peer.
vcid	32-bit identifier of the virtual circuit (VC) between the routers at each end of the Layer 2 control channel.
pw-class *pw-class-name*	Specifies the pseudowire class configuration from which the data encapsulation type is taken.
sequencing {transmit | receive | both}	(Optional) Sets the sequencing method to be used for packets received or sent in sessions. • **transmit**—Sets sequencing of data packets received from the session. • **receive**—Sets sequencing of data packets sent into the session. • **both**—Sets sequencing of data packets that are both sent and received from the session.

Command Default

None.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The combination of the *peer-ip-address* and *vcid* arguments must be unique on the router. Each pseudowire configuration must have a unique combination of *peer-ip-address* and *vcid* configuration.

The same *vcid* value that identifies the attachment circuit must be configured using the **pseudowire** command on the local and remote router at each end of a Layer 2 session. The virtual circuit identifier creates the binding between a pseudowire and an attachment circuit.

The **pw-class** *pw-class-name* value binds the pseudowire configuration of an attachment circuit to a specific pseudowire class. In this way, the pseudowire class configuration serves as a template that contains settings used by all attachment circuits bound to it with the **pseudowire** command.

Examples

The following example shows how to bind the attachment circuit to a Layer 2 pseudowire for a xconnect service for the pseudowire class named pwclass1.

```
Router(config-if)# pseudowire 172.24.13.196 10 pw-class pwclass1
```

Related Commands

Command	Description
pseudowire-class	Specifies the name of a pseudowire class and enters pseudowire class configuration mode.

show mpls l2transport binding

To display virtual circuit (VC) label binding information, use the **show mpls l2transport binding** command in privileged EXEC mode.

show mpls l2transport binding [*vc-id* | *ip-address* | **local-label** *number* | **remote-label** *number*]

Syntax Description

vc-id	(Optional) VC label binding information for the specified VC is displayed.
ip-address	(Optional) VC label binding information for the specified VC destination is displayed.
local-label *number*	(Optional) Displays VC label binding information for the specified local assigned label.
remote-label *number*	(Optional) Displays VC label binding information for the specified remote assigned label.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example is a sample output from the **show mpls l2transport binding** command that shows the VC label binding information.

```
Router# show mpls l2transport binding
```

```
Destination Address: 10.5.5.51, VC ID: 108
  Local Label: 16
  Remote Label: 18
```

Related Commands

Command	Description
show mpls l2transport vc	Displays information about virtual circuits and static pseudowires that have been enabled to route Layer 2 packets on a router.

show mpls l2transport vc

To display information about virtual circuits (VCs) and static pseudowires that have been enabled to route Layer 2 packets on a router, use the **show mpls l2transport vc** command in privileged EXEC mode.

show mpls l2transport vc [**vcid** *vc-id-min* | *vc-id-min*] [*vc-id-max*] [**interface** *type number* [*local-circuit-id*]] [**destination** {*ip-address* | *hostname*}] [**detail**] [**pwid** *pw-identifier*] [**stitch** *endpoint endpoint*]

Syntax Description

vcid	(Optional) Displays the VC ID.
vc-id-min	(Optional) Minimum VC ID value. The range is from 1 to 4294967295.
vc-id-max	(Optional) Maximum VC ID value. The range is from 1 to 4294967295.
interface *type number*	(Optional) Displays the interface of the router that has been enabled to transport Layer 2 packets.
local-circuit-id	(Optional) Local circuit number.
destination	(Optional) Displays the remote router.
ip-address	(Optional) IP address of the remote router.
hostname	(Optional) Host name assigned to the remote router.
detail	(Optional) Displays the detailed information about the VCs.
pwid *pw-identifier*	(Optional) Displays the number of a pseudowire for a single VC. The valid entries range from 1 to 4294967295.
stitch *endpoint endpoint*	(Optional) Displays the dynamically stitched pseudowires between the specified endpoints.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

If you do not specify any keywords or arguments, the command displays a summary of all the VCs.

Examples

The following is a sample output from the **show mpls l2transport vc** command that shows information about the interfaces and VCs that have been configured to transport various Layer 2 packets on the router.

```
Router# show mpls l2transport vc
```

```
Local intf     Local circuit    Dest address   VC ID    Status
-----------    --------------   ------------   ------   -------
Te7/2           Eth VLAN 100    47.47.47.47     1        UP
Te7/2           Eth VLAN 300    47.47.47.47     5        UP
```

The following is a sample output that shows information from the **show mpls l2transport vc detail** command.

```
Router# show mpls l2transport vc detail
```

```
Local interface: Gi36/1 up, line protocol up, Eth VLAN 1 up
 Interworking type is Ethernet
 Destination address: 70.70.70.70, VC ID: 1, VC status: down
   Output interface: none, imposed label stack {}
   Preferred path: not configured
   Default path: no route
   No adjacency
 Create time: 4d11h, last status change time: 3d15h
 Signaling protocol: LDP, peer unknown
   Targeted Hello: 80.80.80.80(LDP Id) -> 70.70.70.70, LDP is DOWN, no
binding
   Status TLV support (local/remote)   : disabled/None (no remote binding)

     LDP route watch                   : enabled
     Label/status state machine        : local standby, AC-ready, LnuRnd
     Last local dataplane   status rcvd: No fault
     Last BFD dataplane     status rcvd: Not sent
     Last local SSS circuit status rcvd: No fault
     Last local SSS circuit status sent: DOWN(Hard-down, not-ready)
     Last local  LDP TLV    status sent: None
     Last remote LDP TLV    status rcvd: None (no remote binding)
     Last remote LDP ADJ    status rcvd: None (no remote binding)
   MPLS VC labels: local 1698, remote unassigned
   PWID: 4608
   Group ID: local 0, remote unknown
   MTU: local 9600, remote unknown
   Remote interface description:
 Sequencing: receive disabled, send disabled
 Control Word: On
 VC statistics:
   transit packet totals: receive 0, send 0
   transit byte totals:   receive 0, send 0
   transit packet drops:  receive 0, seq error 0, send 0
```

Related Commands

Command	Description
show mpls l2transport binding	Displays virtual circuit (VC) label binding information.

status redundancy

To designate one pseudowire as the master or slave to display status information for both active and backup pseudowires, use the **status redundancy** command in pseudowire class configuration mode. To disable the pseudowire as the master or slave, use the **no** form of this command.

status redundancy {master | slave}

no status redundancy {master | slave}

Syntax Description

master	Designates the pseudowire to work as the master.
slave	Designates the pseudowire to work as the slave.

Command Default

The pseudowire is in slave mode.

Command Modes

Pseudowire-class configuration mode (config-pw)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

One pseudowire must be the master and the other must be assigned the slave. You cannot configure both the pseudowires as master or slave.

Examples

The following example shows how to designate the pseudowire as the master.

```
Router(config-pw)# status redundancy master
```

status (pseudowire class)

To enable the router to send pseudowire status messages to a peer router, even when the attachment circuit is down, use the **status** command in pseudowire class configuration mode. To disable the pseudowire status messages, use the **no** form of this command.

status

no status

Syntax Description

This command has no arguments or keywords.

Command Default

Pseudowire status messages are sent and received if both routers support the messages.

Command Modes

Pseudowire class configuration (config-pw)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Both the 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.

Examples

The following example shows how to enable the router to send pseudowire status messages to a peer router.

```
Router> enable
Router# configure terminal
Router(config)# pseudowire-class test1
Router(config-pw)# status
Router(config-pw)# encapsulation mpls
```

Related Commands

Command	Description
show mpls l2transport vc	Displays information about virtual circuits (VCs) and static pseudowires that have been enabled to route Layer 2 packets on a router.

switching tlv

To advertise the stitching point type, length, variable (TLV) in the label binding, use the **switching tlv** command in pseudowire class configuration mode. To disable the stitching point TLV, use the **no** form of this command.

switching tlv

no switching tlv

Syntax Description

This command has no arguments or keywords.

Command Default

Stitching point TLV data is advertised to peers.

Command Modes

Pseudowire class configuration (config-pw-class)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The pseudowire stitching point TLV information includes the following information:

- Pseudowire ID of the last pseudowire segment traversed
- Pseudowire stitching point description
- Local IP address of the pseudowire stitching point
- Remote IP address of the last pseudowire stitching point that was crossed or the T-PE router

By default, stitching point TLV data is advertised to peers.

Examples

The following example shows how to enable the display of the pseudowire stitching TLV.

```
Router(config)# pseudowire-class class1
Router(config-pw-class)# switching tlv
```

Related Commands

Command	Description
show mpls l2transport binding	Displays stitching point TLV information.
show mpls l2transport vc	Displays information about virtual circuits (VCs) and static pseudowires that have been enabled to route Layer 2 packets on a router.

vccv

To configure the pseudowire Virtual Circuit Connection Verification (VCCV) control channel (CC) type for pseudowires, use the **vccv** command in pseudowire class configuration mode. To disable a pseudowire VCCV CC type, use the **no** form of this command.

vccv {**control-word** | **router-alert** | **ttl**}

no vccv {**control-word** | **router-alert** | **ttl**}

Syntax Description

control-word	Specifies the CC Type 1: control word.
router-alert	Specifies the CC Type 2: MPLS router alert label.
ttl	Specifies the CC Type 3: MPLS pseudowire label with Time to Live (TTL).

Command Default

The pseudowire VCCV CC type is set to Type 1 (control word).

Command Modes

Pseudowire-class configuration (config-pw-class)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

When an initiating provider edge (PE) device sends a setup request message to a remote PE device, the message includes VCCV capability information. This capability information is a combination of the CC type and the control verification (CV) type. Use the **vccv** command to configure the CC type capabilities of the MPLS pseudowire.

If the CV type for the MPLS pseudowire is set to a type that does not use IP/UDP headers, then you must set the CC type to the CC Type 1: control word.

Examples

The following example shows how to configure the MPLS pseudowire class to use CC Type 1.

```
Router(config)# pseudowire-class bfdclass
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# protocol none
Router(config-pw-class)# vccv control-word
```

Related Commands

Command	Description
bfd-template	Creates a BFD template and enters BFD configuration mode.
pseudowire-class	Specifies the name of the pseudowire class and enters pseudowire class configuration mode.
vccv bfd status signaling	Enables status signaling for VCCV BFD.
vccv bfd template	Enables VCCV BFD for a pseudowire class.

vccv bfd status signaling

To enable status signaling for Bidirectional Forwarding Detection (BFD) over Virtual Circuit Connection Verification (VCCV), use the **vccv bfd status signaling** command in pseudowire class configuration mode. To disable status signaling, use the **no** form of this command.

vccv bfd status signaling

no vccv bfd status signaling

Syntax Description

This command has no arguments or keywords.

Command Default

VCCV BFD status signaling is disabled.

Command Modes

Pseudowire-class configuration (config-pw-class)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use this command to allow BFD to provide status signaling functionality that indicates the fault status of an attachment circuit (AC).

Examples

The following example shows how to enable VCCV BFD status signaling for a pseudowire class.

```
Router(config)# pseudowire-class bfdclass
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# protocol none
Router(config-pw-class)# vccv control-word
Router(config-pw-class)# vccv bfd template bfdtemplate raw-bfd
Router(config-pw-class)# vccv bfd status signaling
```

Related Commands

Command	Description
bfd-template	Creates a BFD template and enters BFD configuration mode.
pseudowire-class	Specifies the name of the pseudowire class and enters pseudowire class configuration mode.
vccv	Configures the pseudowire VCCV CC type for MPLS pseudowires.

Command	Description
vccv bfd template	Enables VCCV BFD for a pseudowire class.

vccv bfd template

To enable BFD over VCCV for a pseudowire class, use the **vccv bfd template** command in pseudowire class configuration mode. To disable VCCV BFD, use the **no** form of this command.

vccv bfd template *name* {**udp** | **raw-bfd**}

no vccv bfd template *name* {**udp** | **raw-bfd**}

Syntax Description

name	Name of the BFD template to use.
udp	(Optional) Enables support for BFD with IP or User Datagram Protocol (UDP) header encapsulation.
raw-bfd	(Optional) Enables support for BFD without IP/UDP header encapsulation.

Command Default

VCCV BFD is not enabled for a pseudowire class.

Command Modes

Pseudowire-class configuration (config-pw-class)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The BFD template specified by the *name* argument is created using the **bfd-template** command, and contains settings for the BFD interval values.

VCCV defines two types encapsulation for VCCV messages to differentiate them from data packets: BFD with IP/UDP headers and BFD without IP/UDP headers. Support for BFD without IP/UDP headers can be enabled only for pseudowires that use a control word.

If the VCCV carries raw BFD, the control word must be set to BFD without IP/UDP headers. BFD without IP/UDP headers enables the system to identify the BFD packet when demultiplexing the control channel.

Examples

The following example shows how to enable the BFD template without support for IP/UDP header encapsulation.

```
Router(config)# pseudowire-class bfdclass
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# protocol none
Router(config-pw-class)# vccv control-word
Router(config-pw-class)# vccv bfd template bfdtemplate raw-bfd
Router(config-pw-class)# vccv bfd status signaling
```

Related Commands

Command	Description
bfd-template	Creates a BFD template and enters BFD configuration mode.
pseudowire-class	Specifies the name of the pseudowire class and enters pseudowire class configuration mode.
vccv	Configures the pseudowire VCCV CC type for pseudowires.
vccv bfd status signaling	Enables status signaling for VCCV BFD.

xconnect

To bind an attachment circuit to a pseudowire, and to configure a static pseudowire, use the **xconnect** command in one of the supported configuration modes. To restore the default values, use the **no** form of this command.

xconnect *peer-ip-address vcid* {**encapsulation** {**mpls** [**manual**]} | **pw-class** *pw-class-name*}[**pw-class** *pw-class-name*] [**sequencing** {**transmit** | **receive** | **both**}]

no xconnect

Syntax Description

peer-ip-address	IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable.
vcid	32-bit identifier of the virtual circuit (VC) between the PE routers.
encapsulation mpls	Specifies MPLS as the tunneling method to encapsulate the data in the pseudowire.
pw-class *pw-class-name*	(Optional) Specifies the pseudowire class for advanced configuration.
sequencing	(Optional) Sets the sequencing method to be used for packets received or sent.
transmit	(Optional) Sequences data packets received from the attachment circuit.
receive	(Optional) Sequences data packets sent into the attachment circuit.
both	(Optional) Sequences data packets that are both sent and received from the attachment circuit.

Command Default

The attachment circuit is not bound to the pseudowire.

Command Modes

Xconnect configuration(config-if-xconn)

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The combination of the *peer-ip-address* and *vcid* arguments must be unique on the router. Each xconnect configuration must have a unique combination of *peer-ip-address* and *vcid* configuration.

The same *vcid* value that identifies the attachment circuit must be configured using the **xconnect** command on the local and remote PE router. The VC ID creates the binding between a pseudowire and an attachment circuit.

The **pw-class** keyword with the *pw-class-name* value binds the xconnect configuration of an attachment circuit to a specific pseudowire class. In this way, the pseudowire class configuration serves as a template that contains settings used by all the attachment circuits bound to it with the **xconnect** command.

Examples

The following example shows how to configure a xconnect service for a TenGigabitEthernet4/1 interface by binding the Ethernet circuit to the pseudowire named 123 with a remote peer 209.165.200.225. The configuration settings in the pseudowire class named vlan-xconnect are used.

```
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# xconnect 209.165.200.225 123 pw-class vlan-xconnect
```

Related Commands

Command	Description
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
mpls control-word	Enables the MPLS control word in a static pseudowire connection.
mpls label	Configures a static pseudowire connection by defining local and remote pseudowire labels.
pseudowire-class	Configures a template of pseudowire configuration settings used by the attachment circuits transported over a pseudowire.

QoS Command Reference

This chapter describes commands used to configure Quality of Service (QoS).

- table-map (value mapping), page 227

bandwidth

To specify or modify the bandwidth allocated for a class belonging to a policy map, use the **bandwidth** command in policy-map class configuration mode. To remove the bandwidth specified for a class, use the **no** form of this command.

bandwidth {*bandwidth-value* | **percent** *x%* | **remaining percent** *x%* | **remaining ratio** *ratio*}

no bandwidth {*bandwidth-value* | **percent** *x%* | **remaining percent** *x%* | **remaining ratio** *ratio*}

Syntax Description

bandwidth value	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.
percent *x%*	Specifies the amount of bandwidth, in percentage from the available bandwidth, to be assigned to the class. The value ranges from 1 to 100 percent.
remaining percent *x%*	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 ranges from 1 to 100 percent.
remaining ratio *ratio*	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.

Command Default

Bandwidth is not specified.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The restrictions and usage guidelines to configure quality of service (QoS) egress bandwidth on a CPT system are as follows:

- Bandwidth action is not supported on classes with match criteria as qos-group 3 or 7, or multicast-priority class.
- The **bandwidth** command cannot be used in combination with Bandwidth Remaining Ratio (BRR) or Bandwidth Remaining Percentage (BRP) in a class-map or a policy-map.
- The system does not validate for the total CIR configured on all the targets under the various congestion points. Therefore, ensure that the total committed information rate (CIR) configured does not exceed the total bandwidth available:
  - Total CIR configured under a 1 Gbps interface shall not exceed 1 Gbps; this includes CIR in policy applied on interface as well as services on that interface.
  - Total CIR configured under a 10 Gbps interface shall not exceed 10 Gbps; this includes CIR in policy applied on interface as well as services on that interface.
  - Total CIR on all targets on a CPT 50 shelf shall not exceed 9.882 Gbps; this is the least bandwidth for a CPT 50 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 shall not exceed 13 Gbps. The same is applicable if two CPT 50 shelves are connected to the two SFP+ interfaces of the same fabric card.

The restrictions and usage guidelines to configure QoS egress bandwidth remaining ratio or bandwidth remaining percent on a CPT system are as follows:

- The **bandwidth remaining ratio and bandwidth remaining percent** command is not supported in combination with bandwidth action in a class-map or a policy-map.
- The **bandwidth remaining ratio and bandwidth remaining percent** command is not supported on classes with match criteria as qos-group 3 or 7 or multicast-priority class

BRR is implemented on logical interfaces using hierarchical policy-maps.

Examples

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
```

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
```

Related Commands

Command	Description
class-map	Creates a class-map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
class-name {*class-name* | **class-default** }	Specifies the name of the class whose policy you want to create or change.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.
show policy-map	Displays the policy-map information.

class

To specify the name of the class whose policy you want to create or change, or to specify the default class (commonly known as the **class-default** class) before you configure its policy, use the **class** command in policy-map configuration mode. To remove a class from the policy map, use the **no** form of this command.

class {*class-name* | **class-default**}

no class {*class-name* | **class-default**}

Syntax Description

class-name	User-defined class name to which the policy applies.
class-default	Specifies that the policy applies to the default traffic class.

Command Default

A class is not specified.

Command Modes

Policy-map configuration (config-pmap)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Within a policy map, the **class** command can be used to specify the name of the class whose policy you want to create or change. First, the policy map must be identified. To identify the policy map (and enter the required policy-map configuration mode), use the **policy-map** command before you use the **class** (policy-map) command. After you specify a policy map, you can configure the policy for new classes or modify the policy for any existing classes in that policy map.

The class name that you specify in the policy map ties the characteristics for that class—that is, its policy—to the class map and its match criteria, as configured using the **class-map** command.

The **class-default** keyword is used to specify the predefined default class called class-default. The class-default class is the class to which traffic is directed if that traffic does not match any of the match criteria in the configured class maps.

Examples

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 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 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
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
police [cir | rate] *bps-value* **[bc | burst]** *bc* **[be | peak-burst]** *be* **conform-action** *action* **exceed-action** *action* **violate-action** *action*	Specifies a maximum bandwidth usage by a traffic class through the use of a token bucket algorithm.
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).
police [cir | rate] percent *%* **[bc | burst]** *bc* **[be | peak-burst]** *be* **conform-action** *action* **exceed-action** *action* **violate-action** *action*	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.

class-map

To create a class map to be used for matching packets to a specified class, use the **class-map** command in global configuration mode. To remove an existing class-map from the router, use the **no** form of this command. The **class-map** command enters class-map configuration mode in which you can enter one of the **match** commands to configure the match criteria for this class.

class-map [match-any] *class-map-name*

no class-map [match-any] *class-map-name*

Syntax Description

[match-any]	(Optional) 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	Name of the class for the class-map. This argument is used for both the class-map and to configure a policy for the class in the policy map. The class name cannot contain spaces and can have a maximum of 40 alphanumeric characters.

Command Default

Class-map is not configured by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use the **class-map** command to specify the class that you create or modify to meet the class-map match criteria. This command enters class-map configuration mode where you can enter one of the match commands to configure the match criteria for this class. Packets that arrive at either the input interface or the output interface (determined by how the **service-policy** command is configured) are checked against the match criteria configured for a class-map to determine if the packets belong to that class.

In the class-map configuration mode, the following configuration commands are available:

- **exit**—Used to exit from class-map configuration mode.
- **no**—Used to remove a match statement from a class-map.
- **match**—Used to configure classification criteria. The optional match subcommands and the description are listed in this table.

Command	Description
match cos *cos-number* **Example:** Router(config-cmap)# match cos 2	Matches a packet on the basis of a Layer 2 class of service (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.
match ip dscp *ip- dscp-value* **Example:** Router(config-cmap)# match ip dscp 6	Identifies a specific IP differentiated services code point (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 Multiprotocol Label Switching (MPLS) experimental (EXP) value in the topmost label. • *exp-value* — MPLS EXP value. The value can range from 0 to 7.

Examples

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 a configure 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 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
```

Related Commands

Command	Description
class class-default	Specifies that the policy applies to the default traffic class.

Command	Description
class *class-name*	User-defined class name to which the policy applies.
match cos	Matches a packet on the basis of a Layer 2 CoS number.
match ip precedence	Identifies the IP precedence value as match criteria.
match ip dscp	Identifies a specific IP DSCP value as a match criterion.
match mpls experimental topmost	Matches the MPLS EXP value in the topmost label.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
show class-map	Displays the class-map information.

match ip precedence

To specify the IP precedence values to use as the match criteria, use the **match ip precedence** command in the class-map configuration mode. To remove IP precedence values from a class map, use the **no** form of this command.

match [ip] precedence *ip-precedence-value*

no match [ip] precedence *ip-precedence-value*

Syntax Description

ip	(Optional) Specifies that the match is for IPv4 packets.
ip-precedence-value	IP precedence value. The value can range from 0 to 7. You can enter up to four different values, separated by a space.

Command Default

IP precedence values are not configured as the match criteria.

Command Modes

Class-map configuration mode (config-cmap)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

You can enter up to four matching criteria, separated by a space, in one **match ip precedence** statement.

Examples

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
```

Related Commands

Command	Description
class-map	Creates a class-map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy-map that can be attached to one or more targets to specify a service policy.

Command	Description
service-policy (service configuration)	Attaches a policy-map to an input or an output target.
show class-map	Displays all class-maps and their matching criteria.
set ip precedence	Marks the precedence value in the IP header with a value between 0 to 7.

match cos

To match a packet on the basis of a Layer 2 class of service (CoS) marking, use the **match cos** command in class-map configuration mode. To remove a specific Layer 2 CoS marking as a match criterion, use the **no** form of this command.

match cos *cos-number*

no match cos *cos-number*

Syntax Description

cos-number	Packet CoS bit value. Specifies that the packet CoS bit value must match the specified CoS value. The value can range from 0 to 7. You can enter up to four different values, separated by a space.

Command Default

Packets are not matched on the basis of a Layer 2 CoS marking.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

You can enter up to four matching criteria, separated by a space, in one **match cos** statement.

Examples

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
```

Related Commands

Command	Description
class-map	Creates a class-map to be used for matching packets to a specified class.

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
show class-map	Displays all class-maps and their matching criteria.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
service-policy (service configuration)	Attaches a policy-map to an input or an output target.

match ip dscp

To specify one or more differentiated service code point (DSCP) values as a match criterion, use the **match ip dscp** command in the class-map configuration mode. To remove a specific DSCP value from a class map, use the **no** form of this command.

match [ip] dscp *ip- dscp-value*

no match [ip] dscp *ip- dscp-value*

Syntax Description

ip	(Optional) Specifies that the match is for IPv4 packets.
ip- dscp-value	IP DSCP value. The value can range from 0 to 63. You can enter up to eight different values, separated by a space.

Command Default

DSCP values are not configured as the match criteria.

Command Modes

Class-map configuration mode (config-cmap)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

You can enter up to eight IP DSCP values, separated by a space, in one **match ip dscp** statement.

Examples

The following example shows how to set multiple match criteria; in this case, two IP DSCP value:

```
Router# enable
Router# configure terminal
Router(config)# class-map ipdscp5
Router(config-cmap)# match ip dscp 1 5
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
service-policy	Attaches a policy map to an input or an output target.

Command	Description
show class-map	Displays all class-maps and their matching criteria.
set ip dscp	Marks the precedence value in the IP header with a value between 0 to 63.

match mpls experimental topmost

To match the Multiprotocol Label Switching (MPLS) experimental (EXP) value in the topmost label header, use the **match mpls experimental topmost** command in the class-map configuration mode. To remove the EXP match criterion, use the **no** form of this command.

match mpls experimental topmost *exp-value*

no match mpls experimental topmost *exp-value*

Syntax Description

exp-value	MPLS EXP value in the topmost label. You can enter up to eight different values, separated by a space.

Command Default

MPLS EXP values are not configured as the match criteria.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Ingress marking of the MPLS EXP bit for MPLS traffic is not supported. Egress MPLS EXP marking is supported only in the interface mode of an MPLS interface.

Examples

The following example shows how to match the MPLS EXP value 3 in the topmost label header:

```
Router(config-cmap)# match mpls experimental topmost 3
```

Related Commands

Command	Description
platform set mpls-exp-topmost from qos-group, discard-class table	(Only for VPWS initiation and LSR scenarios) Maps the MPLS-EXP value from the table map.

match qos-group

To match a packet on the basis of traffic class represented by the qos-group, use the **match qos-group** command in the class-map configuration mode. To remove the group-group value, use the **no** form of this command.

match qos-group *qos-group-value*

no match qos group *qos-group-value*

Syntax Description

qos-group-value	Matches a packet on the basis of traffic class represented by the qos-group. The value can range from 0 to 7.

Command Default

A qos-group is not configured as the match criteria.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The **match qos-group** command is used by the class-map to identify a specific QoS group value marking on a packet. This command is supported only at the egress.

Examples

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
```

Related Commands

Command	Description
class-map	Creates a class-map to be used for matching packets to a specified class.

Command	Description
class-name {*class-name* | **class-default** }	Specifies the name of the class whose policy you want to create or change
policy-map	Creates or modifies a policy-map that can be attached to one or more targets to specify a service policy.

platform

To associate table maps at the egress to an interface for Virtual Private Wire Service (VPWS) initiation and Label Switching Router (LSR) scenarios use the **platform set mpls-exp-topmost from qos-group, discard-class table** *table-map-name* command in the service configuration mode. To remove the table maps from the interface at egress, use the **no** form of the command.

platform set mpls-exp-topmost from qos-group, discard-class table *table-map-name*

no platform set mpls-exp-topmost from qos-group, discard-class table *table-map-name*

To associate table maps at the egress to an interface for Virtual Private Wire Service (VPWS) termination use the **platform set cos from qos-group, discard-class table** *table-map-name table-map-name* command in the service configuration mode. To remove the table maps from the interface at egress, use the **no** form of the command .

platform set cos from qos-group, discard-class table *table-map-name*

no platform set cos from qos-group, discard-class table *table-map-name*

Syntax Description

set mpls-exp-topmost from qos-group, discard-class	(Only for VPWS initiation and LSR scenarios) Maps the Multiprotocol Label Switching (MPLS) experimental (EXP) value from the table map.
set cos from qos-group, discard-class	(Only for VPWS termination scenario) Maps the VLAN CoS value from the table map.
table *table-map-name*	Indicates the use of table-map. *table-map-name* —Name of the table-map.

Command Default

The table-maps are not associated to the interface.

Command Modes

Service configuration mode (config-if-srv-instance).

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command is used only during the VPWS initiation, LSR, and VPWS termination scenarios. The **platform set cos from qos-group** command is accepted at the service instance level.

Examples

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
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
class-name	Specifies the name of the class whose policy you want to create or change.
map from *from-value1, from-value2* **to** *to-value*	Maps the QoS-group and discard values to the MPLS EXP or VLAN COS bit.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
show table-map	Displays the configuration of a specified table map or all table maps.
set qos-group	Marks a QoS group identifier (ID) with a value between 0 to 7 that can be used later to classify packets.
set discard-class	Sets the discard-class internal label to a specified value between 0 to 2. This command is supported only during table-map creation.
service-policy	Attaches a policy map to an input or an output target.
table-map	Creates or specifies the name of the table map.

police (policy map)

To create a policer and configure the policy-map class to use it, use the **police** command in policy-map class configuration mode. To delete the policer from the policy-map class, use the **no** form of this command.

police [cir | rate] *bps-value* **[bc | burst]** *bc* **[be | peak-burst]** *be* **[conform-action** *action***] [exceed-action** *action* **] [violate-action** *action* **]**

no police [cir | rate] *bps-value* **[bc | burst]** *bc* **[be | peak-burst]** *be* **[conform-action** *action***] [exceed-action** *action* **] [violate-action** *action* **]**

Police (percent):

police [cir | rate] percent *%* **[bc | burst]** *bc* **[be | peak-burst]** *be* **[conform-action** *action***] [exceed-action** *action* **] [violate-action** *action* **]**

no police [cir | rate] percent *%* **[bc | burst]** *bc* **[be | peak-burst]** *be* **[conform-action** *action***] [exceed-action** *action* **] [violate-action** *action* **]**

Police (two-rate):

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* **]**

no 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* **]**

Syntax Description

cir	Specifies the committed information rate (CIR) used for policing traffic.
rate	Specifies the police rate used for policing traffic.
bps value	Average rate in bits per second. The valid values range from 8000 to 10000000000 seconds.
bc	Specifies the committed (conform) burst size used for policing traffic.
burst	Specifies the burst size used for policing traffic.
bc	Committed (conform) burst size or burst size in bytes. The valid values range from 1000 to 256000000. **Note** The burst size must be in milli-seconds or micro-seconds while using police (percent) command.
pir	Specifies the peak information rate (PIR) used for policing traffic.
peak-rate	Specifies the peak rate used for policing traffic.
pir	Peak information rate or peak rate in bits per second. The valid values range from 8000 to 10000000000 seconds.

be	Specifies the excess burst size used for policing traffic.
peak-burst	Specifies the peak-burst size used for policing traffic.
be	Excess burst size or peak-burst size in bytes. The valid values range from 1000 to 256000000 bytes. **Note** The burst size must be in milli-seconds or micro-seconds while using police (percent) command.
conform-action	Action to take on packets whose rate is less than the conform burst. You must specify a value for peak-burst-in-msec before you specify the conform-action.
exceed-action	Action to take on packets whose rate is within the conform and conform plus exceed burst.
violate-action	Action to take on packets whose rate exceeds the conform plus exceed burst. You must specify the exceed-action before you specify the violate-action.
action	Action taken on a packet when it conforms, exceeds, or violates the interface bandwidth: • 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 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.
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.

Command Default

Policing is not configured.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
9.3.0	This command was introduced

Usage Guidelines

The **police** command specifies the maximum bandwidth used by a traffic class through the use of a token bucket algorithm. The **police (percent)** command calculates the CIR on the basis of a percentage of the maximum amount of bandwidth available on the interface. When a policy map is attached to the interface, the equivalent CIR value in bits per second (bps) is calculated on the basis of the interface bandwidth and the percent value entered with this command. The police (two-rate) command configures traffic policing using two-rates, the CIR and the PIR.

Examples

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 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#
```

Related Commands

Command	Description
class-map	Creates a class-map to be used for matching packets to a specified class.
class-name {*class-name* | **class-default** }	Specifies the name of the class whose policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
show policy-map	Displays the policy-map information.

policy-map

To enter policy-map configuration mode and create or modify a policy map that can be attached to one or more targets to specify a service policy, use the **policy-map** command in the global configuration mode. To delete a policy map, use the **no** form of this command.

policy-map *policy-map-name*

Syntax Description

policy-map-name	Policy map name. This is the name of the policy map and can have a maximum of 40 alphanumeric characters.

Command Default

The policy map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use the **policy-map** command to specify the name of the policy map to be created, added, or modified before you configure policies for classes whose match criteria are defined in a class map. The **policy-map** command enters policy-map configuration mode, in which you can configure or modify the class policies for a policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. Use the **class-map** and **match** commands to configure match criteria for a class.

Examples

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 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
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
class-name { *class-name* | **class-default** }	Specifies the name of the class whose policy you want to create or change
police [cir | rate] *bps-value* **[bc | burst]** *bc* **[be | peak-burst]** *be* **conform-action** *action* **exceed-action** *action* **violate-action** *action*	Specifies a maximum bandwidth usage by a traffic class through the use of a token bucket algorithm.
police [cir | rate] percent *%* **[bc | burst]** *bc* **[be | peak-burst]** *be* **conform-action** *action* **exceed-action** *action* **violate-action** *action*	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
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).
show policy-map	Displays the policy-map information.
service-policy	Attaches a policy map to an input or an output target.

priority

To give priority to a class of traffic belonging to a policy map, use the **priority** command in the policy-map class configuration mode. To remove a previously specified priority for a class, use the **no** form of this command.

priority [*bandwidth-value*] **[percent** *x%* **]**

no priority [*bandwidth-value*] **[percent** *x%* **]**

Syntax Description

bandwidth value	Maximum bandwidth uses 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.
percent	Specifies that the amount of guaranteed bandwidth is specified by the percentage of available bandwidth.
x%	Rate of traffic that is given low latency handling of *x%* of the parent interface bandwidth or *x%* parent class committed information rate (CIR) if policy not applied on an interface. The percentage can be a number from 1 to 100.

Command Default

Priority is not set.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The **priority** command enables the rate-limit option to ensure that a particular rate is not exceeded. However, in the CPT system, egress rate limiting is achieved using shapers that can cause additional delays. Hence it is advised to ensure that for low latency queuing traffic, rate limiting is done at ingress, and the rates specified at egress are just placeholders and are never hit. Hitting the rate limit at egress would mean increased latencies for low latency queuing traffic. The **priority** command is supported only under class-map with match qos-group 3 or 7 and multicast-priority class.

Examples

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
```

Related Commands

Command	Description
class-map	Creates a class-map to be used for matching packets to a specified class.
class-name { *class-name* | **class-default** }	Specifies the name of the class whose policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.
show policy-map	Displays the policy-map information.

service-policy

To attach a traffic policy to a target and to specify the direction in which the policy should be applied (either on packets coming into the target or packets leaving the target), use the **service-policy** configuration command. Only one traffic policy can be applied to an interface in a given direction. To detach a traffic policy from a target, use the **no** form of this command.

service-policy {input | output} *policy-map-name*

no service-policy {input | output} *policy-map-name*

Syntax Description

input	Attaches the policy-map to the input target.
output	Attaches the policy-map to the output target.
policy-map-name	Name of a service policy map (created using the policy-map command) to be attached. The name can be a maximum of 40 alphanumeric characters.

Command Default

A service policy is not specified nor a policy map is attached.

Command Modes

Service configuration mode (config-if-srv-instance).

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The **input** and **output** keywords indicate the direction in which the policy map is applied. The value for the *policy-map-name* argument represents a quality of service (QoS) policy map configured on the CPT system using the **policy-map** *policy-map-name* global configuration command. The policy-map must already exist and must contain the QoS feature to be applied to the target, according to the provisions specified by the service level agreement (SLA).

Examples

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
```

Related Commands

Command	Description
class-map	Creates a class-map to be used for matching packets to a specified class.
class-name {*class-name* | **class-default** }	Specifies the name of the class whose policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.
show policy-map	Displays the policy-map information.

set cos

To set the Layer 2 class of service (CoS) value of a packet, use the **set cos** command in the policy-map class configuration mode. To remove a specific CoS value setting, use the **no** form of this command.

set cos *cos-value*

no set cos

Syntax Description

cos-value	CoS value between 0 to 7 in an 802.1Q tagged frame.

Command Default

This command is disabled by default.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

For Multiprotocol Label Switching (MPLS) traffic flows, the **set cos** command can be used only in service policies that are attached in the output direction of an interface. Packets entering an interface cannot be set with a CoS value.

For Ethernet virtual circuit (EVC) traffic flows, the **set cos** command can be used only in service policies that are attached in the input direction of an interface.

Examples

The following example shows how to create 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 cos value:

```
Router# enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set cos 1
```

Related Commands

Command	Description
class-map	Creates a class-map to be used for matching packets to a specified class.

Command	Description
class-name {*class-name* | **class-default** }	Specifies the name of the class whose policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
set ip precedence	Marks the IP precedence in the ToS byte with a value between 0 to 7.
set ip dscp	Marks the IP DSCP in the ToS byte with a value between 0 to 63.
set qos group	Marks a QoS group ID with a value between 0 to 7 that can be used later to classify packets.
set discard-class	Sets the discard-class internal label to a specified value between 0 to 2. This command is supported only during table-map creation.

set discard-class

To mark a packet with a discard-class value, use the **set discard-class** command in policy-map class configuration mode. To remove the marked discard-class value of a packet, use the **no** form of this command.

set discard-class *value*

no set discard-class *value*

Syntax Description

value	Discard-class internal label to a specified value. This is a value specified between 0 to 2. This command is supported only during table-map creation.

Command Default

This command is disabled by default.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command is supported only during table-map creation.

Examples

The following example shows the usage of **set discard-class** command:

```
!Ingress policy-map for pseudo-wire initiation
policy-map IngressPolicyMap
 class IngressClassmap1
  set qos-group 1
  set discard-class 0
 class IngressClassmap2
  set qos-group 2
  set discard-class 1
 class IngressClassmap3
  set qos-group 3
  set discard-class 2
 class IngressClassmap4
  set qos-group 4
  set discard-class 0
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.

Command	Description
class-name {*class-name* | **class-default** }	Specifies the name of the class whose policy you want to create or change.
map from *from-value1, from-value2* **to** *to-value*	Maps the QoS-group and discard values to the MPLS EXP or VLAN COS bit.
platform set mpls-exp-topmost from qos-group, discard-class table *table-map-name*	(Only for VPWS initiation and LSR scenarios) Maps the MPLS-EXP value from the table map.
platform set cos from qos-group, discard-class table *table-map-name*	(Only for VPWS termination scenario) Maps the VLAN CoS value from the table map.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
set qos-group *qos group value*	Marks a QoS group identifier (ID) with a value between 0 to 7 that can be used later to classify packets.
service-policy	Attaches a policy map to an input or an output target.
table-map *table-map-name*	Creates or specifies the name of the table map.

set ip dscp

To mark a packet by setting the IP differentiated services code point (DSCP) value in the type of service (ToS) byte, use the **set ip dscp** command in policy-map class configuration mode. To remove a previously set IP DSCP value, use the **no** form of this command.

set ip dscp *ip-dscp-value*

no set ip dscp

Syntax Description

ip-dscp-value	Marks the IP DSCP in the ToS byte with a value between 0 to 63.

Command Default

This command is disabled by default.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The **set ip dscp** command cannot be used with the **set ip precedence** command to mark the same packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

Examples

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 DSCP value:

```
Router# enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip dscp 7
```

Related Commands

Command	Description
class-map	Creates a class-map to be used for matching packets to a specified class.

Command	Description
class-name { *class-name* | **class-default** }	Specifies the name of the class whose policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
set cos	Marks the CoS value between 0 to 7 in an 802.1Q tagged frame
set ip precedence	Marks the IP precedence in the ToS byte with a value between 0 to 7.
set qos group	Marks a QoS group ID with a value between 0 to 7 to classify packets.
set discard-class	Sets the discard-class internal label to a specified value between 0 to 2. This command is supported only during table-map creation.

set ip precedence

To set the precedence value in the IP header, use the **set ip precedence** command in the policy-map class configuration mode. To leave the precedence value at the current setting, use the **no** form of this command.

set ip precedence *ip-precedence-value*

no set ip precedence

Syntax Description

ip-precedence-value	Marks the precedence value in the IP header with a value between 0 to 7.

Command Default

This command is disabled by default.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The **set ip precedence** command cannot be used with the **set ip dscp** command to mark the same packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

Examples

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
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
class-name { *class-name* **| class-default }**	Specifies the name of the class whose policy you want to create or change.

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
set cos *cos value*	Marks the CoS value between 0 to 7 in an 802.1Q tagged frame.
set ip dscp *ip dscp value*	Marks the IP DSCP in the ToS byte with a value between 0 to 63.
set qos group *qos group value*	Marks a QoS group identifier (ID) with a value between 0 to 7 that can be used later to classify packets.
set discard-class *value*	Sets the discard-class internal label to a specified value between 0 to 2. This command is supported only during table-map creation.

set qos-group

To set a quality of service (QoS) group ID to classify packets, use the **set qos-group** command in the policy-map class configuration mode. To remove the group ID, use the **no** form of this command.

set qos-group *qos-group-value*

no set qos-group *qos-group-value*

Syntax Description

qos-group-value	Marks a QoS group identifier (ID) with a value between 0 to 7 is used to classify packets.

Command Default

This command is disabled by default.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The **set qos-group** command enables you to associate a group ID with a packet.

Examples

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 qos-group value:

```
Router# enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set qos-group 1
```

Related Commands

Command	Description
class-map	Creates a class-map to be used for matching packets to a specified class.
class-name { *class-name* | **class-default** }	Specifies the name of the class whose policy you want to create or change.

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
set cos	Marks the CoS value between 0 to 7 in an 802.1Q tagged frame.
set ip dscp	Marks the IP DSCP in the ToS byte with a value between 0 to 63.
set ip precedence	Marks the IP precedence in the ToS byte with a value between 0 to 7.
set discard-class	Sets the discard-class internal label to a specified value between 0 to 2. This command is supported only during table-map creation.

shape

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, use the **shape** command in the policy-map class configuration mode. To remove shaping and leave the traffic unshaped, use the **no** form of this command.

shape {average percent *x%* **| average** *cir -value***}**

no shape {average percent *x%* **| average** *cir -value***}**

Syntax Description

average percent *x%*	Shapes a class to a percentage of visible bandwidth. • *%*—Percentage. The value should range from 1 to 100.
average *cir-value*	Specifies the average rate of traffic shaping. • *cir-value*—Committed information rate (CIR) value in bps. The committed information rate (CIR) value ranges from 8000 to 10000000000 bps.

Command Default

Shaping is not specified.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
9.3.0	This command was introduced.

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 match criteria as qos-group 3 or 7, 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.

Examples

The following example shows how to enable 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
```

The following example shows how 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
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
class-name { *class-name* | **class-default** }	Specifies the name of the class whose policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.
show policy-map	Displays the policy-map information.

show class-map

To display class maps and their matching criteria, use the **show class-map** command in user EXEC or privileged EXEC mode.

show class-map [*class-map-name*]

Syntax Description

class-map-name	(Optional) Name of the class-map. The class-map name can be a maximum of 40 alphanumeric characters.

Command Default

All class maps are displayed.

Command Modes

User EXEC (>), Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

You can use the **show class-map** command to display all class maps and their matching criteria. If you enter the optional *class-map-name* argument, the specified class map and its matching criteria will be displayed.

Examples

The following is a sample output from the show class-map command displaying a specific class map:

```
Router# show class-map ipp5
```

```
class Map match-any ipp5 (id 1)
match ip precedence 5
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.

show policy-map

To display the configuration of all classes for a specified service policy map or of all classes for all existing policy maps, use the **show policy-map** command in user EXEC or privileged EXEC mode.

show policy-map [*policy-map-name*]

Syntax Description

policy-map	(Optional) Name of the service policy map whose complete configuration is to be displayed. The name can be a maximum of 40 characters.

Command Default

All existing policy map configurations are displayed.

Command Modes

User EXEC (>) and Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The **show policy-map** command displays the configuration of a policy map created using the **policy-map** command. You can use the **show policy-map** command to display all class configurations comprising any existing service policy map, whether or not that policy map has been attached to an interface.

Examples

The following is a sample output from the **show policy-map** command that displays police actions on separate lines:

```
Router# show policy-map Premium
```

```
Policy Map Premium
Class P1
priority
police percent 50 25 ms 0 ms
conform-action transmit
exceed-action transmit
violate-action drop
```

Related Commands

Command	Description
class-map	Creates a class-map to be used for matching packets to a specified class.

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.

show policy-map class

To display the configuration for the specified class of the specified policy map, use the **show policy-map class** command in user EXEC or privileged EXEC mode.

show policy-map *policy-map-name* **class** *class-name*

Syntax Description

policy-map-name	Name of a policy map that contains the class configuration to be displayed.
class-name	Name of the class whose configuration is to be displayed.

Command Default

This command displays the class configuration for any service policy map.

Command Modes

User EXEC (>), Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

You can use the **show policy-map class** command to display any single class configuration for any service policy map, whether or not the specified service policy map has been attached to an interface.

Examples

The following is a sample output from the **show policy-map class** command displaying configurations for the class called class7 that belongs to the policy map called po1:

```
Router# show policy-map po1 class class7
```

```
Class class7
Bandwidth 937 (kbps) Max Thresh 64 (packets)
```

Related Commands

Command	Description
class-map	Creates a class-map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.

Command	Description
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.

show policy-map interface

To display the statistics and the configurations of the input and output policies that are attached to an interface, use the **show policy-map interface** command in user EXEC or privileged EXEC mode.

show policy-map interface *interface-type interface-number*

Syntax Description

interface-type	Type of interface
interface-number	Interface number.

Command Default

This command displays the packet statistics of all classes that are configured for all service policies on the specified interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The **show policy-map interface** command displays the packet statistics for classes on the specified policy-map interface only if a service policy has been attached to the interface.

Examples

The following is a sample output from the **show policy-map interface** command:

```
Router# show policy-map interface ten 2/4
```

```
Limited counter support. Refer documentation for details.
 TenGigabitEthernet2/4

  Service-policy output: Egress

  Counters last updated 00:00:20 ago

    Class-map: EgressClassmap1 (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 1
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      queue limit 352 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
```

```
      shape (average) cir 10000000, bc 40000, be 40000
      target shape rate 10000000
```

Related Commands

Command	Description
class-map	Creates a class-map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.

table-map (value mapping)

To create a table-map that is used for mapping the values from qos-group and discard-class to the Multiprotocol Label Switching (MPLS) experimental (EXP) or Ethernet class of service (CoS) bit at egress use the **table-map** (value mapping) command in the global configuration mode. To disable the use of this table map, use the **no** form of this command. .

table-map *table-map-name* **map from** *from-value1, from-value2* **to** *to-value*

no table-map *table-map-name* **map from** *from-value1, from-value2* **to** *to-value*

Syntax Description

table-map-name	Name of the table-map. This can have a maximum of 40 alphanumeric characters.
map from	Indicates that a “map from” value is used. 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	Indicates that a “map to” value is used. Maps the QoS-group and discard values to the MPLS EXP or VLAN CoS bit.
to-value	Value of the MPLS EXP or VLAN CoS bits, which can range from 0 to 7.

Command Default

Table-map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

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.

Examples

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
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
class-name {*class-name* | **class-default** }	Specifies the name of the class whose policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to one or more targets to specify a service policy.
platform set mpls-exp-topmost from qos-group, discard-class table	(Only for VPWS initiation and LSR scenarios) Maps the MPLS-EXP value from the table map.
platform set cos from qos-group, discard-class table	(Only for VPWS termination scenario) Maps the VLAN CoS value from the table map.
show table-map	Displays the configuration of a specified table map or all table maps.
set qos-group	Marks a QoS group ID with a value between 0 to 7 that can be used later to classify packets.
set discard-class	Sets the discard-class internal label to a specified value between 0 to 2. This command is supported only during table-map creation.

High Availability Command Reference

This chapter describes commands to configure high availability.

crashdump-timeout

To set the longest time that the newly active fabric card waits before reloading the previously active fabric card, use the **crashdump-timeout** command in redundancy mode. To reset the default time that the newly active fabric card waits before reloading the previously active fabric card, use the **no** form of this command.

crashdump-timeout [*mm* | *hh:mm*]

Syntax Description

mm	(Optional) Time, in minutes, that the newly active fabric card waits before reloading the previously active fabric card. The range is from 5 to 1080 minutes.
hh:mm	(Optional) Time, in hours and minutes, that the newly active fabric card waits before reloading the previously active fabric card. The range is from 5 minutes to 18 hours.

Command Default

The default timeout for this command is 5 minutes.

Command Modes

Redundancy mode (config-red)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use this command to specify the length of time that the newly active fabric card waits before reloading the previously active fabric card.

Examples

The following example shows how to set the time before the previously active fabric card is reloaded.

```
Router(config-red)# crashdump-timeout 10
```

network area

To define the interfaces on which Open Shortest Path First (OSPF) protocol runs and to define the area ID for those interfaces, use the **network area** command in router configuration mode. To disable OSPF routing for the interfaces, use the **no** form of this command.

network *ip-address wildcard-mask* **area** *area-id*
no network *ip-address wildcard-mask* **area** *area-id*

Syntax Description

ip-address	IP address.
wildcard-mask	Wild card mask address.
area-id	Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. To associate areas with IP subnets, specify a subnet address as the value of the *area-id* argument.

Command Default

This command is disabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The *ip-address* and *wildcard-mask* arguments together enable one or multiple interfaces to be associated with a specific OSPF area using a single command. To associate areas with IP subnets, specify a subnet address as the value of the *area-id* argument.

Examples

The following example shows how to initialize OSPF routing process 109, and defines four OSPF areas.

```
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# ip address 209.165.200.225 255.255.255.0
Router(config)# router ospf 109
Router(config-router)# network 209.165.200.226 0.0.0.255 area 10.9.50.0
Router(config-router)# network 209.165.200.227 0.0.255.255 area 2
Router(config-router)# network 209.165.200.228 0.0.0.255 area 3
Router(config-router)# network 0.0.0.0 255.255.255.255 area 0
```

Related Commands

Command	Description
router ospf	Configures an OSPF routing process.

nsf cisco

To enable Cisco Nonstop Forwarding (NSF) operations on a router that is running the Open Shortest Path First (OSPF) protocol, use the **nsf cisco** command in router configuration mode. To return to the default, use the **no** form of this command.

nsf cisco [**enforce global** | **helper** [**disable**]]
no nsf cisco [**enforce global** | **helper** [**disable**]]

Syntax Description

enforce global	(Optional) Cancels Cisco NSF restart on all the interfaces when neighboring networking devices that are not NSF-aware are detected on any interface during the restart process.
helper	(Optional) Configures Cisco NSF helper mode.
disable	(Optional) Disables Cisco NSF helper mode.

Command Default

Cisco NSF restarting mode is disabled but helper mode is enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command enables Cisco NSF on an OSPF router. When the Cisco NSF is enabled on a router, the router is Cisco NSF capable and will operate in restarting mode.

By default, neighboring Cisco NSF-aware routers operate in NSF helper mode during a graceful restart. To disable Cisco NSF helper mode on a Cisco NSF-aware router, use this command with the **disable** keyword. To reenable helper mode after explicitly disabling helper mode on a Cisco NSF-aware router, use the **no nsf cisco helper disable** command.

If neighbors that are not Cisco NSF-aware are detected on a network interface during a Cisco NSF graceful restart, restart is aborted only on that interface and continues on other interfaces. To cancel restart for the entire OSPF process when neighbors that are not Cisco NSF-aware are detected during restart, configure this command with the **enforce global** keywords.

Examples

The following example shows how to enable Cisco NSF restarting mode on a router. This example causes the Cisco NSF restart to be canceled for the entire OSPF process if neighbors that are not Cisco NSF-aware are detected on any network interface during the restart.

```
Router(config)# router ospf 24
Router(config-router)# nsf cisco enforce global
```

Related Commands

Command	Description
nsf ietf	Enables IETF NSF.

nsf ietf

To configure Internet Engineering Task Force (IETF) Nonstop Forwarding (NSF) operations on a router that is running Open Shortest Path First (OSPF), use the **nsf ietf** command in router configuration mode. To return to the default, use the **no** form of this command.

nsf ietf [**restart-interval** *seconds* | **helper** [**disable** | **strict-lsa-checking**]]
no nsf ietf [**restart-interval** | **helper** [**disable** | **strict-lsa-checking**]]

Syntax Description

restart-interval *seconds*	(Optional) Specifies length of the graceful restart interval, in seconds. The range is from 1 to 1800. The default value is 120 seconds.
helper	(Optional) Configures IETF NSF helper mode.
disable	(Optional) Disables helper mode on an IETF NSF-aware router.
strict-lsa-checking	(Optional) Enables strict link-state advertisement (LSA) checking for helper mode.

Command Default

IETF NSF graceful restart mode is disabled but the helper mode is enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command enables IETF NSF on an OSPF router. When IETF NSF is enabled on a Cisco router, the router is IETF NSF-capable and will operate in restarting mode.

By default, neighboring IETF NSF-aware routers operate in IETF NSF helper mode during a graceful restart. To disable IETF NSF helper mode on an IETF NSF-aware router, use this command with the **disable** keyword. To reenable helper mode after explicitly disabling helper mode on an IETF NSF-aware router, use the **no nsf ietf helper disable** command.

Strict LSA checking enables a router in IETF NSF helper mode to terminate the graceful restart process if it detects a changed LSA that would cause flooding during the graceful restart process. Configure strict LSA checking on IETF NSF-aware and IETF NSF-capable routers but it is effective only when the router is in helper mode.

Examples

The following example shows how to enable IETF NSF restarting mode on a router and changes the graceful restart interval from default (120 seconds) to 200 seconds:

```
Router(config)# router ospf 24
Router(config-router)# nsf ietf restart-interval 200
```

Related Commands

Command	Description
nsf cisco	Enables Cisco NSF.

router ospf

To configure an Open Shortest Path First (OSPF) routing process, use the **router ospf** command in global configuration mode. To terminate an OSPF routing process, use the **no** form of this command.

router ospf *process-id*
no router ospf *process-id*

Syntax Description

process-id	Identification parameter internally used for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.

Command Default

OSPF routing process is not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

You can specify multiple OSPF routing processes in each router.

Examples

The following example shows how to configure an OSPF routing process and assign a process number of 109.

```
Router(config)# router ospf 109
```

Related Commands

Command	Description
network area	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

show cef nsf

To display the current Cisco Nonstop Forwarding (NSF) state of Cisco Express Forwarding on both the active and standby fabric cards, use the **show cef nsf** command in privileged EXEC mode.

show cef nsf

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

If the **show cef nsf** command is entered before a switchover occurs, no switchover activity is reported. After a switchover occurs, enter the **show cef nsf** command to display details about the switchover as reported by the newly active fabric card.

Examples

The following is a sample output from the **show cef nsf** command.

```
Router# show cef nsf
```

```
Last switchover occurred: 00:01:30.088 ago
Routing convergence duration: 00:00:34.728
FIB stale entry purge durations:00:00:01.728 - Default
00:00:00.088 - Red
Switchover
Slot Count Type Quiesce Period
1 2 sso 00:00:00.108
2 1 rpr+ 00:00:00.948
3 2 sso 00:00:00.152
5 2 sso 00:00:00.092
6 1 rpr+ 00:00:00.632
No NSF stats available for the following linecards:4 7
```

Related Commands

Command	Description
show cef state	Displays the state of Cisco Express Forwarding on a networking device.

show cef state

To display the state of Cisco Express Forwarding on a networking device, use the **show cef state** command in privileged EXEC mode.

show cef state

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to verify that Cisco Express Forwarding is Cisco NSF capable.

```
Router# 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.
```

Related Commands

Command	Description
show cef nsf	Displays the current Cisco NSF state of Cisco Express Forwarding on both the active and standby fabric cards.

show ip ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the **show ip ospf** command in user EXEC or privileged EXEC mode.

show ip ospf [*process-id*]

Syntax Description

process-id	(Optional) Process ID. If this argument is included, the information for the specified routing process is included.

Command Modes

User EXEC (>), Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following is sample output from the **show ip ospf** command.

```
Router# show ip ospf 1
```

```
Routing Process "ospf 1" with ID 40.40.40.40
Start time: 00:01:08.623, Time elapsed: 1d00h
Supports only single TOS(TOS0) routes
Supports opaque LSA
```

Related Commands

Command	Description
show ip ospf neighbor	Displays OSPF neighbor information on a per-interface basis.
show ip ospf nsf	Displays IP OSPF NSF state information.

show ip ospf neighbor

To display Open Shortest Path First (OSPF) neighbor information on a per-interface basis, use the **show ip ospf neighbor** command in privileged EXEC mode.

show ip ospf neighbor [*interface-type interface-number*] [*neighbor-id*] [**detail**]

Syntax Description

interface-type interface-number	(Optional) Type and number associated with a specific OSPF interface.
neighbor-id	(Optional) Neighbor hostname or IP address in A.B.C.D format.
detail	(Optional) Displays all the neighbors in detail.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following is sample output from the **show ip ospf neighbor** command showing a single line of summary information for each neighbor.

```
Router# show ip ospf neighbor
```

```
Neighbor ID    Pri    State       Dead Time   Address       Interface
10.199.199.137 1     FULL/DR      0:00:31   192.168.80.37
TenGigabitEthernet 4/1
172.16.48.1    1     FULL/DROTHER 0:00:33   172.16.48.1
TenGigabitEthernet 4/2
```

The following is sample output from the **show ip ospf neighbor detail** command.

```
Router# show ip ospf neighbor detail
```

```
Neighbor 45.45.45.45, interface address 5.5.5.1
    In the area 0 via interface TenGigabitEthernet5/1
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 5.5.5.2 BDR is 5.5.5.1
    Options is 0x12 in Hello (E-bit, L-bit)
    Options is 0x52 in DBD (E-bit, L-bit, O-bit)
    LLS Options is 0x1 (LR)
    Dead timer due in 00:00:39
    Neighbor is up for 00:00:57
    Index 3/3, retransmission queue length 0, number of retransmission 0
```

```
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
Neighbor 45.45.45.45, interface address 2.2.2.1
    In the area 0 via interface TenGigabitEthernet4/4
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 2.2.2.1 BDR is 2.2.2.2
    Options is 0x12 in Hello (E-bit, L-bit)
    Options is 0x52 in DBD (E-bit, L-bit, O-bit)
    LLS Options is 0x1 (LR)
    Dead timer due in 00:00:37
    Neighbor is up for 00:03:54
    Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
Neighbor 45.45.45.45, interface address 1.1.1.1
    In the area 0 via interface TenGigabitEthernet5/3
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 1.1.1.2 BDR is 1.1.1.1
    Options is 0x12 in Hello (E-bit, L-bit)
    Options is 0x52 in DBD (E-bit, L-bit, O-bit)
    LLS Options is 0x1 (LR)
    Dead timer due in 00:00:38
    Neighbor is up for 00:00:59
    Index 2/2, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing processes.
show ip ospf nsf	Displays IP OSPF NSF state information.

show ip ospf nsf

To display IP Open Shortest Path First (OSPF) Nonstop Forwarding (NSF) state information, use the **show ip ospf nsf** command in user EXEC or privileged EXEC mode.

show ip ospf nsf

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>), Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following is sample output from the **show ip ospf nsf** command.

```
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
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing processes.
show ip ospf neighbor	Displays OSPF neighbor information on a per-interface basis.

show issu capability

To display the In-Service Software Upgrade (ISSU) capability of a client, use the **show issu capability** command in user EXEC or privileged EXEC mode.

show issu capability {**entries** | **groups** | **types**} [*client_id*]

Syntax Description

entries	Displays a list of capability types and dependent capability types that are included in a single capability entry. Types within an entry can also be independent.
groups	Displays a list of capability entries based on the priority order (in the order that they are negotiated in a session).
types	Displays an ID that identifies a particular capability.
client_id	(Optional) Client registered to the ISSU infrastructure. To obtain a list of client IDs, use the **show issu clients** command.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

ISSU capability is a functionality where an ISSU client can support and is required to interoperate with peers. When an ISSU-aware client establishes its session with the peer, an ISSU negotiation takes place. The ISSU infrastructure uses the registered information to negotiate the capabilities and the message version to be used during the session.

Examples

The following example is a sample output of the **show issu capability types** command displaying the ISSU capability types for the IP host ISSU client (clientid=2082):

```
Router# show issu capability types 2082
```

```
Client_ID = 2082,  Entity_ID = 1 :
    Cap_Type = 0
```

Related Commands

Command	Description
show issu	Displays software upgrade information.
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.

show issu clients

To list the current ISSU clients, that is, the applications and protocols on the network supported by ISSU, use the **show issu clients** command in user EXEC or privileged EXEC mode.

show issu clients

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

To implement the ISSU versioning functionality, a client must first register its client capability, and client message information with the ISSU infrastructure during system initialization.

The **show issu clients** command lists all the ISSU clients currently operating in the network, along with their Client ID numbers and the number of entities each client contains.

Examples

The following is a sample output of the **show issu clients** command displaying the ISSU clients:

```
Router# show issu clients
```

```
 Client_ID = 1101,  Client_Name = ISSU NGXP CARD OIR client,  Entity_Count
 = 1
 Client_ID = 1102,  Client_Name = ISSU NGXP HAL RM Client,  Entity_Count
 = 1
 Client_ID = 1104,  Client_Name = ISSU NGXP MTM client,  Entity_Count =
1
 Client_ID = 1105,  Client_Name = ISSU NGXP PBMGR client,  Entity_Count
= 1
 Client_ID = 1106,  Client_Name = ISSU NGXP CIM IPC client,  Entity_Count
 = 1
 Client_ID = 1107,  Client_Name = ISSU NGXP rep IPC client,  Entity_Count
 = 1
 Client_ID = 1108,  Client_Name = ISSU NGXP l2pt IPC client,  Entity_Count
 = 1
 Client_ID = 1109,  Client_Name = ISSU NGXP mtm IPC client,  Entity_Count
 = 1
 Client_ID = 1110,  Client_Name = ISSU NGXP QOS IPC client,  Entity_Count
 = 1
 Client_ID = 1111,  Client_Name = ISSU NGXP PB IPC client,  Entity_Count
```

```
 = 1
 Client_ID = 1112,  Client_Name = ISSU NGXP RM IPC client,  Entity_Count
 = 1
 Client_ID = 1113,  Client_Name = ISSU NGXP igmp_sn IPC client,
Entity_Count = 1
```

Related Commands

Command	Description
show issu capability	Displays the ISSU capability of a client.
show issu entities	Displays the ISSU entity information.
show issu negotiated	Displays results of a negotiation that occurred concerning message versions or client capabilities.
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status for the impending software upgrade is compatible.

show issu comp-matrix

To display information regarding the ISSU compatibility matrix, use the **show issu comp-matrix** command in user EXEC or privileged EXEC mode.

show issu comp-matrix {**negotiated** | **stored**}

Syntax Description

negotiated	Displays negotiated compatibility matrix information.
stored	Displays stored compatibility matrix information.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Before attempting an ISSU, check the compatibility level between the Cisco Carrier Packet Transport (CPT) software versions on the active and the standby fabric cards. ISSU will not work if the two versions are incompatible. Use the **show issu comp-matrix** command with the **negotiated** keyword to display information on the negotiation of the compatibility matrix data between two software versions on a given system. Use the **show issu comp-matrix** command with the **stored** keyword to display stored compatibility matrix information.

Examples

The following example is a sample output of the **show issu comp-matrix negotiated** command displaying negotiated compatibility matrix information:

```
Router#  show issu comp-matrix negotiated

 Cid     Eid      Sid     pSid    pUid      Compatibility

=========================================================
  2       1       262151  3       1         COMPATIBLE
  3       1       262160  5       1         COMPATIBLE
  4       1       262163  9       1         COMPATIBLE
  5       1       262186  25      1         COMPATIBLE
  7       1       262156  10      1         COMPATIBLE
  8       1       262148  7       1         COMPATIBLE
  9       1       262155  1       1         COMPATIBLE
  10      1       262158  2       1         COMPATIBLE
```

```
11      1       262172  6       1         COMPATIBLE
100     1       262166  13      1         COMPATIBLE
110     113     262159  14      1         COMPATIBLE
200     1       262167  24      1         COMPATIBLE
2002    1       -       -       -         UNAVAILABLE
2003    1       262185  23      1         COMPATIBLE
2004    1       262175  16      1         COMPATIBLE
```

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.
show issu sessions	Displays ISSU session information for a specified client.

show issu endpoints

To display the ISSU endpoint information, use the **show issu endpoints** command in user EXEC or privileged EXEC mode.

show issu endpoints

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Endpoint is an execution unit within a redundancy domain. The ISSU infrastructure communicates between the two endpoints to establish a session and perform session negotiation for ISSU clients.

Examples

The following is a sample output of the **show issu endpoints** command displaying ISSU endpoints:

```
Router# show issu endpoints
```

```
My_Unique_ID = 5/0x5,  Client_Count = 71
This endpoint communicates with 2 peer endpoints :
        Peer_Unique_ID  CAP   VER  XFORM ERP  Compatibility
          3/0x       3    1     2     1   3      Not same
          4/0x       4    1     2     1   3       Same

Shared Negotiation Session Info :
   Nego_Session_ID = 95
   Nego_Session_Name = shared nego session
   Transport_Mtu = 4096
   Ses_In_Use = 2
```

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.

show issu entities

To display information about entities in one or more ISSU clients, use the **show issu entities** command in user EXEC or privileged EXEC mode.

show issu entities [*client-id*]

Syntax Description

client-id	(Optional) Identification number of a single ISSU client.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

An entity is a logical group of sessions that possess some common attributes. Enter a Client_ID to view information only about entities of a client. If a Client_ID is not specified, the command displays all the entities of the ISSU clients known to the device.

If the Client_ID number is not known, use the **show issu clients** command to display the current list of clients with their names and ID numbers.

Examples

The following example is a sample output of the **show issu entities** command displaying the entity information for a specific ISSU client:

```
Router# show issu entities 1106
```

```
Client_ID = 1106 :
    Entity_ID = 1,  Entity_Name = ISSU NGXP CIM IPC entity:
       MsgType MsgGroup CapType CapEntry CapGroup
        Count    Count   Count   count    Count
         26        1       1       1        1
```

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.

Command	Description
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status for the impending software upgrade is compatible.

show issu fsm

To display the ISSU finite state machine (FSM) information corresponding to an ISSU session, use the **show issu fsm** command in user EXEC or privileged EXEC mode.

show issu fsm [*session_id*]

Syntax Description

session_id	(Optional) Session ID corresponding to an ISSU session.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following is a sample output of the **show issu fsm** command displaying and verifying the ISSU state:

```
Router# show issu fsm 55
```

```
 Session_ID = 55 :
  FSM_Name          Curr_State      Old_State       Error_Reason
  FSM_L1            TRANS           P_VER           none
  FSM_L2_HELLO      EXIT            RCVD            none
  FSM_L2_A_CAP      A_INIT          unknown         none
  FSM_L2_P_CAP      P_EXIT          P_REQ           none
  FSM_L2_A_VER      A_INIT          unknown         none
  FSM_L2_P_VER      P_EXIT          P_VER_REQ       none
  FSM_L2_TRANS      COMP            COMP            none
Current FSM is FSM_L2_TRANS
Session is compatible
Negotiation started at 2d23h, duration is 0.052 seconds
```

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.

Command	Description
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status for the impending software upgrade is compatible.

show issu message

To display checkpoint messages for a specified ISSU client, use the **show issu message** command in user EXEC or privileged EXEC mode.

show issu message {**groups** | **types**} [*client_id*]

Syntax Description

groups	Displays information on the message group supported by the specified client.
types	Displays information on all the message types supported by the specified client.
client_id	(Optional) Specifies a Client ID.

Command Default

If client ID is not specified, displays message groups or message types information for all the clients registered to the ISSU infrastructure.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

ISSU messages are synchronized data (also known as checkpoint data) sent between two endpoints.

When an ISSU-aware client establishes its session with a peer, an ISSU negotiation takes place. The ISSU infrastructure uses the registered information to negotiate the capabilities and the message version to be used during the session.

Examples

The following is a sample output of the **show issu message groups** command displaying message groups for Client_id 2082:

```
Router# show issu message groups 2082
```

```
Client_ID = 2082,  Entity_ID = 1 :
   Message_Group = 1 :
                  Message_Type = 1,  Version_Range = 1 ~ 1
                  Message_Type = 2,  Version_Range = 1 ~ 1
                  Message_Type = 3,  Version_Range = 1 ~ 1
                  Message_Type = 4,  Version_Range = 1 ~ 1
                  Message_Type = 5,  Version_Range = 1 ~ 1
```

```
                    Message_Type = 6,  Version_Range = 1 ~ 1
                    Message_Type = 8,  Version_Range = 1 ~ 1
                    Message_Type = 9,  Version_Range = 1 ~ 1
                    Message_Type = 10,  Version_Range = 1 ~ 1
                    Message_Type = 11,  Version_Range = 1 ~ 1
                    Message_Type = 12,  Version_Range = 1 ~ 1
                    Message_Type = 13,  Version_Range = 1 ~ 1
                    Message_Type = 14,  Version_Range = 1 ~ 1
                    Message_Type = 15,  Version_Range = 1 ~ 1
                    Message_Type = 16,  Version_Range = 1 ~ 1
                    Message_Type = 17,  Version_Range = 1 ~ 1
                    Message_Type = 18,  Version_Range = 1 ~ 1
                    Message_Type = 19,  Version_Range = 1 ~ 1
                    Message_Type = 20,  Version_Range = 1 ~ 1
                    Message_Type = 21,  Version_Range = 1 ~ 1
```

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.

show issu negotiated

To display the session negotiation details about the ISSU message version or client capabilities, use the **show issu negotiated** command in user EXEC or privileged EXEC mode.

show issu negotiated {**version** | **capability**} *session-id*

Syntax Description

version	Displays the results of a negotiation about versions of the messages exchanged during the specified session, between the active and standby endpoints.
capability	Displays the results of a negotiation about the capabilities of the client application for the specified session.
session-id	Number used by the ISSU to identify a particular communication session between the active and the standby devices.

Command Default

Displays negotiated capability or version information for all the ISSU sessions.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

If the session_ID number is not known, enter the **show issu sessions** command. It will display the session_ID.

Examples

The following example is a sample output of the **show issu negotiated version** command displaying results of a negotiation about message versions.

```
Router# show issu negotiated version 55
```

```
Session_ID = 55 :
    Message_Type = 1,  Negotiated_Version = 1,  Message_MTU = 24
    Message_Type = 2,  Negotiated_Version = 1,  Message_MTU = 788
    Message_Type = 3,  Negotiated_Version = 1,  Message_MTU = 16
    Message_Type = 4,  Negotiated_Version = 1,  Message_MTU = 20
    Message_Type = 5,  Negotiated_Version = 1,  Message_MTU = 16
    Message_Type = 6,  Negotiated_Version = 1,  Message_MTU = 12
    Message_Type = 8,  Negotiated_Version = 1,  Message_MTU = 788
    Message_Type = 9,  Negotiated_Version = 1,  Message_MTU = 16
```

```
    Message_Type = 10, Negotiated_Version = 1,  Message_MTU = 788
    Message_Type = 11, Negotiated_Version = 1,  Message_MTU = 16
    Message_Type = 12, Negotiated_Version = 1,  Message_MTU = 16
    Message_Type = 13, Negotiated_Version = 1,  Message_MTU = 32
    Message_Type = 14, Negotiated_Version = 1,  Message_MTU = 20
    Message_Type = 15, Negotiated_Version = 1,  Message_MTU = 16
    Message_Type = 16, Negotiated_Version = 1,  Message_MTU = 20
    Message_Type = 17, Negotiated_Version = 1,  Message_MTU = 16
    Message_Type = 18, Negotiated_Version = 1,  Message_MTU = 12
    Message_Type = 19, Negotiated_Version = 1,  Message_MTU = 1380
    Message_Type = 20, Negotiated_Version = 1,  Message_MTU = 20
    Message_Type = 21, Negotiated_Version = 1,  Message_MTU = 12
    Message_Type = 22, Negotiated_Version = 1,  Message_MTU = 48
    Message_Type = 23, Negotiated_Version = 1,  Message_MTU = 2360
    Message_Type = 24, Negotiated_Version = 1,  Message_MTU = 16
    Message_Type = 25, Negotiated_Version = 1,  Message_MTU = 20
    Message_Type = 26, Negotiated_Version = 1,  Message_MTU = 8008
    Message_Type = 27, Negotiated_Version = 1,  Message_MTU = 12
```

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.
show issu message types	Displays the formats, versions, and maximum packet size of ISSU messages supported by a particular client.
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status for the impending software upgrade is compatible.

show issu sessions

To display detailed information about a particular ISSU client, including whether the client status for the impending software upgrade is compatible, use the **show issu sessions** command in user EXEC or privileged EXEC mode.

show issu sessions *client-id*

Syntax Description

client-id	Identification number used by the ISSU for the client.

Command Default

Displays session information for all the clients registered to the ISSU infrastructure.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

A session is bidirectional and a reliable connection that is established between two endpoints. Sync-data and negotiation messages are sent to the peer endpoint through a session.

When an ISSU-aware client establishes its session with the peer, an ISSU negotiation takes place. The ISSU infrastructure uses the registered information to negotiate the capabilities and the message version to be used during the session.

Examples

The following is a sample output of the **show issu sessions** command:

```
Router# show issu sessions 1106
```

```
Client_ID = 1106,  Entity_ID = 1 :

*** Session_ID = 55,  Session_Name = NGXP CIM IPC :

      Peer     Peer   Negotiate  Negotiated   Cap      Msg     Session
    UniqueID    Sid     Role       Result   GroupID  GroupID  Signature
        3        56   PASSIVE   COMPATIBLE    1        1         0
                            (policy)

   Negotiation Session Info for This Message Session:
        Nego_Session_ID = 55
        Nego_Session_Name = NGXP CIM IPC
        Transport_Mtu = 0
```

```
         Compat_Result: raw_result =   COMPATIBLE,  policy_result =
COMPATIBLE


 *** Session_ID = 107,  Session_Name = NGXP CIM IPC :

       Peer     Peer   Negotiate  Negotiated   Cap      Msg     Session
     UniqueID    Sid     Role       Result   GroupID  GroupID  Signature
         4         79   PASSIVE   COMPATIBLE    1        1         0
                              (policy)

    Negotiation Session Info for This Message Session:
         Nego_Session_ID = 107
         Nego_Session_Name = NGXP CIM IPC
         Transport_Mtu = 0
         Compat_Result: raw_result =   COMPATIBLE,  policy_result =
COMPATIBLE
```

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.
show issu message	Displays the formats, versions, and maximum packet size of ISSU messages supported by a particular client.
show issu negotiated	Displays the results of a negotiation that occurred concerning message versions or client capabilities.

show redundancy

To display current or historical status and related information on planned or logged handovers, use the **show redundancy** command in privileged EXEC mode.

show redundancy [**clients** | **config-sync** | **counters** | **domain** | **history** | **idb-sync-history** | **interlink** | **states** | **switchover** | **trace**]

Syntax Description

clients	(Optional) Displays the redundancy-aware client application and protocol list.
config-sync	(Optional) Displays redundancy configuration synchronization status.
counters	(Optional) Displays redundancy-related operational measurements.
domain	(Optional) Displays information about the redundancy domain.
history	(Optional) Displays past status and related information about logged handovers.
idb-sync-history	(Optional) Displays redundancy Interface Descriptor Blocks (IDB) synchronization history.
interlink	(Optional) Displays interlink utilization.
states	(Optional) Displays redundancy-related states.
switchover	(Optional) Displays the switchover counts, the uptime since active, and the total system uptime.
trace	(Optional) Displays redundancy trace.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command displays the redundancy configuration mode of the fabric card. This command also displays information about the number of switchovers, system uptime, processor uptime, and redundancy state, and reasons for any switchovers.

Examples

The following is a sample output from the **show redundancy** command.

```
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)
```

The following is a sample output from the **show redundancy states** command.

```
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
```

The following is a sample output from the **show redundancy history** command.

```
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
```

The following is a sample output from the **show redundancy switchover history** command.

```
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
```

REP Command Reference

This chapter describes commands to configure Resilient Ethernet Protocol (REP).

rep admin vlan

To configure a Resilient Ethernet Protocol (REP) administrative VLAN for REP to transmit hardware flood layer (HFL) messages, use the **rep admin vlan** command in global configuration mode. To return to the default configuration with VLAN 1 as the administrative VLAN, use the **no** form of this command.

rep admin vlan *vlan-id*

no rep admin vlan

Syntax Description

vlan-id	The 48-bit static MAC address.

Command Default

The default value of the administrative VLAN is VLAN 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The range of the REP administrative VLAN is from 2 to 4094.

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.

You can verify your settings by entering the **show interfaces rep detail** privileged EXEC command.

Examples

The following example shows how to configure VLAN 100 as the REP administrative VLAN:

```
Router(config)# rep admin vlan 100
```

Related Commands

Command	Description
show interfaces rep detail	Displays detailed REP configuration and status for all interfaces or the specified interface, including the administrative VLAN.

rep block port

To configure a REP VLAN load balancing on the REP primary edge port, use the **rep block port** command in interface configuration mode. To return to the default configuration, use the **no** form of this command.

rep block port {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}
no rep block port {**id** *port-id* | *neighbor-offset* | **preferred**}

Syntax Description

id *port-id*	Specifies the VLAN blocking alternate port by entering the unique port ID, which is automatically generated when REP is enabled. The REP port ID is a 16-character hexadecimal value. You can display the port ID for an interface by entering the **show interface** *interface-id* **rep detail** command in privileged EXEC mode.
neighbor-offset	Identifies the VLAN blocking alternate port by entering the offset number of a neighbor. The range is from –256 to +256; a value of 0 is invalid.
preferred	Selects the regular segment port previously identified as the preferred alternate port for VLAN load balancing.
vlan	Identifies the VLANs to be blocked.
vlan-list	VLAN ID or range of VLAN IDs to be displayed. Enter a VLAN ID from 1 to 4094 or a range or sequence of VLANs (such as 1-3, 22, 41-44) to be blocked.
all	Blocks all the VLANs.

Command Default

The default behavior after you enter the **rep preempt segment** command in privileged EXEC (for manual preemption) is to block all VLANs at the primary edge port. This behavior remains until you configure the **rep block port** command.

If the primary edge port cannot determine which port is to be the alternate port, the default action is no preemption and no VLAN load balancing.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

You must enter this command on the REP primary edge port.

When you select an alternate port by entering an offset number, this number identifies the downstream neighbor port of an edge port. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset

number –1) and its downstream neighbors. Do not enter an offset value of 1 because that is the offset number of the primary edge port itself.

If you have configured a preempt delay time by entering the **rep preempt delay seconds** command in interface configuration mode and a link failure and recovery occurs, VLAN load balancing begins after the configured preemption time period elapses without another link failure. The alternate port specified in the load-balancing configuration blocks the configured VLANs and unblocks all other segment ports. If the primary edge port cannot determine the alternate port for VLAN balancing, the default action is no preemption.

Each port in a segment has a unique port ID. To determine the port ID of a port, enter the **show interfaces** *interface-id* **rep detail** command in privileged EXEC mode.

Examples

The following example shows how to configure REP VLAN load balancing.

```
Router# configure terminal
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# rep block port id 0009001818D68700 vlan 1-100
Router(config-if)# end
```

Related Commands

Command	Description
rep preempt delay	Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.
rep preempt segment	Manually starts REP VLAN load balancing on a segment.
show interfaces rep detail	Displays REP detailed configuration and status for all the interfaces or the specified interface, including the administrative VLAN.

rep lsl-age-timer

To configure the REP link status layer (LSL) age-out timer value, use the **rep lsl-age-timer** command in interface configuration mode. To restore the default age-out timer value, use the **no** form of this command.

rep lsl-age-timer *milliseconds*

no rep lsl-age-timer *milliseconds*

Syntax Description

milliseconds	REP LSL age-out timer value in milliseconds (ms). The range is from 120 ms to 10000 ms in multiples of 40 ms.

Command Default

The default LSL age-out timer value is 5 ms.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The **rep lsl-age-timer** command is used to configure the REP LSL age-out timer value. While configuring REP configurable timers, we recommend that you configure the REP LSL number of retries first and then configure the REP LSL age-out timer value.

Examples

The following example shows how to configure REP LSL age-out timer value.

```
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
```

Related Commands

Command	Description
rep lsl-retries	Configures the number of retries before the REP link is disabled.

rep lsl-retries

To configure the REP link status layer (LSL) number of retries, use the **rep lsl-retries** command in interface configuration mode. To restore the default number of retries, use the **no** form of this command.

rep lsl-retries *number-of-retries*

no rep lsl-retries *number-of-retries*

Syntax Description

number-of-retries	Number of LSL retries. The range of retries is from 3 to 10.

Command Default

The default number of LSL retries is 5.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The **rep lsl-retries** command is used to configure the number of retries before the REP link is disabled. While configuring REP configurable timers, we recommend that you configure the REP LSL number of retries first and then configure the REP LSL age-out timer value.

Examples

The following example shows how to configure REP LSL retries.

```
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
```

Related Commands

Command	Description
rep lsl-age-timer	Configures the REP link status layer age-out timer value.

rep preempt delay

To configure a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered, use the **rep preempt delay** command in interface configuration mode. To remove the configured delay, use the **no** form of this command.

rep preempt delay *seconds*

no rep preempt delay

Syntax Description

seconds	Number of seconds to delay REP preemption. The range is from 15 to 300 seconds. The default is manual preemption without delay.

Command Default

REP preemption delay is not set. The default is manual preemption without delay.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

You must enter this command on the REP primary edge port.

You must enter this command and configure a preempt time delay if you want VLAN load balancing to automatically trigger after a link failure and recovery.

If VLAN load balancing is configured, after a segment port failure and recovery, the REP primary edge port starts a delay timer before VLAN load balancing occurs. Note that the timer restarts after each link failure. When the timer expires, the REP primary edge alerts the alternate port to perform VLAN load balancing (configured by using the **rep block port** interface configuration command) and prepares the segment for the new topology. The configured VLAN list is blocked at the alternate port, and all other VLANs are blocked at the primary edge port.

You can verify your settings by entering the **show interfaces rep** privileged EXEC command.

Examples

The following example shows how to configure a REP preemption time delay of 100 seconds on the primary edge port.

```
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# rep preempt delay 100
Router(config-if)# exit
```

Related Commands

Command	Description
rep block port	Configures VLAN load balancing.
rep preempt segment	Manually starts REP VLAN load balancing on a segment.
show interfaces rep detail	Displays REP configuration and status for all interfaces or the specified interface.

rep preempt segment

To manually start REP VLAN load balancing on a segment, use the **rep preempt segment** command in privileged EXEC mode.

rep preempt segment *segment-id*

Syntax Description

segment-id	ID of the REP segment. The range is from 1 to 1024.

Command Default

Manual preemption is the default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Enter this command on the segment, which has the primary edge port on the router.

Ensure that all the other segment configuration is 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* command in interface configuration mode 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.

If you do not configure VLAN load balancing, entering this command results in the default behavior—the primary edge port blocks all VLANs.

You configure VLAN load balancing by entering the **rep block port** command in interface configuration mode on the REP primary edge port before you manually start preemption.

Examples

The following example shows how to manually trigger REP preemption on segment 100.

```
Router# rep preempt segment 100
```

Related Commands

Command	Description
rep block port	Configures VLAN load balancing.

Command	Description
rep preempt delay	Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.
show interfaces rep detail	Displays REP configuration and status for all interfaces or the specified interface.
show rep topology	Displays REP topology information for a segment or for all segments.

rep segment

To enable REP on the interface and to assign a segment ID to the interface, use the **rep segment** command in interface configuration mode. To disable REP on the interface, use the **no** form of this command.

rep segment *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]
no rep segment

Syntax Description

segment-id	Segment for which REP is enabled. Assign a segment ID to the interface. The range is from 1 to 1024.
edge	(Optional) Configures the port as an edge port. Each segment has only two edge ports.
no-neighbor	(Optional) Specifies the segment edge as one with no external REP neighbor.
primary	(Optional) Specifies that the port is the primary edge port where you can configure VLAN load balancing. A segment has only one primary edge port.
preferred	(Optional) Specifies 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.

Command Default

REP is disabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

REP ports must be a Layer 2 IEEE 802.1Q port or 802.1AD port. You must configure two edge ports on each REP segment, a primary edge port and a port to act as a secondary edge port.

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 remain in a blocked state until notified that it is safe to unblock. Be aware of this to avoid sudden connection losses.

When REP is enabled on an interface, the default is for the port to be a regular segment port.

Examples

The following example shows how to enable REP on a regular (nonedge) segment port.

```
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# rep segment 100
```

The following example shows how to enable REP on a port and identify the port as the REP primary edge port.

```
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# rep segment 100 edge primary
```

The following example shows how to enable REP on a port and identify the port as the REP secondary edge port.

```
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# rep segment 100 edge
```

The following example shows how to enable REP as an edge no-neighbor port.

```
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# rep segment 1 edge no-neighbor primary
```

Related Commands

Command	Description
show interfaces rep detail	Displays REP configuration and status for all the interfaces or the specified interface.
show rep topology	Displays information about all the ports in the segment, including the one that was configured and selected as the primary edge port.

rep stcn

To configure a REP edge port to send segment topology change notifications (STCNs) to another interface or to other segments, use the **rep stcn** command in interface configuration mode. To disable the sending of STCNs to the interface or to the segment, use the **no** form of this command.

rep stcn {**interface** *interface-id* | **segment** *segment-id-list*}
no rep stcn {**interface** | **segment**}

Syntax Description

interface *interface-id*	Specifies a physical interface or port channel to receive STCNs.
segment *segment-id-list*	Specifies one REP segment or a list of segments to receive STCNs. The segment range is from 1 to 1024. You can also configure a sequence of segments (for example 3 to 5, 77, 100).

Command Default

Transmission of STCNs to other interfaces or segments is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Enter this command on a segment edge port to send STCNs to one or more segments or to an interface. You can verify your settings by entering the **show interfaces rep detail** privileged EXEC command.

Examples

The following example shows how to configure a REP edge port to send STCNs to segments 25 to 50.

```
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# rep stcn segment 25-50
Router(config-if)# end
```

Related Commands

Command	Description
show interfaces rep detail	Displays REP configuration and status for all the interfaces or the specified interface.

show interfaces rep detail

To display detailed REP configuration and status for all the interfaces or the specified interface, including the administrative VLAN, use the **show interfaces rep detail** command in privileged EXEC mode.

show interfaces [*interface-id*] **rep detail**

Syntax Description

interface-id	(Optional) Physical interface used to display the port ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to display the REP configuration and status for a specified interface.

```
Router# show interfaces 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
```

Related Commands

Command	Description
rep admin vlan	Configures a REP administrative VLAN for REP to transmit HFL messages.
rep block port	Configures REP VLAN load balancing on the REP primary edge port.
rep preempt delay	Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.
rep reempt segment	Manually starts REP VLAN load balancing on a segment.
rep stcn	Configure a REP edge port to send STCNs to another interface or to other segments.

show rep topology

To display REP topology information for a segment or for all segments, including the primary and secondary edge ports in the segment, use the **show rep topology** command in privileged EXEC mode.

show rep topology [**segment** *segment-id*] [**archive**] [**detail**]

Syntax Description

segment *segment-id*	(Optional) Specifies the segment for which to display REP topology information. The ID range is from 1 to 1024.
archive	(Optional) Displays the previous topology of the segment. This keyword is useful for troubleshooting a link failure.
detail	(Optional) Displays detailed REP topology information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following is sample output from 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
```

The following is sample output from 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]
```

Related Commands

Command	Description
rep preempt segment	Manually starts REP VLAN load balancing on a segment.
rep segment	Enables REP on an interface and assigns a segment ID.

LAG and LACP Command Reference

This chapter describes commands to configure Link Aggregation Group (LAG) and Link Aggregation Control Protocol (LACP).

channel-group

To configure the interface in a channel group and set the Link Aggregation Control Protocol (LACP) mode, use the **channel-group** command in interface configuration mode. To remove the channel-group configuration from the interface, use the **no** form of this command.

channel-group *channel-group-number* **mode** {**active** | **passive**}

no channel-group *channel-group-number*

Syntax Description

channel-group-number	Integer that identifies the channel group. The range is from 1 to 128.
mode	Sets the LACP mode.
active	Enables LACP unconditionally.
passive	Enables LACP only when an LACP device is detected. This is the default state.

Command Default

No channel groups are assigned.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

You do not have to disable the IP address that is assigned to a physical interface that is part of a channel group, but we highly recommend in doing so. A port-channel must be created before member links are assigned to it.

Examples

The following example shows how to add the interface TenGigabitEthernet 4/1 to the channel group specified by port-channel 1:

```
Router(config)# interface port-channel 1
Router(config-if)# exit
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# channel-group 1
```

Related Commands

Command	Description
interface port-channel	Creates a port-channel virtual interface.

Command	Description
lacp port-priority	Sets the LACP priority for a physical interface.
lacp system-priority	Sets the LACP priority for a system.
show interfaces port-channel	Displays traffic that is seen by a specific port channel.

interface port-channel

To create a port-channel virtual interface, use the **interface port-channel** command in global configuration mode.

interface port-channel *channel-number*

Syntax Description

channel-number	Channel number assigned to this port-channel interface.

Command Default

The port-channel virtual interface is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to create a port-channel interface.

```
Router(config)# interface port-channel 2
```

Related Commands

Command	Description
channel-group	Configures the interface in a channel group.
interface port-channel	Creates a port-channel virtual interface.
lacp min-bundle	Defines the minimum number of active bundled LACP ports allowed in a port channel.
lacp max-bundle	Defines the maximum number of active bundled LACP ports allowed in a port channel.
show interfaces port-channel	Displays traffic that is seen by a specific port channel.

lacp fast-switchover

To enable LACP 1:1 link redundancy, use the **lacp fast-switchover** command in interface configuration mode. To disable LACP 1:1 link redundancy, use the **no** form of this command.

lacp fast-switchover

no lacp fast-switchover

Syntax Description

This command has no arguments or keywords.

Command Default

LACP 1:1 link redundancy is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Before entering the **lacp fast-switchover** command, ensure the following:

- The port channel protocol type is LACP.
- The **lacp max-bundle** command has been entered on the port channel. The **lacp fast-switchover** command does not affect the **lacp max-bundle** command.

When you enable LACP 1:1 link redundancy, based on the system priority and port priority, the port with the higher system priority chooses the link as the active link and the other link as the standby link. When the active link fails, the standby link is selected as the new active link without taking down the port channel. When the original active link recovers, it reverts to its active link status. During this switch over, the port channel is also up.

Examples

The following example shows how to enable LACP 1:1 link redundancy:

```
Router(config-if)# lacp fast-switchover
```

Related Commands

Command	Description
lacp max-bundle	Defines the maximum number of active bundled LACP ports allowed in a port channel.

lacp max-bundle

To define the maximum number of active bundled LACP ports allowed in a port channel, use the **lacp max-bundle** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

lacp max-bundle *max-bundle-number*

no lacp max-bundle

Syntax Description

max-bundle-number	Maximum threshold of active member links allowed in the LACP bundle. The range from is 1 to 8. The maximum threshold value must be greater than or equal to the minimum threshold value.

Command Default

A maximum number of active bundled LACP ports is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The value specified in the *max-bundle-number* argument determines the number of active links that are bundled in the port channel. The remaining links are in hot-standby mode.

Examples

The following example shows how to set three ports to bundle in port channel 2:

```
Router(config)# interface port-channel 2
Router(config-if)# lacp max-bundle 3
```

Related Commands

Command	Description
interface port-channel	Creates a port-channel virtual interface.
lacp fast-switchover	Enables LACP 1:1 link redundancy.
lacp port-priority	Sets the LACP priority for a physical interface.
show interfaces port-channel	Displays traffic that is seen by a specific port channel.

lacp min-bundle

To define the minimum number of active bundled LACP ports allowed in a port channel, use the **lacp min-bundle** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

lacp min-bundle *min-bundle-number*

no lacp min-bundle

Syntax Description

min-bundle-number	Minimum threshold of active member links allowed in the LACP bundle. The range is from 1 to 8. The default is 1.

Command Default

A minimum number of active bundled LACP ports is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use this command to configure the minimum number of active links allowed in an LACP bundle. When the number of active links falls below this minimum threshold, the port channel shuts down.

Examples

The following example shows how to set the minimum number of active links to five ports:

```
Router(config)# interface port-channel 2
Router(config-if)# lacp min-bundle 5
```

Related Commands

Command	Description
interface port-channel	Creates a port-channel virtual interface.
show interfaces port-channel	Displays traffic that is seen by a specific port channel.

lacp port-priority

To set the LACP priority for a physical interface, use the **lacp port-priority** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

lacp port-priority *priority*

no lacp port-priority

Syntax Description

priority	Integer that indicates the priority for the physical interface. The range is from 0 to 65535. The default is 32768.

Command Default

The default port priority is set to 32768.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

You may assign a port priority to each port on a device running LACP. You can specify the port priority by using the **lacp port-priority** command or use the default port priority (32768). The port priority is used to decide which ports should be put in standby mode when a hardware limitation or the **lacp max-bundle** command configuration prevents all compatible ports from aggregating. Priority is supported only on port channels with LACP-enabled physical interfaces.

Note A high priority number means a low priority.

To verify the configured port priority, use the **show lacp internal** command.

Examples

The following example shows how to set a port priority of 23700 for an interface:

```
Router(config-if)# lacp port-priority 23700
```

Related Commands

Command	Description
channel-group	Creates a channel group.

Command	Description
lacp max-bundle	Defines the maximum number of active bundled LACP ports allowed in a port channel.
lacp system-priority	Sets the LACP system priority.
show lacp	Displays information about LACP activity on the device.

lacp system-priority

To set the LACP priority for a system, use the **lacp system-priority** command in global configuration mode. To return to the default setting, use the **no** form of this command.

lacp system-priority *priority*

no lacp system-priority

Syntax Description

priority	Integer that indicates the LACP priority for the system. The range is from 0 to 65535. The default is 32768.

Command Default

The default system priority is set to 32768.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

You can assign a system priority to each device running LACP. You can specify the system priority by using the **lacp system-priority** command or use the default system priority (32768). The system priority is used with the MAC address of the device to form the system ID and is used during negotiation with the other systems. The system priority is supported only on port channels with LACP-enabled physical interfaces.

Note A high priority number means a low priority.

To verify the configured system priority, issue the **show lacp** command.

Examples

The following example shows how to set a system priority of 25500 for a device:

```
Router(config)# lacp system-priority 25500
```

Related Commands

Command	Description
channel-group	Creates a channel group.
lacp port-priority	Sets the priority of a port.

Command	Description
show lacp	Displays information about LACP activity on the device.

port-channel load-balance

To configure a member link for load balancing, use the **port-channel load-balance** command in interface configuration mode. To disable load balancing, use the **no** form of this command.

port-channel load-balance {**link** *link-id*}

Syntax Description

link *link-id*	Integer that identifies the member link for load balancing. The range is from 1 to 8.

Command Default

The member link is not configured for load balancing.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The Cisco CPT supports manual load balancing and platform default load balancing. It 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.

Examples

The following example shows how to configure manual load balancing:

```
Router(config)# interface port-channel 1
Router(config-if)# port-channel load-balance link 1
```

show interfaces port-channel

To display the traffic on specific port channel, use the **show interfaces port-channel** command in privileged EXEC mode.

show interfaces port-channel *channel-number*

Syntax Description

channel-number	(Optional) Port channel number. The range is 1 to 128.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following is a sample output of the **show interfaces port-channel** command that shows how to view the information for a port channel interface.

```
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
```

Related Commands

Command	Description
channel-group	Configures the interface in a channel group and sets the LACP mode.
interface port-channel	Creates a port-channel virtual interface.
lacp max-bundle	Defines the maximum number of active bundled LACP ports allowed in a port channel.
lacp min-bundle	Defines the minimum number of active bundled LACP ports allowed in a port channel.

show lacp

To display LACP information, use the **show lacp** command in privileged EXEC mode.

show lacp {*channel-group-number* | **counters** | **internal [detail]** | **neighbor [detail]** | **sys-id**}

Syntax Description

channel-group-number	Number of the channel group. The range is from 1 to 128.
counters	Displays information about the LACP traffic statistics.
internal	Displays LACP internal information.
detail	(Optional) Displays detailed internal information.
neighbor	Displays information about the LACP neighbor.
sys-id	Displays the LACP system identification. It is a combination of the port priority and the MAC address of the device.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use the **show lacp** command to troubleshoot problems related to LACP in a network. If you do not specify a value for the argument *channel-group-number*, all the channel groups are displayed.

Examples

The following are sample outputs of the **show lacp** command that shows how to view the 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 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
```

Related Commands

Command	Description
lacp port-priority	Sets the priority for the physical interfaces.
lacp system-priority	Sets the priority of the system.

MAC Learning Command Reference

This chapter describes commands to configure MAC learning.

clear mac-address-table

To remove a specified address (or set of addresses) from the MAC address table, use the **clear mac-address-table** command in privileged EXEC mode.

clear mac-address-table [**address** *mac-addr*] [**bridge-domain** *bridgedomain-id*] [**interface** *type number*]

Syntax Description

address *mac-addr*	(Optional) Specifies the MAC address to clear.
bridge-domain *bridgedomain-id*	(Optional) Clears the MAC address from the specified bridge domain.
interface *type number*	(Optional) Clears the MAC address from the specified interface.

Command Default

When no options are specified, all the dynamically added MAC addresses are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

If the **clear mac-address-table** command is used without options, all the MAC addresses are removed. If you specify an address but do not specify an interface, the address is deleted from all the interfaces. If you specify an interface but do not specify an address, all the addresses on the specified interface are removed.

Examples

The following example shows how to remove a MAC address from the MAC address table on a bridge domain:

```
Router# clear mac-address-table address
0000.bbbb.cccc interface TenGigabitEthernet 4/1 bridge-domain 100
```

The following example shows how to remove a MAC address from the MAC address table on all the bridge domains:

```
Router# clear mac-address-table address 0000.bbbb.cccc
```

Related Commands

Command	Description
show mac-address-table	Displays information about the MAC address table.

mac learning

To reenable MAC learning on the bridge domain, use the **mac learning** command in bridge domain configuration mode. To disable MAC learning, use the **no** form of this command.

mac learning

no mac learning

Syntax Description

This command has no arguments or keywords.

Command Default

MAC learning is enabled on the bridge domains by default.

Command Modes

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

MAC address learning is enabled by default only for point–to–multipoint bridge domains and can also be disabled.

Examples

The following example shows how to reenable MAC learning on a bridge domain:

```
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:

```
Router> enable
Router# configure terminal
Router(config)# bridge-domain 100
Router(config-bdomain)# no mac learning
Router(config-bdomain)# end
```

Related Commands

Command	Description
mac static address	Configures a static MAC address on a service instance.

Command	Description
mac limit maximum addresses	Configures the maximum number of MAC addresses allowed on a bridge domain.

mac limit maximum addresses

To configure the maximum number of MAC addresses allowed on a bridge domain, use the **mac limit maximum addresses** command in bridge domain configuration mode. To return to the default state, use the **no** form of this command.

mac limit maximum addresses *maximum-addresses*

no mac limit maximum addresses *maximum-addresses*

Syntax Description

maximum-addresses	Integer that specifies the maximum number of MAC addresses allowed on a bridge domain. The range is from 1 to 128000.

Command Default

Maximum number of MAC addresses are allowed on the bridge domain.

Command Modes

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to set the maximum number of MAC addresses on a specific bridge domain to 1000:

```
Router> enable
Router# configure terminal
Router(config)# bridge-domain 100
Router(config-bdomain)# mac limit maximum addresses 1000
Router(config-bdomain)# end
```

Related Commands

Command	Description
mac learning	Enables MAC learning on a bridge domain.

mac static address

To configure a static MAC address on a service instance, use the **mac static address** command in service instance configuration mode. To remove a static MAC address, use the **no** form of this command.

mac static address *mac-addr*

no mac static address *mac-addr*

Syntax Description

mac-addr	The 48-bit static MAC address.

Command Default

MAC static addresses are not configured.

Command Modes

Service instance configuration (config-if-srv)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Static MAC address configuration is supported only on Ethernet virtual circuit (EVC) bridge domain interfaces. The static MAC address configuration does not apply to the Multicast VLAN Registration (MVR) bridge domain.

Examples

The following example shows how to configure a MAC static address in service instance configuration mode:

```
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
```

Related Commands

Command	Description
mac learning	Enables MAC learning on a bridge domain.

show mac-address-table

To display information about the MAC address table, use the **show mac-address-table** command in privileged EXEC mode.

show mac-address-table [**address** *mac-addr*] [**bridge-domain** *bridgedomain-id*] [**interface** *type number*] [**count**]

Syntax Description

address *mac-addr*	(Optional) Displays information about the MAC address table for a specific MAC address.
bridge-domain *bridgedomain-id*	(Optional) Displays information about the MAC address table for a specific bridge domain.
interface *type number*	(Optional) Displays information about the MAC address table for a specific interface.
count	(Optional) Displays the number of entries that are currently in the MAC address table.

Command Default

When no options are specified, the command displays the entire MAC address table.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The *mac-addr* is a 48–bit MAC address and the valid format is H.H.H. The *bridgedomain-id* is the bridge domain number.

Examples

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
```

Related Commands

Command	Description
clear mac-address-table	Deletes entries from the MAC address table.

IGMP Snooping Command Reference

This chapter describes commands used to configure Internet Group Management Protocol (IGMP) snooping.

ip igmp snooping

To enable Internet Group Management Protocol (IGMP) snooping, use the **ip igmp snooping** command in the bridge domain configuration mode. To disable IGMP snooping, use the **no** form of this command.

ip igmp snooping

no ip igmp snooping

Syntax Description

This command has no arguments or keywords.

Command Default

IGMP snooping is not enabled.

Command Modes

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

On a CPT system, IGMP snooping can be configured at the bridge domain 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.

Examples

The following example shows how to enable IGMP snooping on a bridge domain:

```
Router(config)# bridge-domain 30
Router(config-bdomain)# ip igmp snooping
```

Related Commands

Command	Description
show ip igmp snooping	Displays the IGMP snooping configuration.

ip igmp snooping immediate-leave

To enable Internet Group Management Protocol (IGMP) Immediate-Leave processing on a bridge-domain, use the **ip igmp snooping immediate-leave** command in global configuration mode. To disable Immediate-Leave processing on the bridge domain, use the **no** form of this command.

ip igmp snooping immediate-leave

no ip igmp snooping immediate-leave

Syntax Description

This command has no arguments or keywords.

Command Default

By default, IGMP Immediate-Leave processing is disabled.

Command Modes

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The Immediate Leave feature is supported only on IGMP version 2 hosts.

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
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the bridge domain.
ip igmp snooping mrouter	Configures a multicast router port.

ip igmp snooping mrouter

To configure a port as a multicast router port, use the **ip igmp snooping mrouter** command in the service-instance configuration mode. To remove the configuration, use the **no** form of this command.

ip igmp snooping mrouter

no ip igmp snooping mrouter

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Service-instance configuration (config-if-srv)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Static connections to multicast routers are supported only at the EFP.

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
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the bridge domain.
show ip igmp snooping mrouter	Displays the information about the dynamically learned and manually configured multicast router interfaces.

ip igmp snooping report-suppression

To turn on IP IGMP snooping report suppression, use the **ip igmp snooping report-suppression** command in the bridge domain configuration mode. To turn off report suppression, use the **no** form of this command.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

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.

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
```

Related Commands

Command	Description
show ip igmp snooping	Displays the IGMP snooping configuration.

show ip igmp snooping

To display the Internet Group Management Protocol (IGMP) snooping configuration of a device, use the **show ip igmp snooping** command in the privileged EXEC mode.

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***]**

Syntax Description

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.
mrouter	(Optional) Displays information about dynamically learned and manually configured multicast router ports.
querier	(Optional) Displays IGMP querier information.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

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)
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the bridge domain.
ip igmp snooping immediate-leave	Enables IGMP snooping immediate leave.
ip igmp snooping mrouter	Configures a multicast router port.

show ip igmp snooping querier

To display information about the IP address and the receiving port for the recently received IGMP query messages, use the **show ip igmp snooping querier** command.

show ip igmp snooping querier [vlan *bridge-domain ID* **] [detail]**

Syntax Description

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.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

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
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the bridge domain.

Command	Description
ip igmp snooping mrouter	Configures a multicast router port.

MVR Command Reference

This chapter describes commands used to configure Multicast VLAN Registration (MVR).

mvr

To enable Multicast VLAN Registration (MVR), use the **mvr** command in the bridge domain configuration mode. To disable MVR, use the **no** form of this command.

mvr

no mvr

Syntax Description

This command has no arguments or keywords.

Command Default

MVR is not enabled.

Command Modes

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

On a CPT system, MVR can be configured at the bridge domain level.

Following configuration restrictions are applicable while configuring the MVR 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.

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
```

Related Commands

Command	Description
show mvr	Verifies the MVR configuration.

mvr group

To define a global range of IP multicast groups on which MVR must be enabled, use the **mvr group** command in the bridge domain configuration mode. To remove the IP multicast address groups, use the **no** form of this command.

mvr group *ip-address* [*count*]

no mvr group *ip-address* [*count*]

Syntax Description

ip-address	Group IP address.
count	Group count inside the bridge domain.

Command Default

The IP multicast address on which the MVR feature must be enabled is not defined.

Command Modes

Bridge domain configuration (config-bdomain)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

On a CPT system, MVR can be configured at the bridge domain level.

Following configuration restrictions are applicable while configuring the MVR 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.

The **mvr group** *ip-address* [*count*] command configures an IP multicast address on the CPT system. 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.

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
```

Related Commands

Command	Description
show mvr	Displays the MVR configuration.
show mvr groups	Displays the group MVR configuration.

mvr type

To configure an EFP as the MVR enabled source or receiver, use the **mvr type** command in the service-instance mode. To remove the source or receiver port configuration, use the **no** form of this command.

mvr type {source | receiver bridge-domain *id* **[vlan** *id***] [immediate]}**

no mvr type {source | receiver bridge-domain *id* **[vlan** *id***] [immediate]}**

Syntax Description

source	Configures an MVR EFP as the source.
receiver bridge-domain *id*	Configures an MVR EFP as the receiver. *id* —Bridge domain ID.
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. *id* —VLAN ID.
immediate	(Optional) Enables the Immediate-Leave feature on the receiver EFP.

Command Default

There is no default setting for this command.

Command Modes

Service instance mode (config-if-srv)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Users must configure an MVR bridge domain before configuring the MVR source and receiver EFPs.

An MVR enabled EFP (subscriber port) is configured 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 **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.

Examples

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 pop 1 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
```

Related Commands

Command	Description
show mvr [source-ports] [receiver-ports] [groups]	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.

show mvr

To display the MVR information use the **show mvr** command in the privileged EXEC mode.

show mvr [source-ports] [receiver-ports] [groups]

Syntax Description

source-ports	Displays the details of the MVR enabled source ports.
receiver-ports	Displays the details of the MVR enabled receiver ports.
groups	Displays the details of the MVR enabled groups.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command displays the 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.

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 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)
```

Related Commands

Command	Description
mvr	Enables MVR on the EFP.
mvr group *ip-address count*	Defines a global range of IP multicast groups on which MVR is enabled.

Command	Description
mvr type {source | receiver bridge-domain *id* **[vlan** vlan-id**] [immediate]}**	Configures an EFP as the MVR enabled source or receiver.

RMON Command Reference

This chapter describes commands to configure Remote Monitoring (RMON).

rmon

To enable Remote Monitoring (RMON) on an Ethernet interface, use the **rmon** command in interface configuration mode. To disable RMON on the interface, use the **no** form of this command.

rmon {**native** | **promiscuous**}

Syntax Description

native	Enables RMON on the Ethernet interface. In native mode, the router processes only packets destined for this interface.
promiscuous	Enables RMON on the Ethernet interface. In promiscuous mode, the router examines each packet.

Command Default

RMON is disabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command enables RMON on Ethernet interfaces. A generic RMON console application is recommended in order to use the RMON network management capabilities. Simple Network Management Protocol (SNMP) must also be configured. RMON provides visibility of individual nodal activity and monitors all nodes and their interaction on a LAN segment. When the **rmon** command is used, the router automatically installs an Ethernet statistics study for the associated interface.

RMON can be very data and processor intensive. Measure usage effects to ensure that router performance is not degraded and to minimize excessive management traffic overhead. Native mode is less intensive than promiscuous mode.

Examples

The following example enables RMON on an interface and allows the router to examine only packets destined for the interface.

```
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# rmon native
```

Related Commands

Command	Description
rmon alarm	Sets an alarm on any MIB object.

Command	Description
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

rmon alarm

To set a RMON alarm on a MIB object, use the **rmon alarm** command in global configuration mode. To disable the alarm, use the **no** form of this command.

rmon alarm *number variable interval* {**delta** | **absolute**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *string*]

no rmon alarm number

Syntax Description

number	Alarm number, which is identical to the *alarmIndex* in the alarmTable in the RMON MIB.
variable	MIB object to monitor, which translates into the *alarmVariable* used in the alarmTable of the RMON MIB.
interval	Time in seconds. The alarm monitors the MIB variable, which is identical to the *alarmInterval* used in the alarmTable of the RMON MIB.
delta	Tests the change between MIB variables, which affects the *alarmSampleType* in the alarmTable of the RMON MIB.
absolute	Tests each MIB variable directly, which affects the *alarmSampleType* in the alarmTable of the RMON MIB.
rising-threshold *value*	Specifies the value at which the alarm is triggered.
event-number	(Optional) Event number to trigger when the rising or falling threshold exceeds its limit. This value is identical to the *alarmRisingEventIndex* or the *alarmFallingEventIndex* in the alarmTable of the RMON MIB.
falling-threshold *value*	Specifies the value at which the alarm is reset.
owner *string*	(Optional) Specifies an owner for the alarm, which is identical to the *alarmOwner* in the alarmTable of the RMON MIB.

Command Default

No RMON alarms are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The MIB object must be specified as a dotted decimal value after the entry sequence (for example, ifEntry.10.1). You cannot specify the variable name and the instance (for example, ifInOctets.1) or the entire dotted decimal notation. The variable must be of the form *entry.integer.instance*.

To disable the RMON alarms, you must use the **no** form of the command on each configured alarm. For example, enter **no rmon alarm 1**, where 1 identifies the alarm to be removed.

Examples

The following example shows how to configure an RMON alarm using the **rmon alarm** command:

```
rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-threshold 0 owner user1
```

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.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

rmon collection history

To enable RMON history gathering on an interface, use the **rmon collection history** command in interface configuration mode. To disable the history gathering on an interface, use the **no** form of this command.

rmon collection history controlEntry *integer* [**buckets** *bucket-number*] [**interval** *seconds*] [**owner** *ownername*]

no rmon collection history controlEntry *integer* [**buckets** *bucket-number*] [**interval** *seconds*] [**owner** *ownername*]

Syntax Description

controlEntry	Specifies the RMON group of statistics using a value.
integer	Integer that identifies the RMON group of statistics and matches the index value returned for SNMP requests. The range is from 1 to 65535.
owner	(Optional) Specifies the name of the owner of the RMON group of statistics.
ownername	(Optional) Name of the owner of the RMON group of statistics.
buckets *bucket-number*	(Optional) Specifies the maximum number of buckets desired for the RMON collection history group of statistics.
interval *seconds*	(Optional) Specifies the interval, in seconds, when history should be gathered in a single bucket. When the interval ends, history is collected into a new bucket.

Command Default

The RMON history gathering is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use the **show rmon capture** and **show rmon matrix** commands to display RMON statistics.

Examples

The following example enables RMON history collection with an ID number of 5 and an owner named user1.

```
Router(config-if)# rmon collection history controlEntry 5 buckets 5 interval 10 owner user1
```

Related Commands

Command	Description
show rmon capture	Displays the RMON buffer capture table and current configuration.
show rmon matrix	Displays the RMON matrix table and values associated with RMON variables.

rmon collection host

To enable a RMON MIB host collection group of statistics on an interface, use the **rmon collection host** command in interface configuration mode. To remove the specified RMON host collection, use the **no** form of the command.

rmon collection host controlEntry *integer* [**owner** *ownername*]

no rmon collection host controlEntry *integer* [**owner** *ownername*]

Syntax Description

controlEntry	Specifies the RMON group of statistics using a value.
integer	Integer that identifies the RMON group of statistics and matches the index value returned for SNMP requests. The range is from 1 to 65535.
owner	(Optional) Specifies the name of the owner of the RMON group of statistics.
ownername	(Optional) Name of the owner of the RMON group of statistics.

Command Default

RMON host collection is not specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use the **show rmon hosts** and **show rmon matrix** commands to display RMON statistics.

Examples

The following command shows how to enable an RMON collection host group of statistics with an ID number of 10, and specifies *user1* as the owner:

```
Router(config-if)# rmon collection host controlEntry 10 owner user1
```

Related Commands

Command	Description
show rmon hosts	Displays the RMON hosts table.
show rmon matrix	Displays the RMON matrix table and values associated with RMON variables.

rmon event

To add or remove an event in the RMON event table that is associated with an RMON event number, use the **rmon event** command in global configuration mode. To remove an event in the RMON event table, use the **no** form of this command.

rmon event *number* [**log**] [**trap** *community*] [**description** *string*] [**owner** *string*]

no rmon event number

Syntax Description

number	Assigned event number, which is identical to the *eventIndex* in the eventTable in the RMON MIB.
log	(Optional) Generates an RMON log entry when the event is triggered and sets the *eventType* in the RMON MIB to *log* or *log-and-trap*.
trap *community*	(Optional) Specifies the SNMP community string used for this trap. Configures the setting of the *eventType* in the RMON MIB for this row as either *snmp-trap* or *log-and-trap*. This value is identical to the *eventCommunityValue* in the eventTable in the RMON MIB.
description *string*	(Optional) Specifies a description of the event, which is identical to the event description in the eventTable of the RMON MIB.
owner *string*	(Optional) Owner of this event, which is identical to the *eventOwner* in the eventTable of the RMON MIB.

Command Default

None.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to enable the **rmon event** command.

```
rmon event 1 log trap eventtrap description "High ifOutErrors" owner user
```

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 SNMP trap when the event is triggered.

Related Commands

Command	Description
rmon	Enables Remote Network Monitoring (RMON) on an Ethernet interface.
rmon alarm	Sets a RMON alarm on a MIB object.
show rmon	Displays the current RMON agent status on the router.

show controllers

To display the RMON performance parameters for 15 minute or 1 day intervals, use the **show controllers** command in privileged EXEC mode.

show controllers dwdm *slot/port* **pm interval** {**15-min** | **24-hour**}

Syntax Description

slot/port	Slot and port.
pm interval	Specifies the interval for performance monitoring.
15-min	Displays the performance parameters for a 15-minute interval.
24-hour	Displays the performance parameters for 1 day interval.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to display the RMON performance parameters for a 15-minute interval.

```
Router# show controllers dwdm 4/3 pm interval 15-min
```

show rmon

To display the current RMON agent status on the router, use the **show rmon** command in privileged EXEC mode.

show rmon [**task** | **alarms** | **capture** | **events** | **filter** | **history** | **hosts** | **matrix** | **statistics** | **topn**]

Syntax Description

task	Displays general RMON statistics.
alarms	Displays the RMON alarm table.
capture	Displays the RMON buffer capture table and current configuration.
events	Displays the RMON event table.
filter	Displays the RMON filter table.
history	Displays the RMON history table.
hosts	Displays the RMON hosts table.
matrix	Displays the RMON matrix table and values associated with RMON variables.
statistics	Displays the RMON statistics table
topn	Displays the RMON top-n hosts table

Command Default

The **task** option is displayed.

Command Modes

Privileged Exec (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to display general RMON statistics.

```
Router# show rmon
```

```
145678 packets input (34562 promiscuous), 0 drops
145678 packets processed, 0 on queue, queue utilization 15/64
```

The following example shows how to display the contents of the RMON alarm table.

```
Router# show rmon alarms
```

```
Alarm 2 is active, owned by manager1
 Monitors ifEntry.1.1 every 30 seconds
 Taking delta samples, last value was 0
 Rising threshold is 15, assigned to event 12
 Falling threshold is 0, assigned to event 0
 On startup enable rising or falling alarm
```

The following example shows how to display the contents of the RMON capture table and current configuration.

```
Router# show rmon capture
```

```
Buffer 4096 is active, owned by manager1
 Captured data is from channel 4096
 Slice size is 128, download size is 128
 Download offset is 0
 Full Status is spaceAvailable, full action is lockWhenFull
 Granted 65536 octets out of 65536 requested
 Buffer has been on since 00:01:16, and has captured 1 packets
  Current capture buffer entries:
   Packet 1 was captured 416 ms since buffer was turned on
   Its length is 326 octets and has a status type of 0
   Packet ID is 634, and contains the following data:
00 00 0c 03 12 ce 00 00 0c 08 9d 4e 08 00 45 00
01 34 01 42 00 00 1d 11 e3 01 ab 45 30 15 ac 15
31 06 05 98 00 a1 01 20 9f a8 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00
```

The following example shows how to display the contents of the RMON event table.

```
Router# show rmon events
```

```
Event 12 is active, owned by manager1
 Description is interface-errors
 Event firing causes log and trap to community rmonTrap, last fired
00:00:00
```

The following example shows how to display the contents of the RMON filter table.

```
Router# show rmon filter
```

```
Filter 4096 is active, and owned by manager1
 Data offset is 12, with
 Data of  08 00 00 00 00 00 00 00 00 00 00 00 00 00 ab 45 30 15 ac 15 31
 06
 Data Mask is ff ff 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff
ff ff ff
 Data Not Mask is 0
 Pkt status is 0, status mask is 0, not mask is 0
 Associated channel 4096 is active, and owned by manager1
 Type of channel is acceptFailed, data control is off
```

```
 Generate event index 0
 Event status is eventFired, # of matches is 1482
 Turn on event index is 0, turn off event index is 0
```

The following example shows how to display the contents of the RMON history table.

```
Router# show rmon history
```

```
Entry 1 is active, and owned by manager1
 Monitors ifEntry.1.1 every 30 seconds
 Requested # of time intervals, ie buckets, is 5
 Granted # of time intervals, ie buckets, is 5
  Sample # 14 began measuring at 00:11:00
   Received 38346 octets, 216 packets,
   0 broadcast and 80 multicast packets,
   0 undersized and 0 oversized packets,
   0 fragments and 0 jabbers,
   0 CRC alignment errors and 0 collisions.
   # of dropped packet events is 0
   Network utilization is estimated at 10
```

The following example shows how to display the contents of the RMON hosts table.

```
Router# show rmon hosts
```

```
Host Control Entry 1 is active, and owned by manager1
 Monitors host ifEntry.1.1
 Table size is 51, last time an entry was deleted was 00:00:00
  Creation Order number is 1
   Physical address is 0000.0c02.5808
   Packets: rcvd 6963, transmitted 7041
   Octets: rcvd 784062, transmitted 858530
   # of packets transmitted: broadcast 28, multicast 48
   # of bad packets transmitted is 0
```

The following example shows how to display the contents of the RMON matrix table and values associated with RMON variables.

```
Router# show rmon matrix
```

```
Matrix 1 is active, and owned by manager1
 Monitors ifEntry.1.1
 Table size is 451, last time an entry was deleted was at 00:00:00
```

The following example shows how to display the contents of the RMON statistics table.

```
Router# show rmon statistics
```

```
Interface 1 is active, and owned by config
 Monitors ifEntry.1.1 which has
 Received 60739740 octets, 201157 packets,
 1721 broadcast and 9185 multicast packets,
 0 undersized and 0 oversized packets,
 0 fragments and 0 jabbers,
 0 CRC alignment errors and 32 collisions.
```

```
 # of dropped packet events (due to lack of resources): 511
 # of packets received of length (in octets):
  64: 92955, 65-127: 14204, 128-255: 1116,
  256-511: 4479, 512-1023: 85856, 1024-1518:2547
```

The following example shows how to display the contents of the RMON top-n hosts table.

```
Router# show rmon topn
```

```
Host Entry 1 of report 1 is active, owned by manager1
 The rate of change is based on hostTopNInPkts
 This report was last started at 00:00:00
 Time remaining in this report is 0 out of 0
 Hosts physical address is 00ad.beef.002b
 Requested # of hosts: 10, # of hosts granted: 10
Report # 1 of Top N hosts entry 1 is recording
Host 0000.0c02.5808 at a rate of 12
```

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets a RMON alarm on a MIB object.
rmon collection history	Enables RMON history gathering on an interface.
rmon collection host	Enables RMON MIB host collection group of statistics on an interface.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.

CDP Command Reference

This chapter describes commands used to monitor the router and network using Cisco Discovery Protocol (CDP).

cdp enable

To enable Cisco Discovery Protocol (CDP) on an interface, use the **cdp enable** command in interface configuration mode. To disable CDP on an interface, use the **no** form of this command.

cdp enable

no cdp enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled at the global level and on all the supported interfaces.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

CDP is enabled by default at the global level and on each supported interface to send or receive CDP information.

Examples

The following example shows how to disable CDP only on the TenGigabitEthernet4/1 interface.

```
Router# config terminal
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# no cdp enable
```

Related Commands

Command	Description
cdp run	Reenables CDP on a Cisco device.

cdp run

To enable the CDP, use the **cdp run** command in global configuration mode. To disable CDP, use the **no** form of this command.

cdp run

no cdp run

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled at the global level and on all the supported interfaces.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

CDP is enabled by default at the global level and on each supported interface to send or receive CDP information.

If CDP is disabled globally, you cannot enable it on each interface using the **cdp enable** interface configuration mode command.

Examples

The following example shows how to enable CDP on the TenGigabitEthernet4/1 interface, when CDP is disabled globally.

```
Router(config)# no cdp run
Router(config)# end
Router# show cdp
% CDP is not enabled
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# cdp enable
% Cannot enable CDP on this interface, since CDP is not running
Router(config-if)#
```

Related Commands

Command	Description
cdp enable	Enables CDP on a supported interface.

show cdp

To display global CDP information, including timer and hold-time information, use the **show cdp** command in privileged EXEC mode.

show cdp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following is a sample output from the **show cdp** command that shows that the current router is transmitting CDP advertisements every one minute (the default setting for **cdp timer**). Also shown is that the current router directs its neighbors to hold its CDP advertisements for 3 minutes (the default for **cdp holdtime**), and that the router is enabled to transmit CDP version 2 advertisements.

```
Router# show cdp
```

```
Global CDP information:
     Sending CDP packets every 60 seconds
     Sending a holdtime value of 180 seconds
     Sending CDPv2 advertisements is enabled
```

Related Commands

Command	Description
show cdp entry	Displays information about a specific neighbor device listed in the CDP table.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.
show cdp traffic	Displays traffic information from the CDP table.

show cdp entry

To display information about a specific neighboring device discovered using CDP, use the **show cdp entry** command in privileged EXEC mode.

show cdp entry {* | *entry-name* [**protocol** | **version**]}

Syntax Description

*	Wildcard showing all the CDP neighbors.
entry-name	Name of the neighbor. You can enter an asterisk (*) at the end of an *entry-name*, such as `show cdp entry dev*`, which would show information about the neighbor, device.cisco.com.
protocol	(Optional) Limits the display to information about the protocols enabled on a router.
version	(Optional) Limits the display to information about the version of software running on the router.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following is sample output from the **show cdp entry protocol** command. Only information about the protocols enabled on device.cisco.com are displayed.

```
Router# show cdp entry device.cisco.com protocol
```

```
Protocol information for device.cisco.com:
    IP address: 192.168.68.18
    CLNS address: 490001.1111.1111.1111.00
    DECnet address: 10.1
```

Related Commands

Command	Description
show cdp	Displays global CDP information, including timer and hold-time information.

Command	Description
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.
show cdp traffic	Displays traffic information from the CDP table.

show cdp interface

To display information about the interfaces on which CDP is enabled, use the **show cdp interface** command in privileged EXEC mode.

show cdp interface [*type number*]

Syntax Description

type	(Optional) Type of interface.
number	(Optional) Number of the interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following is sample output from the **show cdp interface** command with an interface specified. The status information and information about CDP timer and holdtime settings is displayed only for TenGigabitEthernet4/1.

```
Router# show cdp interface TenGigabitEthernet4/1
```

```
TenGigabitEthernet4/1 is up, line protocol is up
   Encapsulation ARPA
   Sending CDP packets every 60 seconds
   Holdtime is 180 seconds
```

Related Commands

Command	Description
show cdp entry	Displays information about a specific neighbor device listed in the CDP table.
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.
show cdp traffic	Displays traffic information from the CDP table.

show cdp neighbors

To display detailed information about neighboring devices discovered using CDP, use the **show cdp neighbors** command in privileged EXEC mode.

show cdp neighbors [*type number*] [**detail**]

Syntax Description

type	(Optional) Type of the interface connected to the neighbors.
number	(Optional) Number of the interface connected to the neighbors.
detail	(Optional) Displays detailed information about a neighbor (or neighbors) including network address, enabled protocols, hold time, and software version.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example is sample output from the **show cdp neighbors** command.

```
Router# show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                 S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,

                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce Holdtme  Capability  Platform  Port ID
10.64.107.251    Gig 37/3      176           R I   CPT 600   Gig 36/41
10.64.107.251    Gig 37/1      174           R I   CPT 600   Gig 36/43
10.64.107.251    Gig 36/41     134           R I   CPT 600   Gig 37/3
10.64.107.251    Gig 36/43     134           R I   CPT 600   Gig 37/1
10.64.107.251    Ten 3/2       132           R I   CPT 600   Ten 4/2
10.64.107.251    Ten 4/2       174           R I   CPT 600   Ten 3/2
```

The Device ID column in the output indicates the remote node ID and the Port ID column indicates the remote port.

Related Commands

Command	Description
show cdp entry	Displays information about a specific neighbor device listed in the CDP table.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp traffic	Displays traffic information from the CDP table.

show cdp traffic

To display information about traffic between devices gathered using CDP, use the **show cdp traffic** command in privileged EXEC mode.

show cdp traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example is sample output from the **show cdp traffic** command that specifies information about traffic between devices.

```
Router# show cdp traffic
```

```
Total packets output: 543, Input: 333
Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
No memory: 0, Invalid: 0, Fragmented: 0
CDP version 1 advertisements output: 191, Input: 187
CDP version 2 advertisements output: 352, Input: 146
```

Related Commands

Command	Description
show cdp entry	Displays information about a specific neighbor device listed in the CDP table.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.

Miscellaneous Command Reference

This chapter describes miscellaneous commands to configure CPT services.

show ip interface brief

To display the usability status of interfaces configured for various IP addresses, use the **show ip interface brief** command in privileged EXEC mode.

show ip interface brief [brief]

Syntax Description

brief	(Optional) Displays a summary of the usability status information for each interface.

Command Default

This command has no defaults.

Command Modes

Privileged EXEC

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The **show ip interface brief** command can be used to view a summary of the router interfaces. This command displays the IP address, interface status, and additional information.

Examples

The following is sample output from the **show ip interface brief** command:

```
Router# show ip interface brief
```

```
Interface              IP-Address      OK?    Method Status      Protocol
GigabitEthernet0/1     unassigned      YES    unset  up          up
GigabitEthernet0/2     192.168.190.235 YES    unset  up          up
GigabitEthernet0/3     unassigned      YES    unset  up          up
GigabitEthernet0/4     192.168.191.2   YES    unset  up          up
TenGigabitEthernet2/1  unassigned      YES    unset  up          up
TenGigabitEthernet2/2  unassigned      YES    unset  up          up
TenGigabitEthernet2/3  unassigned      YES    unset  up          up
TenGigabitEthernet2/4  unassigned      YES    unset  down        down
GigabitEthernet36/1    unassigned      YES    unset  down        down
GigabitEthernet36/2    unassigned      YES    unset  down        down
GigabitEthernet36/11   unassigned      YES    unset  down        down
GigabitEthernet36/25   unassigned      YES    unset  down        down
Te36/45                unassigned      YES    unset  down        down
Te36/46                unassigned      YES    unset  down        down
Te36/47                unassigned      YES    unset  down        down
Te36/48                unassigned      YES    unset  down        down
Virtual36              unassigned      YES    unset  up          up
```

The following table describes the significant fields shown in the display.

Table 1: show ip interface brief Field Description

Field	Description
Interface	Type of interface. **Note** The **show ip interface brief** command also displays GigabitEthernet interfaces. These interfaces reside on slot 0 and are used for internal communication between uplinks and Transport Node Controller (TNC).
IP-Address	IP address assigned to the interface.
OK?	**Yes** signifies that the IP address is currently valid. **No** signifies that the IP address is not currently valid.
Method	The method field has the following possible values: • RARP or SLARP—Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request • BOOTP—Bootstrap protocol • TFTP—Configuration file obtained from TFTP server • manual—Manually changed by CLI command • NVRAM—Configuration file in NVRAM • IPCP—ip address negotiated command • DHCP—ip address dhcp command • unassigned—No IP address • unset—Unset • other—Unknown
Status	Indicates the status of interface. Valid values and their meanings are: • up—Interface is administratively up. • down—Interface is administratively down. • administratively down—Interface is administratively down.
Protocol	Indicates the operational status of the routing protocol on this interface.

INDEX

N

P

R

S

T

V

X